White Paper

Procurement Considerations for Next-Generation Networks in the Public Sector

Introduction

Public sector business managers, technologists, and policymakers are increasingly turning to Information Technology (IT) to improve service delivery with the same or fewer resources. But IT procurement poses unique challenges because of the rapid pace of technological advances and lengthy timeframes for competitive processes. As a result, contracts can become obsolete even before the procurement process is complete. For example, existing contract vehicles for networking, communications, and data center technology did not foresee innovations such as cloud computing, the Bring-Your-Own-Device (BYOD) phenomenon, increasing use of video and web conferencing for collaboration and training; and network-connected sensors for public safety and facilities management.

Saddled with inflexible contracting vehicles, public sector organizations often must take on the burden of developing supplemental Requests for Proposal (RFPs) or Requests for Information (RFIs), and of re-issuing or withdrawing RFPs. These activities complicate the procurement process and can delay project starts, hampering government efficiency.

This white paper, intended for public sector CIOs and procurement officers, suggests how to develop flexible RFPs for the Next-Generation Network (NGN) in the public sector. The paper describes:

- IT innovations that governments are expected to adopt over the next decade to increase efficiency, improve citizen services, and reduce costs.
- Network capabilities needed to support current and emerging government services. These include the network infrastructure, cloud and data center solutions, collaboration services, physical security, and connectivity to service providers.
- Scoping the contract to gain the flexibility to take advantage of technological advances; changes in pricing and licensing models; manufacturing innovations; and catalog changes resulting from acquisitions or spinoffs.
- Terms and conditions that either increase or decrease the flexibility of the contract.

IT Trends

The public and private sectors are at the threshold of a massive transition in how and where work is performed. Just a few years ago, work was a place. You sat at a desk and used a PC to access information and applications hosted on on-premises servers. To meet with someone, you took a trip. To learn about departmental news, you went to a meeting or read a newsletter.

Today, work is no longer a place, but an activity. An increasingly mobile workforce expects remote access to use voice, video, and data services from anywhere, any time, on any device, including personal smartphones and tablets. Many existing contracting vehicles did not anticipate the contemporary government workplace, described in the following paragraphs.

Cloud Services

Cloud services are supplanting departmental servers. Some public-sector organizations are building private clouds to provide Infrastructure-as-a-Service (IaaS) to departments, save money, and reduce the wait time for new infrastructure from weeks to hours. Building a private cloud requires servers, storage, networking, and tools that automate provisioning to relieve IT teams from repetitive provisioning chores. Other organizations are using external cloud service providers, usually for IaaS or Software-as-a-Service (SaaS). Examples of SaaS include web conferencing, email security, web security, Gmail, and Microsoft 365. Connecting to a public cloud service requires network devices that provide the necessary performance, flexibility, reliability, and security.

Mobility

A more mobile workforce has created demand for BYOD policies and virtual desktops. Government employees increasingly use mobile devices, such as tablets and smartphones, to work, connecting over Wi-Fi and 3G/4G cellular networks. In a 2012 survey of government employees by Forrester Consulting, 94 percent said they regularly worked on laptops, 63 percent used smartphones, and 18 percent owned tablets, a rapidly growing portion. To offer a BYOD option, you need intelligent security systems and might also need Wi-Fi networks that can support more users. A related initiative is to shift to virtual desktops. With this architecture, applications and data reside in the data center instead of on your desktop PC. This means you can securely access your applications and data from anywhere, using any device, including a personal or government-owned tablet or a thin client. Desktop virtualization requires servers, storage, and networking. You might also want thin clients, a less expensive and longer lasting alternative to traditional PCs and laptops.

Pervasive Video

Video has become a mainstay for communications, collaboration, training, justice, and public safety. Employees in different locations can now collaborate with an in-person experience without travel time, costs, and greenhouse gas emissions. First responders view real-time video feeds of disaster scenes to increase situational awareness. In justice, prisoners, judges, and interpreters can appear in the courtroom without the expense and safety risk of travel. Video surveillance cameras monitoring highways can provide valuable information for safety and maintenance plans. Healthcare specialists can consult with patients in rural locations. Some state and local governments are considering using neighborhood video kiosks for citizen interactions, following the lead of private sector organizations like banks and retailers.

