

# Mobilizing Government

A Primer for Federal Agencies

**WHITE PAPER**

## Summary

Mobile technologies have widespread uses for many federal government agencies. The essential elements that make up these mobile deployments are mobile devices, access to one (or often more) wireless networks, and software which include not only the required job-specific applications but also management and security software.

For the latter functions, the intermittent nature of wireless networks poses unique problems related to reliability and usability which are solved via the use of a mobile VPN. Such a VPN makes the entire deployment practical to manage, handles the security challenges caused by mobile computing use and improves overall productivity and efficiency for both workers and the IT support staff.

## Mobile Computing for Government

More-widespread use of mobile computing and open platforms in the consumer and business realms has led to greater use within the federal government. For military uses, the availability of commercial off-the-shelf products for testing and proving ideas has led to production systems based on those same fundamental technologies, but using ruggedized hardware and private IP-based military and intelligence networks. The following are some of the areas where mobile computing is taking hold.

### Situational Awareness

Situational awareness is a concern in any large scale event that takes place across a broad geography. It applies to both military situations and large-scale emergency-response incidents. Situation awareness involves knowledge of events as they unfold, and understanding them; predicting how they might change over time; and being able to act based on the dynamics of the environment. Mobile computing devices play a role in knowing where assets are located, and gathering and communicating information about relevant events and conditions in the field.

In military applications, mobile computing devices are located in vehicles, or carried by personnel on the ground in some situations (such as control units for unmanned aerial vehicles.) Research has also been underway on equipping individual soldiers with wearable computers. All these mobile devices are potential information-gathering nodes for relaying images, field reports and data to command units.

In civilian use, mobile computers carried by first responders are used in emergency response for communicating information that helps to best marshal the available resources and coordinate the response, in dynamic situations where decisions must be made to minimize the loss of life. Computer-aided dispatch (CAD), geographic information systems (GIS), automatic vehicle location (AVL), records management systems (RMS), weather services, and video camera feeds are all part of the data stream.

### Flight Line Maintenance

Mobile computing for aircraft maintenance has been widely embraced among all branches of the armed services. Technicians carrying mobile computing devices connect with the aircraft systems to download diagnostic and performance data and forward it to the hangar. Technical orders and maintenance manuals are either stored on the laptop and synchronized via wireless connections, or accessed directly from a central server, over-the-air, on-demand. This relieves workers from carrying bulky paper documents. They can also document the procedures performed, order spare parts and check inventory directly from the flight line, making fewer trips back and forth to the hangar.

## **Special Operations**

Coordinating special operations calls for precise communication. Mobile computers in the transport vehicles and devices carried by individuals can be used to access maps, photos, weather data and other essential information, call in air strikes using precise coordinates, and communicate mission status.

## **Command and Control**

On the modern battlefield, networked communications is an integral part of the action. Portable operations centers that can be erected within hours create an ad hoc war room, where commanders use sophisticated multilayer mapping software for tracking movements across varied terrain. Wireless communications via satellite links transmit orders and reports from commanders in the field, allowing them to maneuver anywhere on the battlefield and collaborate with warfighters, command posts and remote analytical centers. Ruggedized laptop computers are deployed in every sort of vehicle, from Humvees to amphibious troop transports to helicopters.

Wireless communications and mobile devices play a corresponding role for civilian responders in large-scale emergencies, such as earthquakes and hurricanes. Under FEMA's direction, portable command centers housed in semi-trailers have been staged at strategic locations around the country for transport to a disaster site for coordinating response. Smaller, more mobile command centers housed in an SUV have been deployed as well. These coordinate the efforts of first responders who carry mobile devices for accessing maps and other data, with uplinks via whatever communication means are available in the aftermath of the event. These can include locally available wireless LANs, cellular networks augmented by portable cell towers when necessary, or satellite links when terrestrial stations are unavailable or inoperable.

## **Mission Planning**

Mission planning for military and intelligence agencies involves a thorough understanding of potential situations and contingencies, calling on geospatial and other data to understand terrain, potential safety hazards, available escape routes, and any elements that might jeopardize or compromise a mission. Since even the most meticulously planned mission is rarely executed exactly as planned, planners must be adaptive. Mobile devices such as ruggedized laptop computers with satellite communications capability provide a platform for accessing up-to-date information and communicating, as circumstances change – whether the variable circumstances were predicted under contingency plans, or are completely unanticipated and call for reinventing strategies on-the-fly.

