ONLINE REPORT
SPONSORED BY:

verizon

SPECIAL REPORT

SUCCESSFUL MOBILE STRATEGIES

INSIDE

DEFENSE MOBILITY POLICY: SLOW AND STEADY WINS THE RACE P2

RIDING THE WIRELESS WAVE P4

THERE'S AN APP FOR THAT P5

IMPROVING TELEWORK ADOPTION P6

MOBILITY: A MOVING TARGET P7

DEFENSE MOBILITY POLICY: SLOW AND STEADY WINS THE RACE

Over the past several years, there has been a lot of progress in sorting out what mobile devices and applications defense personnel can use and what constitutes a truly secure wireless infrastructure. Yet there is still more work to be done.

The first major step toward a true mobility policy came in 2012 with the Department of Defense Mobile Strategy. In that document, DOD CIO Teresa M. Takai laid out the department's IT goals and objectives related to wireless security, mobile device management and mobile and web-enabled apps. The document was followed a year later by an update that described a commercial mobile device implementation plan to allow secure classified and protected unclassified mobile solutions that use commercially available products.

Since that time, DOD has slowly but surely made progress. DISA is now the managing organization for mobility, charged with overseeing applications, approving devices, and making sure security is always front and center. DISA's strategic plan lays this out in some detail, focusing on how it will improve mobile networks through better security.

Earlier this year, DISA also introduced an unclassified mobility capability that will provide defense employees with access to a larger range of mobile devices, applications and services. On the application front, it continues to improve the DOD Mobile App store, which currently supports about 100,000 users and nearly 2,000 unclassified mobile devices.

A work in progress

Despite the progress that has been made up to this point, there are still a lot of issues to work out. For example, today, many defense agencies have their own mobility pilots and in some cases, their own mobility policies. Since that's the case, will there eventually be one comprehensive defense mobility policy? Where does the mobility guidance from the National Institute of Standards and Technology (NIST), Office of Management and Budget, NSA and the Department of Homeland Security fit in? What about Bring Your Own Device (BYOD)? Will there be an overall federal mobility policy that DOD will adapt for its own use?

Alan Webber, research director of innovation and transformation at IDC Government, believes that the mobility policy situation will shake out from the top down—with an overall federal government mobility policy as the model. From there, DOD can narrow and tighten the policy to suit its needs and if necessary, defense agencies can fine-tune it further. Webber believes an overall federal mobility policy will exist within three years.

Once that happens, the DOD still has to fine-tune government mobility policy to fit its needs, both in terms of application management and device management. While DISA has developed a functioning mobile application store that distributes applications to mobile devices for qualified defense personnel, there are still questions around management and security. For example, if an app is determined to have a vulnerability, what is the process of clearing the update and getting it back in the app store quickly? If it's just an update to the user interface, does it go through the same process? And how should the DOD control the code?

Device management also is a tough nut for the DOD to crack. At the moment, NSA is working on policy to determine what devices are acceptable for classified use and which are useful to unclassified use. It's complicated, Webber explained, because a device that DOD might consider non-classified might be

considered classified by DHS. There has been progress in other areas of device management, however. Many devices are working their way through the current unclassified device process, as is Windows 8. DOD's mobile device management (MDM) strategy also is solidifying, although more work has to be done in the areas of security and manageability. According to Takai's statements at February's MobileGov Summit, remaining challenges include developing policies and procedures for identity management and developing a standard configuration for the mobile devices it buys from industry, including which apps can be preloaded on devices.

While many say BYOD will never happen in DOD, others believe it will, at least in some form. It may take the form of personnel being able to choose from a list of approved devices rather than using anything they want, however. Takai herself has said that BYOD is a long-term objective.

"Right now, all of this is like stone soup—everyone is trying to do a piece of it," Webber said. "But they will get there."

RIDING THE WIRELESS WAVE

As wireless networks have become part of the fabric of government business, agencies are discovering more uses for wireless technology. Not only has the adoption of mobile devices throughout government increased the use of government WiFi networks, but video traffic, Voice over Wireless (Vo-Fi), rapid file transfer and even wireless Machine to Machine (M2M) data connections all require faster connections and greater capacity.

