Bring Your Own Device

A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs
August 23, 2012

Product of the Digital Services Advisory Group and Federal Chief Information Officers Council

Contents

Introduction

The Digital Government Strategy (the Strategy) (PDF/HTML), issued by Federal Chief Information Officer (CIO) Steven VanRoekel on May 23, 2012, called for the establishment of a Digital Services Advisory Group (Advisory Group) to promote cross-agency sharing and accelerated adoption of mobile workforce solutions and best practices in the development and delivery of digital services. Milestone Action #3.3 of the Strategy requires the Advisory Group to work with the Federal CIO Council (CIOC) to develop government-wide bring-your-own-device (BYOD)[1] guidance based on lessons learned from successful BYOD programs launched at forward-leaning agencies. Through the BYOD Working Group, the Advisory Group and CIOC produced this document to fulfill the requirements of Milestone Action #3.3.

Implementing a BYOD program is not mandatory. This document is intended to serve as a toolkit for agencies contemplating implementation of BYOD programs. The toolkit is not meant to be comprehensive, but rather provides key areas for consideration and examples of existing policies and best practices. In addition to providing an overview of considerations for implementing BYOD, the BYOD Working Group members developed a small collection of case studies to highlight the successful efforts of BYOD pilots or programs at several government agencies. The Working Group also assembled examples of existing policies to help inform IT leaders who are planning to develop BYOD programs for their organizations.

Future Digital Government Strategy deliverables, such as the Mobile Security Reference Architecture encompassed in Milestone Action #9.1, will help inform agency considerations on BYOD. The National Institute of Standards and Technology (NIST) is also drafting several standards and guidelines focused on mobility, including: Guidelines for Managing and Securing Mobile Devices in the Enterprise[2]; Security and Privacy Controls for Federal Information Systems and Organizations; and Personal Identity Verification (PIV) of Federal Employees and Contractors. Each of these documents should provide further insight into issues associated with the implementation of BYOD solutions.

While the case studies and example policies that the BYOD Working Group has assembled are a great starting point for agencies considering BYOD programs, this work is not finished. The Federal Government still has more to do to address the more complicated issues related to BYOD. This includes how the government can reimburse Federal employees for voice/data costs incurred when they use their personal mobile devices instead of government-issued mobile devices, and additional security, privacy, and legal considerations including supply chain risk management and legal discovery.

Key Considerations

The implementation of BYOD needs to be an iterative process – support of BYOD for commodity enterprise technologies like email and collaboration systems can lay the foundation for expanding to more diverse, mission-specific applications and a broader scope of enterprise offerings. BYOD can be facilitated through applications native to the device, downloaded or installable applications, or even a web browser. The private and public sector entities who have adopted BYOD solutions report that allowing employees to use their personal mobile devices to access company resources often results in increased employee productivity and job satisfaction. From the Federal information security perspective, devices must be configured and managed with information assurance controls commensurate with the sensitivity of the

underlying data as part of an overall risk management framework.

The BYOD Working Group observed additional characteristics about this growing trend:

- BYOD is about offering choice to customers. By embracing the consumerization of Information Technology (IT), the government can address the personal preferences of its employees, offering them increased mobility and better integration of their personal and work lives. It also enables employees the flexibility to work in a way that optimizes their productivity.
- BYOD can and should be cost-effective, so a cost-benefit analysis is essential as the policy is deployed. Such a cost-benefit analysis should take into account both potential increases in employee productivity and potential cost shifts. For example, providing employees access to government services on their personal devices should help reduce the number of government devices that are provided to staff as well as the life-cycle asset management costs associated with these devices. BYOD programs may, however, necessitate government reimbursement for voice/data costs incurred when employees use their personal mobile devices instead of government-issued mobile devices and additional enterprise infrastructure costs in handling the support of BYOD users. Additionally, overall costs may significantly increase for personnel who frequently communicate outside of the coverage area of their primary service provider and incur roaming charges.
- Implementation of a BYOD program presents agencies with a myriad of security, policy, technical, and legal challenges not only to internal communications, but also to relationships and trust with business and government partners. The magnitude of the issues is a function of both the sensitivity of the underlying data and the amount of processing and data storage allowed on the personal device based on the technical approach adopted. Generally speaking, there are three high-level means of implementing a BYOD program:
  - Virtualization: Provide remote access to computing resources so that no data or corporate application processing is stored or conducted on the personal device;
  - Walled garden: Contain data or corporate application processing within a secure application on the personal device so that it is segregated from personal data;
  - Limited separation: Allow comingled corporate and personal data and/or application processing on the personal device with policies enacted to ensure minimum security controls are still satisfied.

The growing trend of BYOD demonstrates that we as IT leaders have changed how we adopt technology. Gone are the days of long projects that address every demand. We must now integrate new technologies in a rapid, iterative, agile, interoperable, and secure method to meet changing market and customer needs. Device agnosticism is more important than ever. Our software, hardware, and applications must be compatible across common systems and personal devices. Our information security controls must also be consistent with existing law and standards to ensure confidentiality, integrity, and availability.[3] Because of these and other considerations, BYOD is not necessarily a good fit for all government agencies – it has to fit the agency's environment, support mission requirements, and meet the specific needs of staff.

The business case for implementing BYOD programs vary from agency to agency, but often involve the following drivers: to reduce costs, increase program productivity and effectiveness, adapt to a changing workforce, and improve user experience. Below is a list of points to consider when determining whether a BYOD program is right for your agency and its staff. The list, which is by no means exhaustive, includes policy and process considerations for Chief Information Officers, Chief Technology Officers, Chief Information Security Officers, Chief Human Capital Officers, Chief Financial Officers, Chief Acquisition Officers, and others.

