WHITE PAPER

CDW·G PEOPLE WHO GET IT™

# MOBILE STRATEGIES FOR GOVERNMENT

## Taking advantage of smartphones and tablets to boost efficiency and improve services

In the landmark digital government strategy, "Building a 21st Century Platform to Better Serve the American People," federal CIO Steve VanRoekel sounds a battle cry for more mobility, both for government itself and for the people it serves.

Mobile computing forms the foundation for what might be dubbed Government 3.0, building on earlier technology adoptions. Gov 1.0 connected workers by e-mail and launched first-generation websites. Gov 2.0 added online services and transactions, built out wireless capabilities and promoted telework. Now, Gov 3.0 envisions pervasive, ubiquitous computing that delivers government services to the public via mobile devices using light, quickly deployed and secure applications.

It also foresees government workforces moving beyond simple telework, which implies fixed telework centers or home offices. Using broadband and high-powered mobile devices, workers can now access applications developed or reengineered specifically for mobility.

TWEET THIS!

## Table of Contents

State, county and municipal governments have also joined the mobility drive, eager to take advantage of the cost reductions and innovation the new mobile era brings.

This white paper will review the benefits of a forward-looking mobile strategy, the challenges and opportunities of emerging bring-your-own-device (BYOD) strategies, mobile security, device and wireless provider selection, and how to ensure that a wireless network infrastructure supports mobile activities.

## Today's Mobility Principles

To get a bead on where mobility is going, it's important to understand the principles on which a mobile strategy is built.

**Mobility is information-centric.** Digital government implements an information-centric approach that aims to bridge the gap between structured, digital data and the vast quantities of unstructured information that remain beyond the effective reach of data systems.

This unharvested information exists in a variety of forms, ranging from paper to word-processing documents, spreadsheets, presentations and PDFs. According to the federal report, this plethora of information represents a "national asset with tremendous potential value to the public, entrepreneurs and to our own government programs." The White House would like to have agency IT leaders tag and otherwise digitize the unstructured information to make it available for applications.

The corollary idea ensures that the resulting data isn't tied to any given application or system, but rather exists as a separate resource freely available to the public, to commercial entrepreneurs and to government agencies themselves. Separating data from applications plays into a mobile strategy by enabling device and application independence. Key to that enablement are open-source application programming interfaces for data sets.

**Mobility requires a shared platform.** Few agencies have anything similar to the IT budgets of the late 1990s and early 2000s. Freeing up development dollars for mobile government innovation requires squeezing cost out of other areas of the IT budget. The digital-mobile strategy envisions much greater use of shared services by cooperating agencies as a way to reduce the cost of infrastructure, maintenance and operations.

This reasoning recognizes the potential in sharing software code, storage and network infrastructure (think cloud computing). Perhaps most important, it recognizes some of the best thinking going into mobility. Sharing also promises savings via the pooled acquisition of formerly fragmented purchases, particularly wireless services and devices.

**Mobility is customer-centric.** Creating the best user experience for government staff and constituencies sounds like a no-brainer. So why don't more agencies do it? The 21st Century Platform Policy demands fidelity to the idea of service delivery optimized for mobile environments.

That's an end state, certainly, but it's also a way of thinking about and approaching mobility. It also prescribes both a strong, intra-governmental governance process for diffusing best practices and the regular measurement of user satisfaction, usability and utility according to objective standards.

**Mobility effects security and privacy.** Governments must ensure the security of sensitive data and personal information attached to applications, and mobility complicates this objective. Government data is a favorite target of cybercriminals. Without special attention, mobile devices can be particularly susceptible to being compromised, and the inevitable breaches would undermine citizens' confidence in mobile applications.

The White House has tasked three agencies — the Defense and Homeland Security departments and the National Institute of Standards and Technology — to develop a specialized mobile security/privacy strategy. The need is no less urgent at the state and local level.