## **Munitions Management**

Tracking munitions involves more than inventory tracking and logistics, but also knowing the environmental conditions during storage including shock, temperature and humidity which can impact viability. Managing temporary storage in remote locations calls for mobile devices with satellite communication capability. In fixed bases or storage depots, mobility brings the data collection to the data source, improving accuracy by eliminating the error-prone process of transferring information from paper forms. Global visibility of the munitions stockpiles and their condition helps to assure that only serviceable munitions go to the frontlines.

## **Military Police**

Military police operate under the same circumstances as civilian police forces and perform the same essential functions: responding to incidents, identifying suspects, making arrests, and gathering evidence. At many bases they patrol jurisdictions on the scale of a small city, so it is not surprising

that mobile devices used in civilian police work have applications for military policing as well. These devices are used for dispatch, mapping, looking up records and identifying individuals. Vehicle-mounted cameras connected to laptop computers allow military police to document incidents.

## **Border Patrol**

Border patrol agents do line watch using every kind of transportation: four-wheel drive vehicles, ATVs, motorcycles, snowmobiles, bicycles, watercraft, horseback and foot patrols. They work in every kind of environment, from populous border towns and major highway crossings to coastal waterways and remote mountainous terrain. Therefore, their mobile devices need to accommodate multiple types of connections: wireless LANs at checkpoints and outposts, cellular data connections where they are available, and satellite connections in the backcountry.

## **The Elements of a Mobile Deployment**

In mission-critical operations, organization members who rely on mobile devices for information need constant connectivity, especially on the battlefield or in the dynamic conditions of a disaster response. In less immediately urgent situations such as maintenance and routine patrols, constant connections allow workers to stay productive and focused on their jobs, so the organization reaps the full benefit of the investment in mobile technology.

## **Mobile Devices**

Mobile devices are typically notebook or tablet computers, although smart phones or other handheld devices may also figure into the deployment. Leading laptop manufacturers offer ruggedized devices that are protected against shock and impacts, sealed against penetration by dust and moisture, work reliably in extreme climates and meet military specifications. These battle-ready, rugged devices are not only vital for protection against failure when mission success is riding on them, but they also pay for themselves with lower failure rates, incidence of damage and support costs.

## **Wireless Networks**

The US military relies heavily on satellite communications for combat communications. At army bases, shipyards and other fixed facilities, wireless LANs that offer higher bandwidth at relatively lower costs also come into play.

For communication that is sensitive-but-unclassified and especially for border patrol and civilian emergency response, cellular data networks are relied on heavily, augmented with satellite networks. In addition, wireless LANs may be available at fixed locations such as headquarter buildings. In the event of a disaster, cellular carriers have disaster teams that move in with cell-sites-on-wheels units and fleets of vehicles in order to replace communication capabilities that may have been knocked out and to provide extra carrying capacity.

Reliable coverage can be an issue especially in areas with natural and man-made barriers to coverage. Carrier coverage maps based on tower locations do not account for local conditions that can block or impede transmission (e.g. mountainous terrain, tunnels, buildings, etc.). Therefore where cellular networks are the primary form of wireless access, most organizations as a practical matter may combine networks from two or more cellular carriers to get the reliable, blanketed coverage they need.