- Technical approach
  - Virtualization
  - Walled garden
  - Limited separation
- Roles and responsibilities
  - Agency
  - User
  - Help/service desk(s)
  - Carrier technical support
- Incentives for government and individuals
  - Survey employees on benefits and challenges
  - Consider voluntary vs. mandatory participation in BYOD program and impact on terms of service
- Education, use, and operation
  - Establish orientation, trainings, and user agreements
  - Establish associated policies collaboratively with union representative
  - Ensure compliance with Fair Labor Standards Act (FLSA) requirements (e.g., institute policies to ensure non-exempt employees do not conduct work after-hours unless directly authorized/instructed)
  - Consider impact of connectivity and data plan needs for of chosen technical approach (e.g., virtualization) on employee reimbursement
  - Implement telework agreements consistent with the Telework Enhancement Act and OMB implementation requirements
- Security
  - Assess and document risks in:
    - Information security (operating system compromise due to malware, device misuse, and information spillover risks)
    - Operations security (personal devices may divulge information about a user when conducting specific activities in certain environments)
    - Transmission security (protections to mitigate transmission interception)
  - Ensure consistency with government-wide standards for processing and storing Federal information
  - Assess data security with BYOD versus the devices being replaced
  - Securely architect systems for interoperability (government data vs. personal data)
- Privacy
  - Identify the right balance between personal privacy and organizational security
  - Document process for employee to safeguard personal data if / when government wipes the device
- Ethics / legal questions
  - Define "acceptable use" from both government and individual perspective
  - Address legal discovery (including confiscation rights) and liability issues (e.g., through pre-defined opt-in requirements in terms of service)
  - Consider implications for equal rights employment (e.g., disparity in quality of personal devices)

- Service provider(s)
  - Identify companies that could offer discounts to government employees
  - Assess opportunities to leverage the Federal Strategic Sourcing Initiative
  - Assess tax implications for reimbursement
- Devices and applications (apps)
  - Identify permitted and supported devices to prevent introduction of malicious hardware and firmware
  - Define content applications that are required, allowed, or banned and consider use of mobile device management (MDM) and mobile application management (MAM) enterprise systems to enforce policies[4]
  - Adopt existing app development best practices to support device-agnosticism and data portability across platforms
  - Address app compatibility issues (e.g., accidental sharing of sensitive information due to differences in information display between platforms)
  - Recommend approach to content storage (cloud vs. device)
  - Clarify ownership of the apps and data
- Asset management
  - Disposal of device if replaced, lost, stolen, or sold, or employment is terminated (must remove government information before disposal)
  - Reporting and tracking lost / stolen personal devices
  - Replacement of personal lost devices if employee chooses not to replace with personal funds
  - Funding for service and maintenance

Case Studies

In the right environment, BYOD programs can be an enormous success. The BYOD Working Group members developed a small collection of case studies that highlight the successful implementation of a BYOD pilot or program at a government agency. These studies include a brief synopsis which summarizes the specific challenges, approaches, and lessons learned of each. None of the BYOD programs discussed in these case studies involve the transmission of classified information. Agencies should consider the applicability of the discussed technical and policy approaches to their own environments.

- The Department of the Treasury's Alcohol and Tobacco Tax and Trade Bureau (TTB) implemented a virtual desktop that allowed a BYOD solution with minimal policy or legal implications;
- The U.S. Equal Employment Opportunity Commission (EEOC) was among the first of several Federal agencies to implement a BYOD pilot that allowed employees to "opt out" of the government-provided mobile device program and install third-party software on their own smartphones that enabled the use of their device for official work purposes;
- The State of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant cost savings by having employees turn in their State-owned device in favor of a personally-owned device, which could save the State approximately half of its current wireless expenditure.

Back to top

Alcohol and Tobacco Tax and Trade Bureau (TTB) Virtual Desktop Implementation

Allowing Bring Your Own Device with Minimal Policy or Legal Implications
August 13, 2012

Robert Hughes
Chief Information Officer
Department of the Treasury
Alcohol and Tobacco Tax and Trade Bureau (TTB)
robert.hughes@ttb.gov

Executive Summary

The Alcohol and Tobacco Tax and Trade Bureau (TTB) decided to reduce the costs, time and effort required to refresh desktop and laptop computers used for client computing needs. TTB has a widely dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about $2 million and disrupted the IT program and business users for several months. TTB determined that the best solution was to centralize all client computing power and applications, user data, and user settings and allow access to TTB resources by thin client computing devices. A thin client is a computing device or program that relies on another device for computational power. Currently about 70 percent of TTB personnel use thin client devices to access all TTB applications and data.

TTB desktop and laptop computers were due for refresh this year. However, the virtual desktop solution allowed TTB to avoid the expense of replacing hardware. The savings achieved paid for TTB's virtual desktop implementation – which cost approximately $800,000 – and saved TTB $1.2 million.

TTB realized additional savings by developing a Linux USB device that can be used to turn old desktop and laptop computers into thin client computing devices for approximately $10 per device. The TTB virtual desktop/thin client implementation uses a small browser plugin, freely available for almost every operating system, which simply turns the end user device into a viewer and controller of the virtual desktop running in the TTB computer rooms. No data touches the end user device. As a result, the TTB virtual desktop implementation has the significant additional benefit of delivering every TTB application, with user data, to a wide range of user

devices without the legal and policy implications that arise from delivering data to or allowing work to be accomplished directly on a personal device.

Challenge

TTB was created as an independent bureau in the Department of the Treasury on January 24, 2003, by the Homeland Security Act of 2002. When TTB was established, all information technology (IT) resources, including capital assets, IT personnel and the funding to procure equipment and to develop core business applications remained with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF). TTB was funded at a level sufficient only to reimburse ATF for existing service. No funding was provided for the initial purchase or subsequent replacement of any of the equipment required to establish and operate TTB's IT Systems. In FY 2005 TTB established an independent IT operation with no base funding to refresh infrastructure equipment.