## The Benefits of a Forward-looking Mobile Strategy

When they mandated a decennial census, the authors of the Constitution had no idea what an information locomotive the federal government would become. Today, the U.S. Census Bureau alone generates terabytes of data monthly.

Census operates within the Department of Commerce, which encompasses several other data-intensive agencies, including the National Oceanic and Atmospheric Administration, the National Institute of Standards and Technology and the U.S. Patent and Trademark Office.

Data growth isn't just a federal issue; it drives innovation at the state and local level as well. Municipalities that once stuck push-pins on maps to detect crime trends now combine digital maps with other applications to create countless government and citizen services.

Agencies at all levels of government are working to make better use of the data they generate, both for program and mission improvement and for deploying better services to their constituencies. Increasingly, those initiatives have a mobile component.

Consumer mobile devices have educated millions to the possibilities inherent in mobile apps. Now consumers want to take their mobile devices and applications to work with them. Citizens who conduct commerce using mobile devices increasingly want government services delivered the same way.

## More Productive Staff

Data gathering requires data collectors. While the Census might be the largest example of field data acquisition by people, government workers hit the streets every day with mobile devices to collect data on human services, agriculture, traffic and engineering, wildlife and forestry, air and water quality, law enforcement and security, geography and housing.

Standard notebook PCs are certainly useful in some field situations. However, they should be considered portable technology, rather than truly mobile. And early mobile devices lacked the combination of connectivity, processing power and display/input capability for handling front-end information gathering.

Today's super lightweight smartphones and tablets feature advanced microprocessors, high-resolution displays and fine-grained touch screens. Those qualities, plus a flat form factor and multiple-hour battery life, let these devices blend easily into mobile workers' routines. Staff work more efficiently, and agencies benefit from a shorter time between field activity and when data is available to applications.

More powerful devices offer more flexibility in configuration. Information can be processed locally and simply stored on-board for later uploading to a government data center.

### Mobile Inspectors Get a Productivity Boost with Tablets

Certain types of government workers have always been mobile — inspectors, for example. Their basic work model consists of gathering data in the field and then processing it as a report that is used for decision-making or results in some sort of permit.

Until now, staff tended to perform these steps serially. Even when they gathered data electronically, for most jurisdictions the process would be gather and store, then return to the office and upload.

That was the case for one unit of the New York City Department of Transportation. Inspectors in its Highway Inspection and Quality Assurance (HIQA) division have used tablets for nearly a decade, originally ruggedized units lacking wireless capability.

To be sure, the older devices saved paper and time. They were replaced with lighter, but still durable, HP EliteBook convertible notebooks. Now the IT staff is issuing true tablet PCs: Asus Eee Slate EP121 devices running Windows 7, equipped with a full-featured mobile app that requires no keyboard.

HIQA workers access a wireless network to upload data from street inspections on the spot, reducing the time required for issuing street work permits from three days to one day.

More commonly, data is collected and immediately transmitted over a broadband connection so no sensitive information is stored in the field.

## Better Service to End Users

The app phenomenon (plus ubiquitous broadband) has conditioned people to expect online services wherever and whenever they want them. In the mid-1990s, the advent of the Internet sparked the movement to online government services. Twenty years later, smartphones are selling worldwide at a rate of more than 400 million per year.

Here again, governments have discovered how to offer citizens and businesses mobile access to services. In spring 2012, President Obama reiterated a call from early in his administration for federal agencies to offer more services as mobile applications. The mobile app initiative is coupled with another standing project, data.gov. Agencies post data sets in accessible formats to the data.gov website, where they become available to anyone who wants to build an app.

As of midsummer 2012, the General Services Administration's online app download site listed a modest 235 government-developed apps in all categories available to the public for iOS, Android and BlackBerry devices. But independent developers have been busy: For example, while the USA.gov app store has just a few NASA apps, a search of the Apple App Store shows dozens of applications that make use of NASA's data.

A robust app market has also developed at the state level. For example, California offers citizens mobile versions of many state websites, plus dozens of state-developed apps.