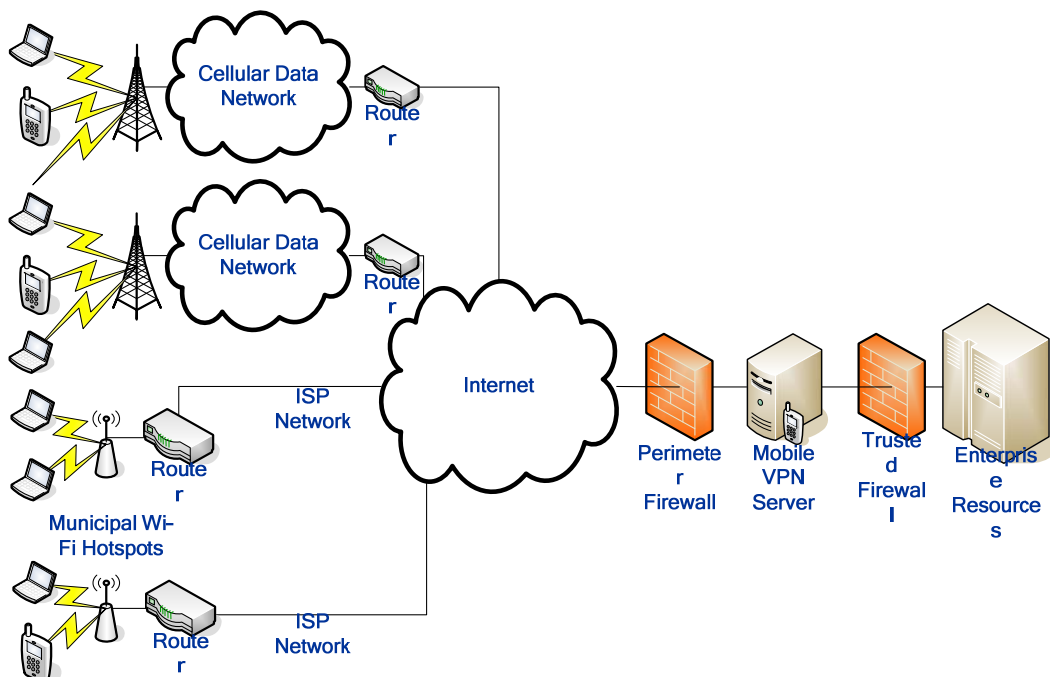
## Software

For standardization, nearly all mobile devices that are used for complex tasks and applications run versions of the Microsoft® Windows® operating system. These devices are tools that workers use in the everyday course of doing their jobs and like any other tool, workers simply expect them to work. They cannot be bothered to update software, tweak network settings, or deal with the minutiae of configuring their devices. If the system is difficult to use, they won't use it. Therefore, as a practical matter there are two additional software packages required for most mobile deployments.

**Systems management software** gives the IT department centralized control and visibility over the installed applications, application versions, configuration, security and status of every mobile device. The larger the deployment, the more essential a remote management system becomes.

**A mobile VPN** is a necessity in a mobile deployment, where workers need applications and connections to be always on, always available. While a conventional VPN handles the vulnerability issues of sensitive or privileged data sent over the public airwaves or the Internet, a mobile VPN goes several steps further. A mobile VPN is a special class of VPN, distinct from IPsec or SSL VPNs, and its defining characteristic is that it maintains a secure tunnel through conditions that would break a conventional VPN. These include going out of coverage range or crossing from one wireless network to another. Whereas an SSL or IPSec VPN cannot manage the vagaries of wireless network connectivity, a mobile VPN is specifically designed for these challenges.

Most organizations that attempt mobile deployments using conventional VPNs or relied on the encryption technologies built into wireless networks, discover the need for a mobile VPN after the fact. Once they implemented a mobile VPN, their networking and device problems disappeared, and support incidents decreased while worker uptime increased.



*Mobile devices communicate via multiple cellular data networks, Wi-Fi hotspots or satellite uplinks in the field, to connect to departmental resources. A mobile VPN secures the connection end-to-end and maintains reliable connections as each device moves between the various networks.*

## The Unseen Challenge: Seamless Connectivity

A mobile VPN solves the single, most vexing problem impacting mobile deployments: maintaining application and user log-in sessions. Continuous connectivity is not always present in a wireless environment. Users may move behind a mountain or into a valley, enter the belly of an aircraft, or simply roam out of range. When users lose their connections, sessions drop, applications often crash, and users have to re-authenticate to the network.

All too often, these problems don't become evident until after an organization has deployed a system, or added applications that aren't mobile-aware. Especially unfortunate, organizations often live with the problems, accepting decreased functionality and productivity because they are unaware that implementing a mobile VPN can solve the problems, quickly and efficiently.