TTB has a very dispersed workforce with many personnel working from home full time and over 80 percent of the workforce regularly teleworking. Replacing desktop and laptop computers every 3 to 4 years cost TTB about $2 million and disrupted the IT program and business users for several months. TTB decided to reduce the costs, time, and effort required to refresh client desktop and laptop computers. After considering several solutions, TTB determined that it would centralize all client computing power and applications, user data, and user settings to allow access to these resources through thin client computing devices. A thin client is a computing device or program that relies on another device for computational power.

Approach

With limited funding to invest in a completely new infrastructure for the virtual desktop implementation, TTB examined its existing hardware, software and technical expertise to determine the path most likely to succeed and achieve the objectives of providing central access to all IT resources while achieving significant savings.

TTB attained considerable success with server virtualization. Approximately 80 percent of the Windows Servers and 20 percent of the Sun Solaris servers at TTB had been virtualized. With this success in hand, TTB was confident that a virtual desktop infrastructure could be built without purchasing numerous physical servers. The infrastructure required to deliver virtual desktop could itself be largely virtualized.

Because TTB was established in 2003 with a significant number of personnel working full time from home, it was imperative from the beginning to support those personnel with a robust remote access capability. Additionally, TTB wanted to take advantage of its investment in Citrix licenses and the significant expertise its technical personnel had gained with the Citrix product suite as they supported remote access. The Citrix virtual desktop offering uses a small browser plugin called Citrix Receiver, which is freely available for download and turns most any device into a thin device. This solution was selected because the Citrix Receiver allows TTB to create thin client devices and support BYOD (initially home computers).

The currently deployed solution has 2 active sites, each with 3 physical servers. Either site can support the entire customer base. The rest of the virtual desktop servers are virtualized. In essence, TTB supports the entire population (650 personnel total in TTB, CDFI, and contractors) with 6 physical servers. Figure 1 is a conceptual view of the TTB virtual desktop.

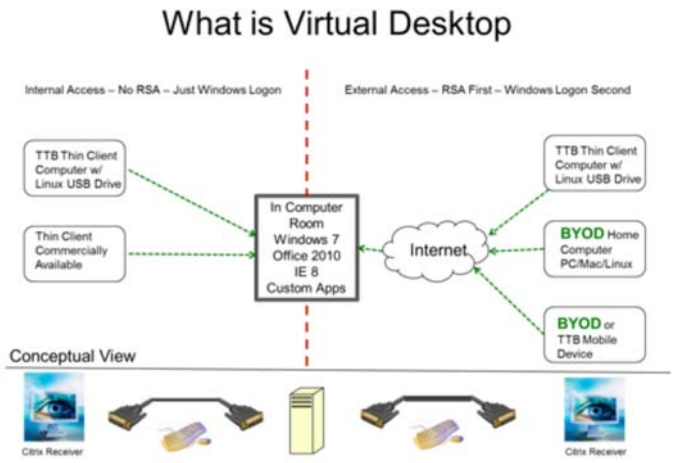

Figure 1

Results

Today about 70 percent of TTB personnel access all TTB computing resources through thin devices, provided by TTB as well as BYOD. There is no typical user setup. If the desired user configuration works, TTB allows it. As an example, a TTB attorney uses a thin client device in the office, a BYOD Mac personal computer when working from home, and a BYOD IPad device when on the road. Several TTB personnel use BYOD Kindle Fire devices for occasional access, for example, if they need to check email when out of the office or they need to approve a time card that was not ready when they were in the office.

The rapid pace of change in the mobile device market makes the virtual desktop solution particularly attractive. Because no data touches the user device, there is no need for a mobile device management (MDM) solution on a non-TTB device. When a device is made available to the public it can be used to access TTB applications and data. The Droid Razr smart phone with a Motorola Lapdock 500 is an example of such a device. A user who has a government-provided smart phone (MDM installed) with a Lapdock would not need an additional computing device. Further, a user who had the same setup, minus the MDM, also could work full time with this BYOD. The ASUS Transformer is another example of a newly available mobile device that has a form factor usable for full-time work.The multiple-device access capability of virtual desktop allows TTB to move toward providing a single device per user.

The final result, which is likely the greatest benefit of the TTB Virtual Desktop solution relative to BYOD, is the minimization or elimination of complex legal and policy issues. Because no data touches the BYOD device and no work is physically accomplished on the BYOD equipment, all requests fordiscovery of information from a user's computer can be satisfied without having to recover anything from the user's personal device.

Lessons Learned

- The primary TTB BYOD lesson learned is to avoid allowing data to touch the personal device. Having all data, settings and processing in a central location and using the BYOD device simply as a viewer significantly simplifies the legal and policy implications.

Hardware/Software

- VMware for server virtualization
- 6 Dell R910 physical servers
- Citrix XenDesktop, XenApp, XenClient (pilot), Receiver, Citrix Provisioning Services
- Netscalers for remote access
- Robust Storage Area Network and Core Network required

Disclaimer

- References to the product and/or service names of the hardware and/or software products used in this case study do not constitute an endorsement of such hardware and/or software products.

Back to top

U.S. Equal Employment Opportunity Commission (EEOC) BYOD Pilot

Transitioning from Blackberry Usage to Bring-Your-Own-Device
July 11, 2012

Kimberly Hancher
Chief Information Officer
U.S. Equal Employment Opportunity Commission
kimberly.hancher@eeoc.gov

Executive Summary

The U.S. Equal Employment Opportunity Commission (EEOC) recently implemented a Bring-Your-Own-Device (BYOD) pilot program to meet urgent IT budget challenges. Employees who want to use their own smartphone for official work purposes must agree to have third-party software installed. This allows the agency to manage security settings on the devices and remotely wipe devices clean of government emails and data if they are lost or stolen.