## More Cost-effective Use of Budget

When staff can perform the same amount of work on a less expensive device, organizations see a nearly instantaneous savings in hardware. As part of its mobile strategy, the Bureau of Alcohol, Tobacco, Firearms and Explosives is retrieving notebook PCs from contract workers and state and local partner officers. They'll have their accounts virtualized and can then use whatever devices they wish.

Mobility brings other efficiencies: With workers spending less time tethered to their desks, agencies have the opportunity to trim their office real estate, substituting hoteling space for cubicles.

Other efficiencies, more difficult to quantify, are equally appreciated: the speed with which staff can access files and data, and the fact that they can do so at a moment's notice anytime, anywhere.

# Mobility and BYOD Initiatives

It wasn't that long ago that the earliest PCs in large organizations were rogue devices spirited in by early adopters. Analysts, researchers and other knowledge workers understood the value of the then-new tools such as VisiCalc.

In that sense, the BYOD concept isn't new. But for the most part, the PC first became an important technology for work; PCs for the home came later.

Today's BYOD movement is driven by people whose personal lives have been revolutionized by the power and flexibility of mobile devices. In earlier generations, work requirements drove innovation. But mobility has reversed that model. The consumerization of IT now drives how large organizations think about technology, access and applications. Mobility ties it all together.

Public-sector organizations were startled when BYOD first surfaced as a computing strategy in 2010. Agency managers were justifiably worried about the costs involved if everyone in an agency or department were to simply expense his or her personal device and wireless plan.

But in fact, several models for BYOD have emerged that keep users satisfied and productive, while reducing costs for agencies. Many organizations use BYOD rollouts to revamp wireless acquisition strategies and consolidate plans. For example, the U.S. Department of Agriculture slashed its mobile phone costs by 20 percent, or $400,000 per month, simply by aggregating its requirements and renegotiating with carriers.

Just as notebook PCs provided an exponential leap in portable productivity over early desktop behemoths, sleek mobile devices provide more ubiquitous productivity than do notebooks, thanks to their long battery life, light weight and near-zero boot-up time.

## BYOD Challenges

It can be a management challenge when individual users choose their own devices. Restricting choices to an approved list can help. However, because users have access to an organization's applications, an acceptable-use policy is imperative. Such policies should stipulate not only the user's responsibilities, but also the rights of the organization with respect to the user's device and should include these elements:

- **Applications:** The policy should specify which outside applications have been approved, and which have not.
- **Personal-use restrictions:** The policy should make clear what users can and cannot do with the device; for instance, prohibiting the types of websites that can't be visited on agency-owned computers.
- **Access**: The policy should clarify the agency's access to the device; for instance, to install a security app that creates a "sandbox" for government apps within the device's memory.
- **Security:** The agency must be able to remotely wipe the device in the event of loss (which means personal apps, photos and such would be lost).
- **Data ownership:** The policy should set procedures for retrieving the government's data when the staffer leaves, or changes agencies or jobs.

Specific security and data privacy policies that apply to agency information remain in place no matter who owns the device. This may require workers to periodically bring devices in so the IT department can make sure security configurations are up to date.

## Ensuring Acceptance of BYOD

The consumerization of IT has driven the BYOD trend. But how well such a program is accepted depends less on who pays for the device than on how carefully the program is structured.

Some critics believe that because users have never had to buy their own desktop or notebook PCs, they would balk at a program requiring them to pay for their own devices. But that assumption isn't borne out.

First, workers bring devices they have already chosen for themselves in their personal lives, so BYOD lets them streamline by consolidating on one device. That makes it an enhancer of efficiency and productivity. Second, when people are already paying for personal talk and data plans, in many cases there is little additional cost to them when adopting BYOD.

### USDA Revs Up Data Collection with Apple iPads

Often the biggest payoff with mobile technology occurs with workers who are already out and about. Replacing pencil-and-paper forms with tablets and well-designed digital forms can really rev up the efficiency and accuracy of field data gathering.

