



Cisco Government Solutions Showcase

Cisco's Government Solutions are Ready to Roll!

- ? Reliable wireless capability that performs in both everyday government-to-government or government-to-citizen applications, and during critical situations.
- ? Voice and data integrated to ensure effortless inter/intra agency communication for an entire organization, between headquarters, and regional as well as field offices.
- ? Ironclad security solutions that ensure informational integrity, and protect performance system-wide, from servers to workstations.

These are no longer distant technological aspirations. These are essential capabilities poised to maximize the efficiency and effectiveness of the Federal, state and local governments throughout their most essential responsibilities. The source for these capabilities is Cisco Systems.

Understand the benefits *and* appreciate the technology.

Step inside the 18-wheeler, and you'll find a series of demonstrations that showcase Cisco solutions. This format was designed to enable customers with the opportunity to realize what sets Cisco apart.

Essential Technologies

Voice: The fundamental means of communicating, voice contact has evolved to include video conferencing. Concurrent with perfecting these capabilities, Cisco is also using advanced software to unify voice platforms. This allows government organizations to leverage their networking infrastructure so that it supports voice communication with the same universal reach as its data communication.

Integrating government communications infrastructure and IP results in management solutions with unified messaging. The result is communication throughout government organizations at any time, to any place. Whether in a field office, regional office, or working from remote locations, all phones, PDAs, tablets or notebooks remain intrinsic and identifiable. Furthermore, the communications management strategy for an entire enterprise can be controlled from a single, central location.

This solution also bridges the gap between email and voice mail. Email can be checked through a communications portal via phone, letting a user actually "listen" to their email. Conversely, a user could also retrieve voice messages as email text. Regardless of how a message originates, it will be received – and under the constant reassurance of a single, secure, unified network.

Security: Paramount on any priority list is guarding against current, as well as potential threats to the system integrity of our government. Foundational to Cisco's security ideology is our "Defense-in-Depth" approach. Rather than rely on a single layer of security, we interlock VPN infrastructure with advanced firewall and intrusion-detection technologies. This ensures secure connectivity between multiple locations such as

headquarters, regional offices and field offices. Furthermore, it suppresses unwanted system traffic, and simplifies the ability for a single management station to prevent malicious technological sabotage. When coupled with Cisco Security Agent, a host-based intrusion detection that stops attacks on an individual workstation level, it creates a complete security solution addressing every level of potential compromise that an agency or department might face.

IP Contact Center: Contending with an endless flow of calls can present a resource-allocation nightmare to government agencies. Cisco's IPCC automatically manages call distribution, and uses Interactive Voice Response to provide callers with a pro-active means of obtaining information even before a representative is needed. If callers, either department employees or citizens, require representative assistance, the system automatically searches for the best-available agent, which streamlines call management and minimizes caller wait-times. Innovative "screen-pop" capability eliminates the need for re-authentication. Web-collaboration sessions allow agents to perform guided web navigation on the caller's behalf, synchronizing an agent's browser screen to the caller's. Web users can even request assistance through the web, clicking a button to establish an automatic voice callback that is connected as soon as the next agent is available.

Infrastructure: From extensive HQ operations to smaller field offices, every government office must be equipped with complimentary technologies including voice, video and data converged over a secure infrastructure. What's more, their capability must not be compromised if any location is disconnected from the overall network.

To ensure this level of performance reliability, Cisco offers a spectrum of products tailored to the specific needs of any size operation. At a headquarters facility, higher-end solutions use integrated Blade technology, firewalls, and VPN and IDS modules integrated onto a single switch. This eliminates costlier implementation of individual appliances, and expedites overall control. In a field office, these technologies are provided via integrated software inside a single router. This gives a small location the same capability as HQ without the need to purchase individual appliances or a "big box". Whether Blade, Appliance or Software, implementation is also established using the same policy; this provides a single security posture across the organization, and centralizes management through a single interface.

Storage Area Networks: Preserving informational integrity, allowing for ease-of-access when necessary, guaranteeing the ability to accommodate expansion, performance-continuation assurance – these are the imperatives of a Storage Area Networks. Key advantages are also the use of storage networks to archive video surveillance data for subsequent review, and the use of Cisco SAN architecture to incorporate IP services into fibre channel SANs. This allows SAN development in a main government data center. Using advanced disk arrays and storage routers, the SAN also becomes the bedrock of business-continuance assurance, a critical component for government planners. Additional innovations allow users to access the storage resources consolidated within the SAN using a host attached to an existing IP network, or even remote SAN sites via TCP/IP.

Mobility: Government users understand that today's technology is untethered. The challenge becomes providing mobility that includes complete network connectivity, ease-of-access and stalwart security emulating anything found in a base office. Cisco provides mobile communications that empowers a field office or remote operation, and also ensures reachback to a regional office. Deployment of specialized routers (capable of being powered by a cigarette lighter) provides serial connectivity even between multiple network technologies. Seamless network rollover links notebooks and tablet PCs to the Mobile IP, and then back to a regional office. This allows government business to continue anytime, anywhere.