The EEOC is among the first Federal agencies to implement a BYOD pilot and the preliminary results appear promising. Last year, the EEOC was paying $800,000 for its Government issued BlackBerry devices. Subsequently, the EEOC's FY2012 IT budget was cut from $17.6 million to $15 million, nearly a 15% reduction. The EEOC's Chief Information Officer, Kimberly Hancher, significantly reduced contractor services, eliminated some software maintenance, and slashed the agency's budget for mobile devices -- leaving only $400,000 allocated for Fiscal Year 2012. Along with the other cost reduction measures, CIO Hancher took the issue to the agency's IT Investment Review Board. She suggested a two-pronged approach to cost reduction:

1. **Optimize rate plans for agency provided mobile devices, and**
2. **Implement a BYOD pilot program.**

In November 2011, EEOC's IT staff pressed the wireless carrier, a GSA Networx contract provider, to help cut costs or risk losing the EEOC's BlackBerry business. Although the carrier was initially reluctant to work expeditiously, the EEOC stood firm in pursuing rate plan optimization. Zero-use devices were eliminated and all remaining devices were moved to a bundled rate plan with shared minutes. FY 2012 costs were reduced by roughly $240,000 through these actions.

The next step was to launch a BYOD pilot program focused on enticing current users of Government provided BlackBerry devices to opt out. For months, EEOC's Hancher worked with information security staff, agency attorneys and the employees' union to draft rules that balanced employee privacy and Government security. By June 2012 many BlackBerry users "opted out" and voluntarily joined the BYOD pilot program.

EEOC's BYOD pilot focused on providing employees with access to agency email, calendars, contacts and tasks. With the mobile device management software, employees may read and write emails with or without Internet connectivity. A few senior executives who own Apple iPads will be provided "privileged" access to the agency's internal systems through the secure Virtual Private Network (VPN).

BYOD Challenge

The EEOC's BYOD program grew out of the necessity of meeting new budget challenges with limited resources. The agency was faced with a 15 percent reduction in its IT operating budget for FY 2012. At first, it was not evident there was much room for needed cuts. Therefore, EEOC decided to conduct research into how employees were using their agency-issued Blackberry devices – and the results were surprising:

> *"Seventy-five percent of our users never made phone calls from their BlackBerrys,"*according to Hancher. *"Email is the killer app. They either used the phone on their desk or they used their personal cell phone to make calls because it's just easier. We also found there were a number of zero-use devices. People have them parked in their desk drawer, and the only time they use it is when they travel."*

During the first quarter of FY 2012, initial efforts went into cutting the recurring costs of the nearly 550 agency-issued Blackberry devices. After conducting an analysis of device usage, the EEOC swiftly submitted orders to the carrier eliminating zero-use devices, demanded that disconnect orders were promptly terminated, and called for remaining Government devices to be moved to a bundled plan with shared voice minutes and unlimited data.

In December 2011, the EEOC launched the first official phase of its BYOD pilot. A BYOD advisory group was created to help the Office of Information Technology flesh out the new program. The advisory group was asked to identify cloud providers for mobile device management, identify security risks, research privacy concerns, draft Rules of Behavior, and create an internal website on the agency's intranet. The advisory group worked for months to socialize the concept of BYOD within the agency's workforce. In turn, nearly 40 employees volunteered to exchange EEOC-issued BlackBerry devices in favor of using their own personal smartphones.

Alpha Phase

During the alpha phase of the BYOD pilot, the EEOC's IT group worked with the mobile device management cloud provider to configure the exchange of electronic mail between the providers' host and the EEOC's email gateway. The IT staff was enthusiastic about the transition to a cloud provider, having managed the agency's BlackBerry Enterprise Services (BES) for many years. The cloud provider would assist with setup, configuration and end-user support. Under the BYOD pilot, the cloud provider conducts all technical support for pilot participants with iOS devices (iPhone and iPads), as well as all Android devices (smartphones and tablets). The EEOC decided to use its existing on-premise BES for additional support as needed.

Within the first few months of alpha pilot's launch, the advisory group reached out to other federal agencies to examine their BYOD programs. The EEOC's first draft of the BYOD Rules of Behavior was circulated among the advisory group, the technical team and the IT Security Officers.

After a number of revisions, the draft policy was ready to share with the union. The Deputy CIO and Chief IT Security Officer met with the union several times to discuss the issues. Again, the Rules of Behavior document was revised and improved upon. An "expectation of privacy" notice was written in bold on Page 1 of the four-page policy.

In March 2012, the BYOD team solicited feedback from the alpha team. A work breakdown structure was created to guide activities and tasks that needed to be completed before launching the next phase of the pilot -- the beta phase. Then, in June 2012, the EEOC provided several choices for the 468 employees who still used agency-issued BlackBerry devices:

1. **Voluntarily return your BlackBerry and bring your own Android, Apple or BlackBerry smartphone or tablet to work.**
2. **Return your BlackBerry and get a Government-issued cell phone with voice features only.**
3. **Keep your BlackBerry with the understanding that EEOC does not have replacement devices.**

The BYOD pilot is expected to run through September 2012, or longer, depending on the agency's comfort level that all policy issues have been appropriately addressed. CIO Hancher projects between 10 percent and 30 percent of BlackBerry users will opt in for the BYOD program. The CIO examined incorporating an incentive to opt out, but could not find a precedent for offering a nominal stipend or reimbursement for business expenses and equipment allocation. Therefore, EEOC decided to proceed with the BYOD pilot and to revisit other outstanding issues once Government-wide BYOD guidance was released. In order to protect sensitive corporate data, EEOC is scheduling some BYOD orientation sessions to train its workforce on critical security ramifications and procedures.