A case in point: The National Agricultural Statistics Service, a unit of the Agriculture Department, collects crop statistics through hundreds of onsite surveys each year. NASS uses part-time enumerators, many of them well past the age of the typical digital native.

Yet NASS officials have had success with iPads. In fact, the effort requires only about a day of training, after which the enumerators — some in their 80s — are ready to go into the field to gather data.

Typically, the iPads' 4G Long Term Evolution (LTE) wireless capability transmits data to agency computers as it's collected. In rural areas where wireless cellular service is nonexistent, data can remain temporarily on the device. But the default mode is for immediate transfer for security purposes. Connectivity ensures security of personally identifiable farm data by bypassing storage.

But agency management can actively encourage BYOD acceptance. Among the best practices are the following:

- **Support the latest devices.** In this rapidly evolving market, don't wait too long to approve a particular mobile device; it may be quickly upgraded or even discontinued.
- **Mobilize enterprise apps.** Optimize the interface and data storage architecture for mobile technology.
- **Make purchasing easy.** By offering department- or governmentwide contracts with broad-line resellers, the government gets good prices and staff avoid the hassle of retail wireless stores.

Citizens and business constituencies also expect mobile government services that are comparable to what is available from commercial services. In many cases, the bar isn't very high. But most governments are still at the beginner's level: Information and nontransactional forms are often available through mobile apps. But core governmental functions, such as driver's license renewals or building permit applications, usually are not.

# Mobile Security

Initially, the mobility trend's security challenges spooked government IT shops — understandable, given tales of lost notebooks and the intermingling of data that occurs on devices with multiple apps.

But agencies at all levels understood the power of mobility to improve fieldwork, enable telework, cut IT costs and offer new services to citizens. And industry leaders, recognizing the security deficiencies, responded.

IT leaders should take a comprehensive view of mobile security as they develop a mobility strategy — that is, security should encompass hardware and software, and it should address user behavior as well as technical security issues. Put another way, think of a security plan as something that applies to the people, the devices and the applications.

Policy underpins security activities. A thorough security policy encompasses four basic mobility elements:

- **User authentication**
- **Application and memory isolation** (to keep the organizational and personal components apart within a device, coupled with data encryption)
- **Device visibility** (within the mobile device management system, which in turn should be visible to the network or unified communications management system)
- **Remote disabling and erasure**

Limiting device selection can head off some security problems. Although security solutions exist for all of the major mobile OSs — iOS, Android, Windows and BlackBerry — attempting to support a plethora of devices will boost expenses and complexity, leaving agencies vulnerable. Choose two OSs to concentrate on.

## Mobile Device Management

MDM is both a class of products and a strategy for securely deploying mobile devices in volume. An MDM strategy ensures that the government's IT department maintains situational awareness of its device fleet — where they are, whether they are configured properly, if software (including security patches) are up to date. MDM guarantees that physical loss does not become data or privacy loss.

MDM tool offerings have grown rapidly, both in functionality and in the number of software makers that offer them. IT departments have ample choice when selecting a vendor to support their mobility strategies. MDM tools have two basic components: an administrative console hosted on a server either onsite or in the cloud, and a client element loaded onto each mobile device.

Key MDM functions include software provisioning, remote backup, remote wiping and locking of lost devices, and GPS tracking. Cloud-hosted MDM solutions are increasingly popular in IT shops that want to avoid the cost of software acquisition and ongoing maintenance, or that lack specific MDM expertise.

MDM package selection should be based on organizational policies that dictate how and where documents and other data are stored. Product functions to look for include the following:

**Secure e-mail and text messaging services:** Most devices don't have this capability natively. It should be present when staffers use agency e-mail and personal accounts on the same device. Clients can be configured in such a way that work documents on the device are invisible to all but the authorized, secured e-mail client.