More Sophisticated Cybersecurity

In addition to protecting confidential information, governments now also need to protect vital services that operate over networks, from energy and transportation to world financial engines and intelligence operations. The

challenge is that today's attackers are more capable than before. In addition, the move to cloud services and mobile computing has altered the nature of security risks. Governments need solutions that can adapt quickly to new threats intended to siphon out private data or to bring down networks. Next-generation security solutions consider the context of a request (who, what, where, when, and how) to decide whether to grant it.

Software-Defined Networking

Network programmability helps government entities optimize existing bandwidth, postponing expensive upgrades. Software-Defined Networking (SDN) enables network devices to dynamically adjust the way they treat voice, video, and data traffic based on current demands. One example is reserving bandwidth during scheduled high-definition videoconferences. Another is making more bandwidth available in college residence halls when administrators don't need the bandwidth.

Big Data Analytics

Governments are beginning to analyze the "big data" they've collected to increase operational efficiency and deliver more personalized citizen service. The amount of data collected is doubling every two years. In government, the big data phenomenon creates new opportunities to better understand citizen habits, the economy, fraud and cost errors, efficient and effective healthcare, educational outcomes, the environment, and more. But traditional analysis tools cannot process huge data sets, which require highly scalable servers, storage, and connections between servers.

Internet of Everything

Networks increasingly carry communications from machine to machine as well as from people to people and people to machines. Today, less than one percent of the world's things are connected to the Internet. That's changing because a new scheme for Internet addresses, called IPv6, provides a practically unlimited number of Internet addresses. Soon, it will be commonplace for people, processes, data, and things to be connected, transforming government activities from public safety and environmental monitoring to facilities management. Examples of things that are now connecting to the Internet include video surveillance cameras, environmental sensors, vehicles, appliances, furniture, and even first responders' clothing. Imagine the ability to locate a firefighter trapped inside a burning building based on sensors sewed into the lining of a jacket. To participate in the Internet of Everything, you need servers, storage, and wired and wireless networks that reach everywhere to connect everything.

Shared Services

Public sector organizations increasingly share IT services to eliminate redundant expenses and gain economies of scale. The public sector has been sharing communications infrastructure and other IT products, software, and services for some time. Now governments and educational institutions are also beginning to share IT services such as virtual desktops, advanced collaboration applications, and infrastructure provisioning. Shared services provide economies of scale, enabling offices, agencies, and departments to introduce new capabilities that they could not afford on their own. Organizations that deliver shared services typically finance the infrastructure, recouping the costs through fees and agency chargeback. And organizations that use shared services convert up-front capital costs for servers and software to a predictable operational cost.

Network Capabilities for Government Services

IT solutions to public sector business needs generally require some combination of the following elements:

- Switches and routers
- Network services that operate in the background to provide a good user experience—for example, fast application response and smooth video
- Endpoints connected to the network such as IP phones, immersive videoconferencing systems, thin clients used to access virtual desktops, IP video surveillance cameras, door access controllers, or sensors
- Compute and storage
- Applications such as Voice over IP (VoIP), instant messaging (IM), or video surveillance monitoring

The success of any solution in meeting the business need depends on the quality of the switches and routers and the underlying network services. A good experience leads to high user adoption. If the experience is poor, employees will not use the solution. Therefore, when developing RFPs, keep in mind that switches are not commodities, like printers or cables. The least expensive switches do little more than transport data. In contrast, switches with the right set of advanced features can do much more, quickly paying back the incremental investment. For example, features that simplify management, automate port configuration, and accelerate troubleshooting can lower staff overhead. The ability to carry voice and video traffic can eliminate the costs of building and maintaining separate networks.

The following summarizes requirements for the NGN in the public sector.