One goal of EEOC's BYOD pilot is to obtain feedback and comment on the first version of the Rules of Behavior. The CIO fully expects modifications to the BYOD policy as the pilot evolves. Some outstanding questions, for example, include whether an enforceable waiver should be added exempting employees from holding the organization accountable. Can the agency offer an equipment allocation or reimbursement for a portion of the data/voice services?

Acceptable Behavior Policy

EEOC is currently in the process of reviewing and revising its Acceptable Behavior Policy for personal mobile devices. The policy document was developed as part of a working group that included the agency's Office of Legal Counsel. Employees who choose to opt into the BYOD program are required to read and sign the policy document first.

CIO Hancher said one thing agencies need to make sure of is that they have documented rules for what employees can and cannot do with Government data on personally-owned devices. Moreover, she said that employees must agree to let agencies examine those devices should it become necessary. EEOC's IT staff is meeting with employees to help decide which device or devices to use and what the likely effects will be. At the current time, personal smartphone devices are the only mobility option for new employees at EEOC.

BYOD Pilot Results

From 2008 to 2011, EEOC's BlackBerry provisioning program grew from about 100 devices to approximately 550 devices. By December 2011 about 23% of the workforce was provided with Government-issued smartphones. Realizing that this pattern was unsustainable, CIO Hancher, with support from the executive leadership and the union, set out to revamp the mobile device program.

The initial alpha pilot was launched with 40 volunteers who turned in their Government BlackBerry in favor of using a personally owned smartphone/tablet (Android,

Apple iOS or BlackBerry). EEOC used cloud based, software-as-a-service for wireless synchronization of agency email, calendar and contacts, as well as mobile device management services.

Within the first three months of 2012, the number of BlackBerry devices was cut from 550 to 462 and monthly recurring costs were lowered by 20-30% by optimizing the rate plans. By June 2012, EEOC launched the beta pilot inviting all BlackBerry users to opt in to BYOD and return their BlackBerry. However, EEOC will allow employees to continue using an EEOC provided BlackBerry if they choose not to opt into BYOD.

The current BYOD program requires employees to pay for all voice and data usage, including those for official work purposes. This cost issue may prompt some users to keep the BlackBerry. However, for EEOC's younger employees, their personal devices appear to be an extension of their personalities, so to speak. For seasoned workers, their personal device allows them to do administrative work from home.

> *"While I'm not advocating working 24 by 7, it is just more comfortable to sit and do timecard approvals on a Friday night in the comfort of your home instead of during the prime time work day when your attention should be on more complex and business-oriented issues,"*said CIO Hancher.

Lessons Learned

- **Socialize the concept of BYOD**. Since this a new concept and the acronym is taking time to be universally recognized, it is advisable to spend time explaining the BYOD concept to the workforce, including at senior staff meetings and executive council sessions.
- **Work with the agency's Legal Counsel and unions early in the process**. Allow input on the BYOD program and policies from leadership officials.
- **Select important security features for implementation**. Work to identify prioritized security settings or policies, implement them carefully, then cycle back to identify additional security measures after the first set are completed.

Hardware/Software

- Notifylink MDM – Cloud provider licensed at $120 per user per year
- GW Mail and GW calendar – $5 apps available through iTunes and Android Market

Disclaimer:

- References to the product and/or service names of the hardware and/or software applications used in this case study do not constitute an endorsement of such hardware and/or software products.

Back to top

State of Delaware BYOD Program

Transitioning from State-owned Blackberries to a Personal Device Reimbursement Plan
July 16, 2012

William B. Hickox
Chief Operating Officer
Delaware Department of Technology & Information
William.Hickox@state.de.us

Executive Summary

In an effort to keep up with the pace of mobile technology, the State of Delaware initiated an effort to not only embrace the concept of BYOD but to realize significant savings by having state employees turn in their state owned device in favor of a personally owned device. In order to encourage the behavior, the State agreed to reimburse a flat amount for an employee using their personal device or cell phone for state business. It was expected that by taking this action the State could stand to save $2.5 million or approximately half of the current wireless expenditure.

There were several challenges including questions about whether a reimbursement was taxable or not, whether the personal device could be secured by the State for Freedom of Information Act (FOIA) requests, and whether utilization of personal devices could/should be mandated. In the end the state decided to make the program voluntary at this time. The state recognizes that not all employees have a personal device or are willing to utilize it for work purposes.

The State of Delaware experience to date has been positive with specific savings and device reductions. The State anticipates continuing to grow the program by limiting the number of state owned devices while encouraging the use of personal devices into the future.

Challenge

The State's Blackberry infrastructure is reaching end of life and requires a lifecycle replacement. In addition, changes in technology are driving agencies to request

devices that are not state standard or currently supported by the Department of Technology & Information (DTI). As such, the State is now at a decision point regarding the future direction of portable wireless devices and the ongoing support of the infrastructure.

Over the last 10 years the nature and use of portable wireless devices in the workplace has changed dramatically. Originally, only a handful of state owned devices (BlackBerrys) existed with the majority of staff relying on state owned cell phones. In addition, at that time very few state employees had personal cell phones and almost none had personal blackberry devices. Today, the proliferation of these state owned devices (approximately 2500 devices) results in significant costs associated with the infrastructure and support of the blackberry system. In addition, due to the changing needs of the agencies, more and different devices such as Droids and iPhones are being requested, which would expand the costs associated with infrastructure and support. The current Blackberry Enterprise Server (BES) which is managed by the state will reach its end of life within the next year and require replacement. However, replacing the BES will only address the state owned devices that are currently approved as standard (Blackberry). It does not address the request for additional portable devices such as iPhones.