Until recently, the state-of-the-art wireless standard was 802.11n, a significant improvement over the original standard, which offered 1-to-2 megabits per second throughput. 802.11n's throughput is 300 Mbps to 450 Mbps. But with wireless networks strained to capacity, the need for much faster throughput and better range and reception is critical for government networks. 802.11ac, introduced in 2013, is as much as three times faster than 802.11n. It operates in the 5 GHz spectrum instead of the 2.4 GHz spectrum, which tends to have less interference from other WiFi networks in the area. It is backwards-compatible with not only 802.11n, but 802.11b and g.

It makes sense to upgrade now versus later; not only does a move to 802.11ac future-proof the WiFi network for further advances, but it lets agencies take advantage of the additional speed and capacity now. According to ABI Research, more new mobile handsets will incorporate 802.11ac than 802.11n by early 2015.

By the end of 2014, the next wave of 802.11ac—called "Wave 2"—will be released. Wave 2 is expected to have throughput of up to nearly 1.9 Gbps and a new feature, called multi-user MIMO, will let multiple devices access separate data streams simultaneously from one access point.

Within three or four years, expect yet another leap forward with 802.11ax, which will improve on MIMO by using frequency-division multiplexing to separate dozens or even hundreds of smaller substreams, each with different frequencies, to increase the spectral efficiency and maximum throughput of each stream. Early predictions put speeds at more than 10 Gbps of data speed in the 5 GHz band. 802.11ax could be particularly useful in increasing throughput in densely populated areas or areas of dense WiFi concentration.

Different WiFi versions for different needs

While speed and capacity for mainstream WiFi applications keep improving, there are other WiFi standards either already available or coming soon that improve speed and capacity for specific use cases. For example, 802.11ad, also known as WiGig, is aimed at helping intelligent devices with direct line of site to each other through a lightning-fast WiFi network in the 60 GHz range. With speeds of up to 7 Gbps, WiGig is optimal for applications like wireless storage, wireless docking and edge caching (the ability to distribute content from a local web server to caching servers that are closer to the end user). Adoption of WiGig is poised for huge growth; according to a report from MarketsandMarkets, the WiGig market is expected to grow at a compound annual growth rate (CAGR) of more than 111 percent from 2014 to 2019.

For agencies that use sensors for functions like intelligence, surveillance, healthcare, data center management, smart street lights and smart meters, the upcoming 802.11ah standard will improve transmission speed and range. Set to debut around 2016, 802.11h will use 900 MHz spectrum to provide a throughput of 150 kbps to 40 Mbhs, making it ideal for long-range communications that can use low power, such as sensor networks, M2M communications, and backhaul networks for sensors.

THERE'S AN APP FOR THAT

When federal employees need to coordinate a meeting, they no longer have to pick up the phone to make a call. Instead, they can access an app on their mobile devices that can share their calendar with team members, coordinate schedules and send reminders. The app even allows users to attach files or documents to the event so everyone has the same material.

More and more, agencies are providing employees with a host of mobile apps that increase productivity and improve collaboration. These productivity apps—mostly commercially available apps fine-tuned for government use—are helping out-of-the-office workers keep on task and remain productive using the mobile device of their choice.

Agencies are also working hard to increase the number of mission-critical apps available to employees. Some are already available. DISA's DOD Application Store has a few dozen apps available for use, with more coming. For example, service members dealing with sexual assault can use DOD Safe Helpline, a crisis support app, to get immediate help. Residents of Scott Air Force Base can use MyMC2 to keep up to date with services and events, and defense employees now have an app for using common access card (CAC) readers with mobile devices. Many others are on the way; the Army is working on readying mobile apps for supply chain management that eventually will be rolled out to all of DOD. The apps will help track the whereabouts of all military gear.

The possibilities are virtually limitless. Apps that take advantage of GPS for tracking and positioning could help in the areas of intelligence, defense, border control, inspections and emergency response, for example.