**Virtual private network clients:** VPNs are used to protect data in transit.

**Secure sandboxes:** On a network or server, sandboxes are usually employed to prevent unsecured applications or test code from infecting adjacent resources. In mobile applications, the model is reversed. Applications execute in a restricted block of memory to prevent whatever else is on the device from touching them.

## Encryption

Encryption of data at rest and in motion is another building block of mobile security. Many MDM packages feature encryption capabilities for documents and other data that may be stored on the device. Whether deployed through MDM or through separate software, encryption is key to device security.

The point of mobility and supporting cloud infrastructures is to offer an alternative (where warranted) to the standard computing model of mass storage on fat clients. Encrypting

### The Cost of Mobility

IT staffs and CIOs understand the efficiencies gained from mobile strategies, but they also know the costs. Because the clamor from users is pushing most organizations into mobility, the IT team must master the costs. The following elements are key to controlling mobility costs.

**Minutes and data plans:** Large organizations can negotiate pooled-minute deals with carriers based on use estimates, then monitor each device's usage and adjust individuals' minutes. Others reimburse or pay for one device only, even though some users carry multiple devices.

One solution for multiple data plans is to require the use of Wi-Fi hotspot devices. Some phones have built-in hotspots for connecting multiple wireless devices, but they burn through battery recharges quickly.

**Device prices:** Governments can either institute BYOD policies or create a catalog of approved devices that they will pay for.

**Software licenses:** Software license costs can balloon when installed on two or three devices per user. Negotiate concurrent-use licenses or limit instances for each user.

full hard disks is expensive and cumbersome, and the danger of leaving open data on notebooks is unacceptable.

That's why many agencies don't allow any local document storage on mobile devices. Some MDM solutions encrypt local documents once the user closes them, and then pulls them off the device and into the cloud or data center.

## Addressing Malware

Malware has not fully emerged as a problem for mobile OSs and applications at the enterprise level. This is partly because the iOS and Android OSs have a surprising amount of malware resistance built in, and their developer registration programs are designed to keep cybercriminals out.

Plus, malware writers tend to aim their attention at downloaded consumer apps unprotected by VPNs, not application clients running in a sandbox. More dangerous are phishing messages to which recipients respond on their mobile devices.

## Authentication Solutions

The password remains a viable component of any user authentication system, and agencies should implement strong password policies.

More organizations are adding a second authentication factor. Options include public-key infrastructure (PKI) tools with one-time-use credentials delivered via text message. Stronger still are encryption-decryption keys stored on removable memory cards. Biometric authentication is gaining traction on mobile devices, mainly with fingerprint readers. A great deal of research is being conducted on facial and iris recognition using built-in cameras.

# Choosing a Provider

As noted earlier, staffers who bring their own device into the workplace often bring their own voice and data plans. But that's not always the case. When choosing a provider, keep in mind that few contractors will be more closely tied to a public-sector agency's operations than its telecom carrier. Carrier selection exerts a huge influence on costs, reliability of operations and cybersecurity. Choosing a carrier requires a careful acquisition strategy because government-size organizations can't switch carriers as simply as consumers can.

Of course, only a limited number of wireless carriers can deliver agency-quality service across a state or region. Mobile users who travel outside of their local geographical area might encounter roaming charges or gaps in service. Some government missions depend on guaranteed service in disaster scenarios, when infrastructure suffers damage or a surge in use overwhelms the cellular capacity in a given area.

## Requirements

Organizations must carefully evaluate their own requirements before enlisting a carrier. The more clearly that competing carriers understand government requirements, the better they'll be able to offer bids that meet those technical needs. At the federal level, established governmentwide telecom contracts — principally, Networx from the General Services Administration — don't absolve individual agencies from thorough requirement analysis.

The chief considerations in establishing telecom requirements are the following:

**Number of users:** How many users will the IT department need to support, and what will their aggregate usage be? Note that telephone minutes and data usage need separate calculations.