Approach

DTI decided that funds should not be expended to lifecycle the BES. Instead, the State should start a two year transition plan to migrate all users off of the existing infrastructure by June 30, 2013 and move them to either a personal device through a proposed reimbursement program or to a device that runs directly through the state's wireless carrier. By doing so, the state stands to save up to $2.5 million dollars annually through the reimbursement program but also would save $75K in lifecycle costs and $120K in ongoing support. This direction would also allow agencies to utilize enhanced devices such as Droids and iPhones to support their business needs.

The above referenced reimbursement program would be as follows:

Beginning February 1, 2011 the Department of Technology and Information (DTI) will initiate a program aimed at reducing the number of state owned wireless communication devices, i.e. cellular phones, PDAs, portable devices, etc. The intended benefits of this program are twofold. Many employees carry personal devices in addition to the state issued device. With the advances in technology, efficiencies can be gained through the combination of these devices. In addition to end user efficiency, by combining devices, there is significant savings for the State.

Employees whose job duties require the frequent need for a cell phone or portable device as determined by their supervisor may receive a monthly voice/data plan reimbursement to cover the costs of state related business. Only in extenuating circumstances will further reimbursement for voice/data plan costs be available to employees who participate. All other employees may submit infrequent business-related cell phone expenses for individual reimbursement.

Determining Employee Eligibility: Employees with job duties that require the frequent need to use a cell phone/PDA for business purpose are eligible, typically include;

- Employees on the road or in the field, but required to remain in touch with others, typically out of the office on business 50 or more annual days.
- Employees available for emergency contact (e.g., duties require them to be contacted anywhere/anytime).
- Employees with 24/7 response requirements.

Dollar Amount of Reimbursement: Eligible employees will receive a reimbursement as follows:

- Voice only - $10 per month
- Data only - $30 per month
- Voice/Data - $40 per month

Results

For the employees that have participated, the State has reduced the expense associated with their devices by 45%. This has resulted in an overall reduction of departmental wireless costs of 15%. As the State continues to grow the program it expects its overall wireless cost savings to continue to grow. While it started out with only DTI participation, it now has Department of Corrections, Department of Transportation, Department of Health and Social Services, and the Governor's Office participation. Altogether the State of Delaware is currently reimbursing over 100 employees for utilizing their personal device and over 1,000 State of Delaware employees are using their personal devices in the BYOD program.

Lessons Learned

- When discussing reimbursement, the State had to ensure that it was not providing a stipend, but in fact a reimbursement after the fact. As such, employees are required to submit an already paid wireless bill that is then processed for reimbursement under the monetary guidelines set above. This avoids the issue associated with stipends being taxable under the IRS regulations.
- Freedom of Information Act requests were another sticking point. However, the State has been able to avoid the issue since all of the state's e-mail is centralized and a copy of every transaction is maintained on the central servers which results in a clean copy being available for discovery if necessary.
- A current challenge is the State's inability to grow the reimbursement program as fast as it would like. This is due to the fact that the wireless carriers are now placing limits on data which has resulted in employees unwilling to agree to use their personal device for work since they no longer have unlimited data and the State will not provide additional reimbursement if employees go over the data maximum.

Disclaimer

- References to the product and/or service names of the hardware and/or software applications used in this case study do not constitute an endorsement of such hardware and/or software products.

Example Policies

The BYOD Working Group assembled sample policies in use at agencies to help inform IT leaders who are considering developing a BYOD program for their agencies. Sample policies include:

Sample #1: Policy and Guidelines for Government-Provided Mobile Device Usage

Version **X, [DATE]**

The following policy and guidelines inform government-provided mobile device users of their allowable usage and features available for business and limited personal use. This document also serves to make clear the responsibility of mobile device users to take proper care of the government furnished equipment entrusted to them. Mobile device care is the responsibility of each mobile device user. Failure to adhere to the guidelines listed below may result in personal liability and/or retraction of device privileges.

The new standard monthly rate plans for **[AGENCY NAME]** issued Blackberry devices include:

- Voice - 300 “anytime” minutes within the Continental US (CONUS), per device.
- Data - unlimited data (e-mail and Internet access) within the CONUS.
- Unlimited Nights (9 pm – 6 am) and Weekends (9 pm Friday to 6 am Monday)
- Unlimited **[PRODUCT NAME]** to **[PRODUCT NAME]** Calling
- Unlimited Domestic Text Messaging
- Everyone is on a bundled voice/data plan with shared voice.

(Government-Provided Cell Phones follow same Voice/Text parameters, No Data)

[AGENCY NAME] expects mobile-device users to:

- Protect their government-issued device from theft, damage, abuse, and unauthorized use;
- If the device is lost or stolen, the user will notify the **[AGENCY NAME]** Help Desk (**[AGENCY HELPDESK PHONE]** or **[AGENCY HELPDESK EMAIL]**) within one hour, or as soon as practical after you notice the device is missing. **[AGENCY OFFICE OF INFORMATION TECHNOLOGY]** will lock and disable the device upon notification. A lost or stolen device will be replaced a maximum of three times, pending availability of devices and funding;
- Maintain usage within the plan parameters identified above. If your business use requirements are dramatically different than the standard plan, you must contact **[AGENCY OFFICE OF INFORMATION TECHNOLOGY]** to discuss other available options; Comply with **[AGENCY NAME]** appropriate use policies when using the device (**[REFERNCE AGENCY APPROPRIATE USE POLICIES]**);
- Abide by the law governing the use of mobile cell phones and/or smartphones while driving (*e.g.*, hands-free use and/or texting); and
- Purchase any additional mobile device accessories (*e.g.*, holsters, cases, car chargers, screen protectors, Bluetooth headsets, etc.) that the user may desire in addition to the items provided by the government.