Common connectivity issues include:

### Coverage Gaps

Nearly all cellular networks have local "dead zones". When workers go out of range or behind an obstacle, they lose their connections. When they have to re-login or re-enter the data they lost, at the very least it impacts productivity. In military, policing or disaster-response scenarios, an inability to connect or an abruptly lost connection can be life-threatening.

A mobile VPN is able to maintain a virtual connection to the application, even though the actual connection may be lost. It also preserves the state of the application, even in the middle of a data transmission, by holding the unsent or pending data in queue. The session simply resumes when the connection is available again.

### Use of Multiple Networks

When crossing a network boundary, users need to log in to each new network to authenticate. They may cross these boundaries dozens or hundreds of times a day. Even applications written specifically for mobile environments cannot handle crossing of network boundaries, and require users to re-authenticate.

A mobile VPN handles multiple networks by maintaining a virtual IP address for each device. As the device encounters a new network, it authenticates to the new network, transparently to the user, and receives a local IP address from the network's DHCP server. The mobile VPN maps the virtual IP address to the local IP address so that even as the local IP address changes, the deployment operates as if it were a single network.

### Suspend/Resume Cycles

For devices running on battery power, suspending a device puts it in a lower-power state. This may be required so the device makes it through a work shift on a single charge. Typically, suspending cuts power to the wireless system, breaking the connection.

A mobile VPN preserves the virtual connection through a suspend-and-resume event.

### Application Reliability

Virtually all off-the-shelf applications, except for those written quite specifically for a mobile environment, assume a permanent network connection. If the connection disappears in the middle of a network operation, the application typically can't re-establish access and crashes. Since many applications perform network operations in the background, at undefined intervals, the user doesn't even have to be actively using the application. And yet, an application failure can occur requiring re-

logging in and retyping any lost data. These application crashes are most often the greatest source of user frustration in a typical mobile deployment. And solving them is considered one of the most important, most welcome attributes of a mobile VPN.

## Support Concerns and User Acceptance

Agencies that have deployed a mobile solution without using a mobile VPN know that sporadic coverage and crashes result in chronic reliability problems, frustrate users and trigger a high number of calls to the help desk.

Technology that makes the worker's mission easier will be accepted. Technology that gets in their way won't. A mobile VPN does its work in the background, handling logins and the complexities of roaming between networks while maintaining applications through coverage gaps. To users, it appears they are constantly connected to a single, seamless network.

## Managing a Mobile Deployment

Mobile devices may be used hundreds of miles away from a data center, on unseen networks, far out of reach of IT personnel. This leads to management challenges far beyond those encountered with fixed machines on a wired network.

### Visibility

The total value of a mobile deployment represents a major investment of taxpayer dollars and with it comes a responsibility to ensure resources are used wisely. While a mobile VPN typically is a fraction of the total deployment cost, it allows use of the entire system to be centrally configured, managed, and observed. A mobile VPN with analytics capability goes a step further, furnishing reports that reveal patterns of use, how devices and networks are being employed, and how they might be used more wisely.

### Control

Managing even a handful of remote devices can be a chore. In a large deployment with hundreds or thousands of devices it can be impossible without an automated solution. A mobile VPN with a central console makes it easy to quarantine devices that are misused, lost or stolen. Policy management capability allows administrators to dictate how devices and applications use the networks, to maximize productivity. And policies may be assigned to individual users or groups of users, affording flexible, streamlined control with permissions based on job function or organizational role.

Ideally, these policies are stored on the VPN server, rather than on the mobile device, and pushed down automatically to the device where they are enforced. A well-defined set of policies locks down a device tightly, which prevents users from tinkering with settings that might override essential security or impair the functionality of the device.

### System Management

A large mobile deployment may include hundreds or thousands of individual mobile devices. Tasks such as operating system upgrades, software rollouts, driver changes, updates and configuration changes which are simple in a small LAN environment are incredibly complex in a mobile deployment where devices are constantly on the move.

System management includes:

- Staging of new devices or those returned from the service center

- Standardizing software versions and configurations within and across various types of users
- Pushing out application updates, device refreshes, and security and network settings with minimal impact or interruption to the user

While system management in LAN environments is a mature industry, mobile environments pose additional challenges surrounding roaming, intermittent connectivity and variable bandwidth. A management system especially designed for a mobile environment, tightly coupled with a mobile VPN that is “connection and bandwidth-aware,” presents an ideal solution for large government deployments.