Table 1. NGN Requirements in Public Sector

NGN Requirements in Public Sector
• **Low total cost of ownership:** Acquisition costs are only a fraction of the total cost of ownership. To lower operational costs, an NGN also needs easy-to-use management and troubleshooting tools and the ability to scale without a network redesign or equipment replacement. • **Global availability:** Availability has a growing impact on the business of government because the network supports critical applications for public safety and citizen services. The growing popularity of cloud services in government requires highly available connections to cloud service providers. • **Consistent quality of experience:** Successfully integrating collaboration capabilities, such as IM and videoconferencing, into business processes requires a good quality of experience. Without it, adoption suffers. • **Transport virtualization:** Rather than building and maintaining multiple networks for voice, video, energy management, and so on, governments are consolidating to a single physical network that supports multiple virtual networks. This lowers costs while also providing economies of scale for management, redundancy, and so on. • **Cybersecurity:** Attacks are becoming more frequent and more sophisticated. The NGN needs information assurance capabilities that allow high-priority applications to continue functioning even during attacks. Requirements include authentication, role-based access control, and prevention of attacks intended to bring down servers. • **Secure mobility:** An increasingly mobile workforce needs access to government services from anywhere, from any device—including personal tablets and smartphones. • **Support for video and other rich-media applications:** The NGN needs the performance and management tools to deliver a consistent video experience without interfering with the performance of other applications running over the same network. These are known as medianet capabilities. • **Energy awareness:** To lower energy consumption, the NGN needs to report energy utilization of devices connected to the network, and automatically power them down when appropriate. An example is powering down wireless access points and Internet Protocol (IP) phones when offices are closed.

Contract Scope

To increase the flexibility of contracts, instead of specifying a “box” that meets specifications such as speed or number of ports, consider writing requests for solutions, or architectures that meet a business need. **Table 2** lists examples.

Table 2. Examples of Requests for Solutions Instead of Products

Examples of Requests for Solutions Instead of Products
• Video or web-conferencing solutions to provide distance learning. • Unified communications to reduce telephone line costs and leverage the data network infrastructure. • Data center consolidation and virtualization solutions to reduce data center space, power, and cooling requirements and increase business agility. • Interoperable communications solutions that enable public safety employees to talk directly using any type of radio or phone and to increase situational awareness by sharing video, building floor plans, and so on. • Mobility solutions that enable eligibility-determination for workers, inspectors, home-health nurses, and other field personnel to retrieve and input case information from the field, lowering travel time and costs. • Video-based arraignment solutions to avoid the time, costs, and public safety risks of transporting prisoners to the courtroom. • Video interpretation solutions to avoid skyrocketing costs and judicial delays while overburdened contract interpreters travel between courtrooms.

To increase the flexibility of RFPs, request that equipment manufacturers submit proposals for all hardware, software, and professional services needed to meet the business need. Solution components include, but are not limited to, the categories shown in **Table 3**.

Table 3. Solution Requirements in RFPs for NGN

Network Infrastructure (Hardware, Software, and Services)
Access Routing
Managed LAN Switching
Wireless LAN for the Organization
Network Security
Virtualization
Optical Networking
Other Related Management/Monitoring Tools, Solutions, and Software
Maintenance Services, Installation and Configuration Services, Professional Services, and Training
Cloud/Data Center (Hardware, Software, and Services)
Content Security
Servers and Storage Area Networking
SaaS
IaaS
Unified Computing
Application Switching
Virtual Desktop
Maintenance Services, Installation and Configuration Services, Professional Services, and Training
Other Related Management/Monitoring Tools, Solutions, Software, and Services
Collaboration Services (Hardware, Software, and Services)
Unified Communications (VoIP and Web-based Tools)
Audio and Video Conferencing (Desk Top and Immersive)
Web Conferencing
Maintenance Services, Installation and Configuration Services, Professional Services, and Training
Other Related Management/Monitoring Tools, Solutions, Software, and Services
Physical Security (Hardware, Software, and Services)
Building Controls
Energy Controls
Video Surveillance

Sensor Networks
Maintenance Services, Installation and Configuration Services, Professional Services, and Training
Other Related Management/Monitoring Tools, Solutions, Software, and Services

Guidelines to maximize the flexibility of the contract:

- Allow manufacturers to provide all network-centric products and services in their price book that meet the scope of the RFP.
- Stipulate that solutions interoperate with existing networking equipment and other IP standards–based solutions.
- Insert a provision to include new network-centric IT products, services, or solutions that are within the RFP scope but not stipulated in the contract. Then contracting officers can add these technologies to the contract, at their discretion, if the product or service is commercially available through the contractor's current price book.
- Allow vendors to include third-party products or services as part of their overall solution. This avoids the need to develop multiple contracts for a single business solution.
- Include anticipatory provisions allowing manufacturers to request the addition of new technologies to their awarded contract offerings. It should not matter whether the products are developed in-house or obtained through product or company acquisitions.
- Make the statewide contracts from the RFP available to all governmental entities within each state, subject to applicable laws, including but not limited to state offices, agencies, departments, boards, bureaus, commissioners, institutions, and colleges and universities. Also make the statewide contract accessible by other downstream government entities, such as state authorities, local governments, municipalities, cities, townships, counties, K-12 school districts, and other political subdivisions of the state.