Privacy Expectations:

Government employees do not have a right, nor should they have an expectation, of privacy while using Government provided devices at anytime, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the Government provided device for limited personal use. By acceptance of the government provided device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

Additional Guidelines:

- **[AGENCY NAME]** Office of Information Technology (OIT) has complete oversight and management of device usage and expenses.
- The government-provided devices are being provided as a productivity tool for business use. OIT reserves the right to terminate services for non-use, limited business use, or excessive personal use. The policy for terminating voice and data services for non-usage is 30 days.
- Due to voice plan minute restrictions, employees should opt to use their work landline phone, when at their workstation, to make and receive calls.
- **[AGENCY NAME]** staff are permitted limited use of Government IT equipment for personal needs if the use does not interfere with official business and imposes no additional expense to the Government. Since voice minutes on the government’s plan are limited, personal phone calls should be limited to brief occasional calls. Calls that are made during the weekend, evening (9 pm – 6 am), or to other **[PRODUCT NAME]** customers do not count against plan minutes. The government plan provides unlimited data, so limited personal Internet use is permitted, but should occur during non-work time. All limited personal use must be in compliance with **[AGENCY NAME]** appropriate use policies.
- Mobile device selection and issuance is based on availability on the GSA contract and certified FIPS 140-2 encryption standard compliance. At this time, only RIM Blackberry devices are certified as compliant with this standard.
- Assistance or support is handled by the **[AGENCY NAME]** Helpdesk by calling **[AGENCY HELPDESK PHONE]** or emailing **[AGENCY HELPDESK EMAIL]**.
- International roaming services may be available on a temporary basis for business travel only. Data rate plans for e-mail and broadband cards are an additional cost to **[AGENCY NAME]** for mobile device users traveling outside the CONUS. Contact OIT 30 days prior to travel to request temporary international roaming feature if you have official government travel plans abroad. Failure to add the international roaming feature could result in cost overages for which the Agency will not be responsible.
- **[AGENCY NAME]** reserves the right to recall/disconnect government-provided mobile devices due to budget restrictions or changes to deployment priorities.

Questions related to the above Policy and Guidelines should be directed to the **[AGENCY NAME]** Helpdesk.

Sample #2: Bring Your Own Device – Policy and Rules of Behavior

[**AGENCY NAME**]

(**Version X, [DATE]**)

This document provides policies, standards, and rules of behavior (ROB) for the use of personally-owned smart phones and/or tablets by **[AGENCY NAME]** employees (herein referred to as users) to access **[AGENCY NAME]** network resources. Access to and continued use of network services is granted on condition that each user reads, signs, respects, and follows the **[AGENCY NAME]**'s policies concerning the use of these devices and services.

The Office of Information Technology (OIT) is piloting a "Bring Your Own Device" (BOYD) program to permit agency personnel to use personally owned smart phones and tablets for business purpose. The policy and ROB vary depending on service usage, as outlined below.

Current Devices Approved for Use During BYOD Pilot:

Android Smart Phones & Tablets
Blackberry Smart Phones & Playbook
iOS iPhones & iPads

Expectation of Privacy: [AGENCY NAME] will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads government email/attachments/documents to their personal device) . This differs from policy for government-provided equipment/services, where government employees do not have the right, nor should they have the expectation, of privacy while using government equipment or services. While access to the personal device itself is restricted, **[AGENCY NAME]** Policy and Rules of Behavior regarding the use/access of government e-mail and other government system/service remains in effect. If there are questions related to compliance with the below security requirements, the user may opt to drop out of the BYOD program versus providing the device to technicians for compliance verification.

With the use of **[PRODUCT NAME]** (standard **[PRODUCT NAME]** access via Internet/Web Browser) and/or **[PRODUCT NAME]** Products, business e-mails are accessed across the Internet and are NOT downloaded to the device; therefore, there are no additional security requirements other than the Overall Requirements noted in Section I.

The Notify-Link is a cloud based mobility solution that provides secure, real-time synchronization of email, calendar, and contacts to and from the Apple/Android devices. With Notify-Link, users have the ability to compose, reply, forward, or delete their email while mobile, as well as open a variety of email attachment formats. With the use of Notify Link Apps, business e-mails and appointments are downloaded and stored on the device, so additional security requirements are necessary.

Users of personally-owned Blackberry Devices can have their device incorporated into the **[AGENCY NAME]** BES environment, assuming the device meets compatibility requirements (to include Verizon service & model eligibility – contact **[AGENCY NAME]** OIT for specific requirements).

Document Transfer involves connecting the personal device to the user's work PC via USB connections for file-sharing (document transfer) or backup purposes. It also includes backing up data/documents to external sources, such as cloud storage services.

VPN BYOD access is available for senior executives or management and requires approval of the Chief Information Officer (CIO). Currently this access is only available for Apple iOS iPad devices. Access is not been approved for Android devices.

I. **Overall Requirements for all BYODs Accessing [AGENCY NAME] Network Services:**

- User will not download or transfer sensitive business data to their personal devices. Sensitive business data is defined as documents or data whose loss, misuse, or unauthorized access can adversely affect the privacy or welfare of an individual (personally identifiable information), the outcome of a charge/complaint/case, proprietary information, or agency financial operations. This excludes government e-mail that is protected through the various security controls listed below;
- User will password protect the device;
- User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer. The user will not "Jail Break" the device (installing software that allows the user to bypass standard built-in security features and controls);
- User agrees that the device will not be shared with other individuals or family members, due to the business use of the device (potential access to government e-mail, etc);
- User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing e-mail attachments. **[AGENCY NAME]** OIT will provide instructions for identifying and removing these unintended file downloads. Follow the premise, "When in Doubt, Delete it Out."