## Monitoring

With workers far removed from IT resources, any problem with a device or network takes much longer to correct, possibly resulting in a dramatic loss of productive hours. A mobile VPN with proactive monitoring capabilities not only detects active problems, but when problems might be imminent. This includes problems with networks, or with a device itself such as a battery that might be failing.

## Fault Isolation and Resolution

In a mobile deployment, access points may be at remote locations. Or, in the case of cellular data networks, entire pieces of the delivery network are outside of IT control. Knowing when a problem might exist at a Wi-Fi access point, within a cellular network, or with the device itself can be problematic. A mobile VPN with a reporting and analytics capability can quickly evaluate connectivity problems across networks and isolate an individual device, network, user or time of day, detecting root causes that otherwise might take hours of sleuthing at the device level.

## Bandwidth Management

Data access contracts with cellular carriers represent a sizable investment of public funds that must be used wisely. A mobile VPN that uses application-proxy technology is able to examine the complete traffic flow and how users, devices and applications use bandwidth across each cellular network. Developing reports on these areas allows administrators to understand when:

- Total bandwidth use is approaching the contracted limit and agreements may need to be renegotiated
- Data-intensive applications (such as streaming media over Web browsers) might be wasting a public resource
- Non-essential applications are being used
- Large file transfers are running over a cellular network that could be more cost-effectively handled over a wired or Wi-Fi connection

## Worker Productivity

An application-proxy mobile VPN can also proactively ensure that individual users and devices use applications and networks properly. Policy management capabilities afford extremely effective control over user and device behavior, with granular control by application, port and IP address over various networks. This ensures proper use of mobile devices which are not personal devices, but a public resource. And even workers who are using their devices as intended can accidentally launch a process, such as initiating an anti-virus signature download or running Windows updates, over a cellular data connection which can bog down their device for many minutes.

## Authentication

Ensuring that users are authorized is a key concern for any network manager, but this situation is of greater concern in a mobile deployment where devices carry sensitive information and are prone to be misplaced, lost or stolen. Law enforcement agencies including the border patrol face stringent requirements for strong two-factor authentication, which is required to access federal criminal databases.

A mobile VPN ensures users are authorized by enforcing secure logins using either its own native directory, or integration with an enterprise directory. Proactive notification capabilities alert administrators when a device has exceeded the number of allowed login attempts, indicating it may have been stolen, with centralized controls that quarantine the device so it cannot be used to access sensitive applications and data. Allowances for smart cards, RSA SecurID, digital certificates, biometric scanners and other two-factor authentication methods add the strong authentication required by federal mandates.

## End-to-End Security

Wireless networks use the public airwaves which clearly poses security risks. And while Wi-Fi and cellular networks offer their own security technologies, some have known vulnerabilities. In addition, any portion of the route that runs over the wired, public Internet remains unencrypted. A mobile VPN creates a secure end-to-end tunnel that encrypts the complete data session from the data center to the wireless device.

In addition, mobile VPNs may also offer Network-Access Control (NAC) capabilities that help protect both the individual device and host network against viruses and spyware. It accomplishes this by verifying that security measures are active, enabled and up-to-date, and that the device has all necessary security patches as specified by the organization's security policy. Some solutions can even remediate the device automatically, without requiring any user intervention. This protects the device and guards against lost productivity, since some malware can severely degrade device performance or burden the network with malicious traffic.