Terms and Conditions

Being aware of suppliers' perspectives on terms and conditions when you craft the RFP can help suppliers offer you advantageous pricing. In general, any non-standard terms or conditions increase the manufacturer's costs, which might result in lower discounts to the buyer. Following are examples:

- **OEM as Prime/Contractor Holder with Resellers as Subcontractors:** Allow manufacturers to use certified resellers as fulfillment agents. This benefits government customers by providing a local source of support and expertise. It also supports state interests in encouraging local hiring and other economic development activity.
- **Limitation of Liability:** Avoid contracts requiring unlimited liability. For products, the liability of each party should be reasonably limited to the greater of $100,000 or the money paid to the OEM under the contract during the 12-month period prior to the event that first gave rise to the liability. For professional services, the liability of the OEM should be limited to the amount paid by the customer during the six months preceding the event or circumstances giving rise to such liability.
- **Most Favored Nation Language or Similar Language:** The firm price requirement is inconsistent with many global OEMs' standard commercial practices, which consider volume commitments, fair-and-reasonable terms and conditions, and so on, when setting prices. The many variables that distinguish each opportunity make it difficult to compare contracts for Most Favored Nation (MFN) purposes.
- **Pricing Based on Minimum Discounts Versus Fixed Price:** The pricing for technology products generally decreases over the course of the product lifecycle. Therefore, it is more favorable for customers if the prime

contract is based on minimum discounts to the OEM's commercially published pricelists rather than fixed pricing. In addition, OEMs must retain the ability to update and refresh their respective price books, as long as the agreed-upon discounts are fixed. Minimum guaranteed discounts do not preclude OEMs and/or their authorized resellers from providing deeper or additional, incremental discounts at their sole discretion.

- **Capital Lease Financing:** To avoid the need for up-front capital outlay, government contracts should allow for manufacturers to offer capital lease financing arrangements under their awarded contracts.
- **Refurbished Equipment:** Allowing manufacturer-certified refurbished equipment gives government customers an option to obtain equipment at substantially lower cost. Attractive warranties address risk concerns.
- **Payment Terms:** The standard commercial payment term is net 30 days. Since many OEMs use resellers under their prime contracts as subcontractors, any payment term that exceeds 30 days will impose a financial hardship on these resellers, many of whom are small or medium-sized businesses.
- **Delivery, Inspection, Acceptance, and Rejection:** Publicly traded technology companies are required to recognize revenues in a timely fashion. Contract terms that require formal acceptance and/or inspection periods are unnecessary because purchasers are typically protected by the OEM's standard warranty and shipping terms.
- **OEM's Standard Warranty:** OEMs invest in complex systems, tools, and business processes to support their standard warranties on a global basis. Modifications to an OEM's standard warranties impose a significant operational and financial burden for the OEM, affecting overall pricing.
- **Standard Maintenance Offerings:** Global OEMs build standard maintenance offerings to provide consistent service levels and keep customer costs down. Contracts that require non-standard maintenance increase costs, affecting discounts.
- **Standard Software License:** To offer non-standard software license terms, OEMs would need to incur the costs to set up separate internal systems, tools, and resources.
- **Consequential, Incidental, Indirect, Special, or Punitive Exclusion:** It is standard in the IT industry to exclude consequential, incidental, indirect, special, or punitive damages in a contract. The potential risk exposure could exceed the contract value and even insurance coverage limits.
- **Liquidated Damages:** Standard terms in the IT industry do not encompass liquidated damages, which are not contemplated under the standard-terms-and-discount structure.
- **Rights and Remedies of State for Default:** It is standard for global OEMs to provide customers with remedies for default. However, it is unreasonable to ask OEMs to assume additional liability on "any loss or damage" incurred by a customer because such damage is equivalent to consequential, incidental, indirect, or special damage.
- **General Indemnity:** The scope of the indemnity should be reasonably limited to the OEM's products and services supplied under the prime contracts. The extent of the indemnification obligations should be apportioned relative to fault.
- **Patent, Copyright, and Trade Secret Indemnity:** It is common for technology vendors to require certain exceptions or exclusions to their IP indemnification obligations. For example, an OEM would not be responsible for indemnifying if its product was modified by a third party or by the OEM itself, or in accordance with the buyer's specifications or instructions. In addition, because OEMs face damages that could exceed the contract value, it is reasonable for OEMs to require limitations of liability with respect to the scope of its IP defense and indemnification obligations. Equally important, OEMs, as the IP owners of