Why, then, is it taking so long for the government to be flooded with apps? There have been many audits of how agencies are both acquiring commercial apps and developing their own, and all have come to the same basic conclusion: they often don't adequately address potential risks, and some use too much bandwidth or other government resources.

Part of the problem is that individual agencies have their own app approval processes, so there is no overall authority or standardization. Many believe that has to change.

Paving the way for more government apps

Federal agencies are taking serious steps to resolve these issues. NIST earlier this year introduced AppVet, a free web-based application that allows agencies to submit and test apps for risk and security issues. The system also analyzes the app to ensure that it conforms to the requirements of the submitting organization.

DigitalGov, run by GSA's Office of Citizen Services and Innovative Technologies, has a free testing service agencies can use to validate that the app is functioning properly on all relevant devices. Volunteer federal app testers evaluate the apps and provide agencies with results they can use to improve apps' usefulness.

The Defense Department has its own system. DISA, the lead agency for mobile apps, requires apps to be submitted to its Mobility Application Validation process. Apps undergo capability testing as well as risk and security assessments before being approved and made available for download.

Another interesting offering is DHS's Mobile Carwash, an offshoot of the Carwash program centered on improving the building, testing and deployment of mobile apps. Agencies that subscribe can access a shared code repository and use an automated orchestration tool to build, test and publish apps. Carwash also provides users with a variety of scans and tests, as well as an issue and risk tracking system.

The number and type of mobile apps for federal employees will continue to grow, especially as standardization and oversight mature. The work on that front continues; in August, the Department of Homeland Security announced intentions to develop a "Seal of Approval" program for apps that can be used by all government agencies. The idea is to create a process similar to how FedRAMP approves cloud-based solutions for government.

IMPROVING TELEWORK ADOPTION

Telework has become more popular throughout government, thanks to widespread initiatives and an understanding that it boosts productivity, improves collaboration, reduces costs, and improves work/life balance and job satisfaction. According to a report from Global Workplace Analytics, telework currently saves the federal government more than $6 billion per year, reduces absenteeism by 31percent and increases productivity by 13 percent.

Yet for many agencies, adoption is still relatively low. According to the Global Workplace Analytics study, only about one-third of federal employees eligible for telework take advantage of it.

There are many reasons why telework hasn't taken off more strongly in government. According to Mobile Work Exchange, the top reason is security; 47percent have concerns about the security of telework arrangements. Second on the list is available funding, followed by culture. Other reasons include lack of training and slow development of mobility policies.

Conquering obstacles

Improving the adoption of telework can help agencies reach the productivity, cost and satisfaction goals that robust telework programs can provide.

Security: While it's understandable that security would be a top concern, telework can actually be as safe as or safer than traditional work structures if it is set up properly. That means addressing every aspect of data security, from paper files and storage devices to removable media and telecommunications equipment. It also means ensuring that government data is fully separate from personal property and information. OPM's 2013 Status of Telework report found that agencies use a variety of methods to secure Personally Identifiable Information, for example:

- Encryption and/or password protection
- Two-factor authentication used for remote access
- Privileged Rules of Behavior are signed for those handling PII
- Only those with a compelling need are allowed to download PII
- Only government-furnished equipment is allowed for telework
- No PII, sensitive or classified information can be physically removed from the agency facility
- No PII, sensitive or classified information can be transmitted electronically from the agency facility

Culture: Culture change is tough, especially when baby boomers are managing millennials. Millennials are the future of government, and they expect to be able to work wherever they want, from whatever device they want, at any time. That means that managers must accept telework. That requires substantial training for managers in how to manage remotely, handle employee concerns, implement change and ensure compliance with processes, rules and regulations related to telework.

Training: In addition to managerial training, teleworking employees also must be trained on how to remain productive from remote locations, how to work on a distributed team, effective communication, and workload management. They should also be trained in the technology they will use to work and collaborate, such as video conferencing, virtual collaboration and remote file access.

While these challenges are difficult, there is progress being made. In August, the Office of Personnel Management issued a memorandum on enhancing workplace flexibilities and work-life programs, designed to encourage more telework throughout the federal government. The memo explains employees' rights to request work schedule flexibility without fear of retaliation, among other issues. OPM plans to issue further guidance to help further adoption of telework and other programs that increase work-life balance for federal employees.