## The Challenges of Mobile Deployments and the Role of a Mobile VPN

	Challenge	Solution
<b>Security</b>		
Data security	Safety of data from compromise as it traverses airwaves and the public Internet	Highest-standard FIPS 140-2 validated AES encryption secures data sessions as devices traverse networks
Device health	Protection of individual devices against viruses, spyware and other malware that can expose data	Network Access Control verifies that every device is compliant with organizational security standards before allowing a connection
Device loss or theft	Devices that are constantly in motion, and prone to being misplaced, forgotten or left unguarded	Central controls make it easy to quarantine devices that are misused, lost or stolen
Compliance	Complying with specific security standards, as required by government mandates	Support for strong authentication meets security policy requirements
<b>Productivity</b>		
Intermittent connectivity	Application crashes and/or repeat logins as workers cross network boundaries, go out of range, or suspend-and-resume devices	Mobile-aware VPN handles complexities of dealing with coverage gaps and roaming between networks, so workers can focus on their essential mission
Variable bandwidth	Data-intensive processes running over slower networks, bogging down device performance	Policies control device and application behavior, and keep data-intensive processes off slower networks.
Multiple networks	Isolating users from complexities of managing devices on multiple networks	Devices automatically use fastest available connection and log in automatically when roaming between departmental Wi-Fi hotspots and multiple cellular data networks
Web performance	Slow performance and page refreshes when using Web applications over cellular networks	Compression and optimization techniques improve throughput and application responsiveness
<b>Management</b>		
Bandwidth usage control	Ensuring intelligent use of a public resource, especially contracted cellular networks	Analytics capability reports on all aspects of user, device and application use, over all networks
Control and visibility	Effective, efficient management of hundreds or thousands of devices deployed in the field	Browser-based administrative console allows all aspects of the system to be centrally configured, managed and observed
User issues	Technically unsophisticated users	User-proof design is transparent, extends centralized control over configuration and minimizes trouble tickets
Troubleshooting	Fault isolation for mobile devices using multiple networks	Reports with drill-down capability uncover problems related to various data networks, time of day or other patterns of use
Monitoring	Need to continuously monitor or “babysit” the deployment	Automated notifications promote hands-off management, including pre-emptive detection of conditions that indicate failure might be imminent

## Reliability to Go: NetMotion Mobility XE Mobile VPN

NetMotion Mobility XE is an award-winning mobile VPN that presents an elegant, single solution to all of the challenges of mobile deployments. NetMotion Mobility XE:

- Keeps application sessions alive to prevent crashes as users encounter no-coverage zones, suspend and resume their devices or cross network boundaries
- Allows applications that were not written specifically with mobile deployments in mind to be used successfully in a mobile environment
- Automatically handles logins on behalf of the user, as well as the technical complexities of configuring for each connection as devices switch between networks
- Authenticates each user, through Mobility XE's own user database or integration with Windows Active Directory
- Supports strong "two-factor" authentication for higher security
- Encrypts all the data transmitted to protect against compromise, using the AES (Advanced Encryption Standard) for the United States
- Ensures that devices have patches that are up-to-date, as well as properly configured, active and updated antivirus and antispyware protection
- Enforces proper bandwidth use by making sure that large data transfers stay off of slower networks, and that mobile computing resources are used appropriately
- Delivers intelligence on the usage and behavior of individuals, devices, applications and networks, to drive higher productivity, monitor use of public resources and fine-tune the deployment
- Does all of the above in way that is essentially invisible to the user, improves productivity, and is highly resistant to user missteps that might impair the functionality of the device

### For More Information

To learn more, visit [www.netmotionwireless.com](http://www.netmotionwireless.com) for case studies detailing various uses of the NetMotion Mobility XE mobile VPN in government, and white papers that explain specific aspects of Mobility XE in depth including security, policy management, network access control and analytics.

© 2011 NetMotion Wireless, Inc. All rights reserved. NetMotion and NetMotion Mobility are registered trademarks, and Mobility XE, Roamable IPsec, InterNetwork Roaming, Best-Bandwidth Routing and Analytics Module are trademarks of NetMotion Wireless, Inc. Microsoft, Microsoft Windows, Active Directory, ActiveSync, Internet Explorer, Windows Mobile, Windows Server, Windows XP, SQL Server, Windows XP Tablet PC Edition and Windows Vista are registered trademarks of Microsoft Corporation. All other trademarks, trade names or company names referenced herein are used for identification purposes only and are the property of their respective owners. NetMotion Wireless technology is protected by one or more of the following US Patents: 5,717,737; 6,198,920; 6,418,324; 6,546,425; 6,826,405; 6,981,047; 7,136,645; 7,293,107; 7,574,208; 7,602,782; 7,644,171; 7,778,260 and Canadian Patent 2,303,987. Other US and foreign patents pending.