their product offerings, should be able to control the defense of any indemnity claim, including settlement negotiations.

- **Rights in Work Product(s):** Such rights generally are only appropriate if the customer is hiring an IT vendor or OEM to create, develop, and/or build hardware and/or software that is *new, original,* or *unique*. Although OEMs may provide some customization to product offerings based on the buyer's technical requirements, such customization is typically limited in nature and does not justify providing buyer with rights into the developed work products.
- **Right to Copy or Modify:** Granting customers the right to copy or modify under an Indefinite Delivery, Indefinite Quantity (IDIQ) contract undermines the technology company's intellectual property rights and control of its assets. The exception is a formal licensing arrangement that includes royalties or licensing fees.
- **Stop Work Order:** These provisions result in significant revenue recognition issues under accounting rules for publicly traded corporations.
- **Returns:** Enterprise IT products are often configured for the customer's technical requirements, and cannot be readily resold if returned. Therefore, for enterprise IT products that are not "off-the-shelf," returns are acceptable only for defective items that are still under OEM warranty. It is standard practice for OEMs to have an "All Sales Final" term, subject to their warranty provisions, which allows for the repair or replacement of defective products.
- **e-Procurement or Online Catalog:** The shopping-cart buying method is not feasible for many enterprise IT products that require complex configuration during the manufacturing process. In addition, many OEMs have complex pricelists that cannot be easily translated or implemented into an online catalog format.
- **Confidentiality Provisions:** Technology companies understand the importance of maintaining their customer's information confidential and often agree to reasonable confidentiality provisions. Technology vendors expect that the confidentiality provisions are reciprocal given that they are routinely asked to share proprietary information regarding their product and services offerings in response to RFPs, RFQs, and other project proposals.
- **Contract Term:** The supplier community supports the existing practice of most customers in issuing multi-year, prime contracts or IDIQs, with automatic one- or two-year renewals or simple extensions. Given the time and resources that both the customer and awarded vendor invest to operationalize new agreements, it is mutually beneficial for all parties involved to have a reasonable multi-year contract term.

Summary

- To create flexible contracts that remain relevant as business needs and technology evolve, request architectures and solutions to business needs instead of limiting the request to specific products.
- Realize that complete solution architectures include some combination of switches and routers, network services, compute and storage resources, endpoints, and applications.
- Consider allowing vendors to include third-party products or services as part of their overall solution. This can reduce the number of contracts you need.
- Keep in mind that switches are not commodities. It is widely accepted that only 20 percent of a network's total cost of ownership is the up-front capital outlay, while the remaining 80 percent is ongoing operational cost. Upfront savings from low-cost switches are generally dwarfed by higher costs for maintenance, management, upgrades, and supplemental equipment needed to introduce new services.
- Become aware of terms and conditions that enable vendors to offer more favorable pricing.

For More Information

To download a copy of a white paper describing the Cisco vision for the NGN in the public sector and how to work efficiently with equipment manufacturers, contact your Cisco account manager or visit: www.networkcontracts.com

Acronyms

BYOD	Bring Your Own Device
IDIQ	Indefinite Delivery Indefinite Quantity
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
MFN	Most Favored Nation
NGN	Next-Generation Network
OEM	Original Equipment Manufacturer
PC	Personal Computer
RFI	Requests for Information
RFP	Requests for Proposal
RFQ	Request for Quotation
SDN	Software-Defined Networking
VoIP	Voice over Internet Protocol

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA CXX-XXXXXX-XX 10/11