**User locations:** Where are users located? This information is needed to map against carriers' coverage. Although broadband wireless is more ubiquitous than it was even five years ago, significant gaps remain, especially with 4G Long Term Evolution (LTE) coverage.

**Data requirements:** Will users regularly move large documents to and from mobile devices or merely send ASCII text gathered in forms? Will they need to view video content or just check websites?

## Choosing a Carrier

In addition to AT&T, Sprint Nextel and Verizon, about three dozen wireless carriers belong to the Cellular Telecommunications and Internet Association. The federal government must, in most instances, deal with companies offering national service. State, county, municipal and tribal

governments may find good deals with regional carriers that link to national networks.

Determining a carrier's coverage area should be the primary consideration when soliciting bids. To verify a carrier's map, take a phone, hop in a car and drive to remote locations within the jurisdiction to test coverage.

Also, make sure the carrier's available devices fit an agency's needs. The iPhone is more widely available now that it has migrated from AT&T. Yet many agencies opt to remain with BlackBerry. Few regional carriers sell all of the big three: iOS, Android and BlackBerry devices. Survey users to determine what mix of touch-screen and keyboard devices is needed.

After narrowing down the possible carriers to those that offer the required coverage and devices, determine the rates for voice, data and roaming. Investigate billing practices too. Will the carrier bill in the aggregate or phone by phone? Will unused capacity carry over month to month? And how does the carrier handle international and out-of-network calls?

## Device Options

When offering devices to staff, organizations face a bewildering array of mobile devices from half a dozen manufacturers. The consumerization trend has spawned staff who are often adamant about what devices they'll work with.

It's possible — and necessary — to narrow down the choice of devices. Start with the many independent sources of smartphone and tablet information. As might be expected, some of the popular, high-end devices may have recurrent quality or performance problems that will require IT staff attention, either in the form of user training or actual tech work. And quite possibly, some models won't work as advertised.

Organizations must support several types of users. The first step is to sort them out. Those who work in the office and have only occasional outside communication needs can probably get by with a basic phone. Even those models have photo and texting capabilities.

Information workers on the go and field staff who are fully mobile will likely require smartphones or tablets, or both. Workers who require the ability to enter data or file reports may opt for tablets, which at the moment still require add-on applications to function as voice devices.

As departments port or reconfigure mission-related applications to mobile devices, the cost and effort will dictate limiting the choice of device operating systems.

Battery life has emerged as a weakness for some popular smartphones and tablets because of their multiple radio systems (cellular, Wi-Fi and Bluetooth) and high- resolution displays. Careful settings can greatly extend battery life.

The network on which the devices operate becomes an important consideration depending on whether the agency regularly needs international service. Half-duplex, push-

### The Mobile Operating Systems Market

Looking back at some of the mobility also-rans such as one-time leader Palm/Treo, it becomes clear that failure to regularly update the operating system can result in obsolescence. Today, mobile devices all use similar chip architectures, screen and memory technology, and voice/data networks. Ultimately, operating systems and third-party application availability make the difference in device selection.

Four OSs currently dominate the mobile market. In order of market share, they are as follows:

- **Android:** Published as an open source platform by Google, the current version Ice Cream Sandwich will soon be supplanted by Jelly Bean. Key features include a market of about 450,000 apps, sophisticated mapping, voice recognition and smart icons that change to indicate new information.
- **iOS:** As of summer 2012, Apple is preparing Version 6 of its OS for iPhone and iPad devices. The App Store has 650,000 apps for the iPhone, plus 225,000 specifically for the iPad. Version 6 of the OS will add a more thorough mapping application, enhancements to Apple's voice recognition system, call filtering, improved messaging and a secure "wallet" for personal payment information.
- **BlackBerry OS:** Now available in Version 7, Research in Motion has pushed back the release of Version 10 until 2013. BlackBerry is considering licensing the software to other phone makers, following the strategy by which Google pushed Android to first place in market share. But BlackBerry remains a closed-source OS.