MOBILITY: A MOVING TARGET

As mobility becomes more and more entrenched in the culture of government, the push is on to make it as safe, user-friendly and widespread as possible. Agencies at every level of government are making progress on all of these fronts, surely and steadily.

Security is at the top of the list. While agencies have made great strides in improving mobile security, the push continues. Last year, a group of 46 federal technologists known as the Mobile Technology Tiger Team developed the Federal Mobile Security Baseline, which gives agencies and departments a set of instructions for assessing risk and improving mobile security.

Another important trend is the concept of the personal mobile workplace, an idea that Gartner identified as one of its Top 10 strategic technology trends for smart government. The idea is that whether a mobile device is agency-issued or employee-owned, the use of mobile devices in the government workplace is inevitable. According to a recent survey by the Mobile Work Exchange, 90 percent of government employees today use at least one mobile device for work purposes. The use of mobile devices in government means that agencies have no choice but to develop policies for allowing and managing these devices that aligns with internal security policies, yet provides employees with enough privacy.

Agencies also are working to improve the user experience, whether that user is a government employee or a citizen. By creating more engaging user experiences and improving usability, agencies hope to increase user acceptance of mobile apps across the board. To help agencies get on the right track, GSA's Office of Citizen Services and Innovative Technologies, in concert with more than 100 participants from 35 federal agencies, states, the private sector, and academia, developed a list of 42 guidelines. These included using plain language, providing user-centered content, optimizing apps for performance, providing well-organized content to create increased feelings of trust and making content easy to share.

Sharing is another major mobility trend. GSA is leading the charge with Mobile Code Catalog, which allows federal agencies to share code to make mobile development easier. The site includes sharable frameworks and modular code for HTML/CSS/JS, ColdFusion, Ruby, Python and JSP, as well as modular code and complete apps for Android, Blackberry, iOS and .Net/Windows. Other resources include test scripts, a Federal App Catalog, federal APIs and a link to the Mobile App Development Program.

Agencies at all levels of government also continue to increase citizen engagement through better mobility. Another one of Gartner's Top 10 strategic technology trends for smart government, mobile citizen engagement is widely considered to be the best way to deliver services, disseminate information and contribute to citizen satisfaction with government. One way governments are improving mobile citizen engagement is by developing user-friendly, citizen-facing apps.

On the federal side, agencies are motivated to develop more citizen-facing apps to comply with the Digital Government Strategy, which requires it. Apps run the gamut, from financial, business and education to health and fitness, medical, news, reference and travel. State and local governments are even more invested, with hundreds of apps for everything from traffic management to first aid.

Coming soon to an agency near you

As exciting as these trends are, advances in technology promise to make the future of mobility in government even more interesting. One of the most exciting areas of focus is wearable technology—an area that IDC Government says will improve smart mobile government.

First responders and soldiers are the most obvious

recipients of wearable gear. For example, DARPA's Warrior Web program is working with Harvard University to develop a lightweight suit to be worn under uniforms to protect parts of the body prone to injury. The suit, which would include sensors that could measure health signs, also could be constructed to allow soldiers to carry heavier loads by making them feel lighter. State and local governments could use similar technology to outfit first responders with wearable, voice-activated, hands-free devices for transmitting and receiving critical voice, video and data information. The devices would be GPS-enabled and have integrated sensors to monitor video, heart rate and external and internal temperatures.

There is a lot of potential for wearable technology in other areas as well. For example, wristbands for emergency signaling and health monitoring or wearable devices to improve worker productivity by keeping people on task may be on the way. Another area ripe for development is using visual devices such as Google Glass for situational awareness. DARPA is working on something similar through its Urban Leader Tactical Response, Awareness & Visualization (ULTRA-VIS) program, which already has a prototype of a tactical augmented reality system that would allow soldiers in the field to see the location of other forces, vehicles, hazards and aircraft in holographic form through a visual display. •