  The current version supports a much smaller app market than competitors Android and iOS, but does offer navigational services and integration with social media sites. Many organizations stay with BlackBerry because of its secure, encrypted e-mail forwarding.
- **Windows Phone 7:** Soon to be supplanted by Windows Phone 8, this OS has not caught on to the extent of Android and iOS. Windows Phone takes a different display route, showing larger and more informational "tiles" that reflect what the user is doing or does frequently. Windows 8 will have a competitive iteration of mapping and voice commands. With its renewed push into mobility, Microsoft has for the first time ported its software to the mainstream mobility hardware platform.

to-talk instant service was originally available only on the Integrated Digital Enhanced Network (IDEN) from Nextel. Now organizations can obtain it on a limited number of handsets from carriers on code division multiple access (CDMA) 3G networks.

Whether to go with the competing 3G CDMA or the global system for mobile communications (GSM) depends on coverage areas, how intensively workers will use data downloads and, to some extent, how widely the carrier has introduced 4G LTE coverage. Fourth-generation devices default to the carrier's 3G network (or even 1G) when out of 4G range.

In terms of features, built-in still and video cameras are likely sufficient for recording evidence or gathering visual data. Web browsers, video and music playback capability, GPS and location services come with most smartphones. Law enforcement and national security work may require disabling these features.

Finally, remote management and remote wiping present other sought-after capabilities.

## WLAN and Network Support

Regardless of whether devices are agency-supplied or arrive via BYOD, they will need to be managed by the wireless management system and must conform to the same usage policies that govern notebook and desktop PCs.

Controller-based management and monitoring systems give the network administrator a single portal through which to view wireless LAN (WLAN) activity as part of the greater agency network. A comprehensive package lets the administrator provision and monitor devices remotely, and even wipe them remotely if necessary.

Mobile devices should default to wireless connections when available in nonoffice locations such as depots, fire and police stations, or park and recreation facilities, because when staffers download data over Wi-Fi, it doesn't apply to their data plan. Think of it as a data-rate conservation measure.

Use site surveys to discover gaps in wireless coverage and to determine the version of 802.11 in place at a particular site. Upgrading to the newest 802.11n standard probably means repositioning access points. Operating at different frequencies and with different propagation characteristics, 802.11n may not work optimally if the IT group simply performs one-for-one switch-outs.

802.11ac waits on the horizon. Some manufacturers have already shipped routers that support this new standard for wireless data transfer rates of up to 500 megabits per second (and twice that in multilink WLANs). Endpoint devices with 802.11ac capability will likely hit the market in early 2013, but early adopters may have to settle for 802.11n speeds before agencies go to the expense of retooling their WLAN infrastructures to accommodate the new standard.

### 4G Mobile Public-safety Network in the Works

In spring 2012, the nation's public-safety organizations got a boost from Congress in their quest to modernize communications. Ultimately, state and local jurisdictions hope to benefit from high-speed, interoperable emergency communications using a portion of the 700-megahertz block of spectrum (known as the D-Block) that was once used by broadcasters.

The D-block came by way of the Middle Class Tax Relief and Job Creation Act of 2012. A section of the bill allocated the D-Block specifically to public-safety use. Congress backed up the designation with a $7 billion appropriation for build-out of the network.

Before the president signed the law in late February, a few jurisdictions (such as Harris County, Texas, and Charlotte, N.C.) had already undertaken projects building 4G LTE safety communications networks by operating under a waiver that anticipated eventual disposition of the D-Block.

Some of these jurisdictions had received federal grants from the Broadband Technology Opportunities Program (BTOP), now superseded by the tax law. The federal government has put these projects on hold until the establishment of the First Responder Network Authority, or FirstNet, a new board required by the law.

But according to the Association of Public-Safety Communications Officials, 4G mobile networks have already demonstrated their usefulness to local governments. One carrier deployed 4G LTE in a command station and on mobile devices for a collegiate rowing event in New Jersey, delivering streaming video to roving park rangers.