II. **Accessing [PRODUCT NAME] (e-Mail/Calendar) Services on BYOD**

a. **Use [PRODUCT NAME] or [PRODUCT NAME]**

b. **Use of Notify-Link Applications**

- As a default, Notify-Link will be enabled to perform an e-mail wipe on the phone after 25 password failed attempts (please be advised that only e-mail on the device will be deleted);
- If the device is lost or stolen, the user will notify the **[AGENCY NAME]** Help Desk (**[AGENCY HELPDESK PHONE]** or **[AGENCY HELPDESK EMAIL]**) within one hour, or as soon as practical after you notice the device is missing. **[AGENCY NAME]** OIT will lock the device, e-mail on the device will be deleted, and notify-link services will be deactivated;
- Users must comply with all **[AGENCY NAME]** password policies, including use of strong passwords, password expiration (6 months), and password history (3).
- **[AGENCY NAME]** reserves the right to terminate government-provided Notify-Link services for non-use. The policy for terminating Notify-Link services in 30 days.

c. **Use of Blackberry Enterprise Server (BES)**

- User will allow **[AGENCY NAME]** to enforce standard **[AGENCY NAME]** BES policies on the personal device, with the exception that the user will be allowed to download third-party apps to personal device;

- If the device is lost or stolen, the user will notify the **[AGENCY NAME]** Help Desk (**[AGENCY HELPDESK PHONE]** or **[AGENCY HELPDESK EMAIL]**) within one hour, or as soon as practical after you notice the device is missing. OIT will lock the device, e-mail on the device will be deleted, and BES services will be deactivated.

III. **Document Transfer**

a. **USB Connection to Work PC**

- Only BYODs that provide FIPS 140-2 device-level encryption may be connected to **[AGENCY NAME]** PCs for document transfer purposes (currently only Blackberry devices are certified as 140-2 compliant);
- User will enable use of a second strong password for authentication upon connection to the PC. This password should be different from the primary device password;
- User will maintain anti-virus (AV) protection on the device (**[AGENCY NAME]** - provided or other). The AV software in use will be identified at the end of this document for review/approval by OIT; and
- User will not download/transfer business data that is considered sensitive or confidential to the personal device, including charge/case-related documents that contain personally identifiable information.

b. **Backing-Up / Storing documents on non-[AGENCY NAME] Servers**

- User will not download/transfer sensitive **[AGENCY NAME]** business data/documents to any non-**[AGENCY NAME]** device.

IV. **Use of Virtual Private Network (VPN) to access Network Services**

- Users must have a need to access internal **[AGENCY NAME]** resources, such as the Integrated Mission System, Document Management System, Network drives, etc., as required by her/his position and duties
- Users may only use **[AGENCY NAME]** approved and configured VPN client software to access **[AGENCY NAME]**'s VPN;
- Users must allow **[AGENCY NAME]** administrators to install Trend Micro security suite (firewall, antivirus, and web site protector applications) on their personal device;
- Users must comply with all **[AGENCY NAME]** Password Policies on their device, including use of strong passwords, password expiration (6 months), and password history (3).
- Users will immediately notify OIT if the device is lost or stolen, at which point **[AGENCY NAME]** will lock the device using Trend Micro and disable the user's VPN access.

USER ACKNOWLEDGMENT AND AGREEMENT

It is **[AGENCY NAME]**'s right to restrict or rescind computing privileges, or take other administrative or legal action due to failure to comply with the above referenced Policy and Rules of Behavior. Violation of these rules may be grounds for disciplinary action up to and including removal.

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of **[AGENCY NAME]** services. I understand that addition of government-provided third party software (such as Ghost-Pattern, Notify Link, Airwatch, Good, etc) may decrease the available memory or storage on my personal device and that **[AGENCY NAME]** is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program. I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by **[AGENCY NAME]** OIT. I understand that business use may result in increases to my personal monthly service plan costs. I further understand that government reimbursement of any business related data/voice plan usage of my personal device is not provided.

Should I later decide to discontinue my participation in the BYOD Program, I will allow the government to remove and disable any government provided third-party software and services from my personal device,

Employee Name: _____

BYOD Device(s): _____

Services to be Used: _____

Anti-Virus or other Security Software installed on the Device: _____

Employee Signature: _____ Date: _____

Sample #3: Mobile Information Technology Device Policy

Effective Date:[DATE]

Responsible Office:[OFFICE NAME]

Updated: (To accommodate access for personally owned devices - BYOD)

1.0 Purpose

This sets forth the security control standards for the issuance, administration, use, and security of mobile information technology (IT) devices that are used to conduct **[AGENCY NAME]** business. These standards are established to protect **[AGENCY NAME]** information on mobile IT devices, which consist of any non-stationary electronic apparatus with capabilities of recording, storing, and/or transmitting data, voice, video, or photo images and include laptops, personal digital assistants (PDAs), cellular phones, satellite phones, digital tablets, secure tokens, and any related storage media or peripheral devices (e.g. CDs, flash memory, Internet Air Cards, etc.).

2.0 Authorities

OMB Circular A-130, Clinger-Cohen Act, Federal Information Security Management Act, NIST SP 800-124, and NIST SP 800-53.

3.0 Policy

It is the policy of the **[AGENCY NAME]** to develop and maintain security control standards for all **[AGENCY NAME]** owned, mobile IT devices that create, access, process or store Agency information, and the information created, collected, and processed on behalf of **[AGENCY NAME]** on these devices. This policy also covers personally owned mobile IT devices that access or store Agency information. These standards are part of the overall **[AGENCY NAME]** Information Security Program authorized by **[AGENCY SECURITY DOCUMENTATION NAME]** and must be followed by all **[AGENCY NAME]** employees, contract personnel, Volunteers, and Trainees. The Chief Information Officer (CIO) directs and oversees compliance with the security control standards for mobile IT devices.

4.0 Roles and Responsibilities

4.1 The Chief Information Officer

The CIO has overall responsibility for establishing the security standards for mobile IT devices and must:

a. Procure all **[AGENCY NAME]** owned mobile IT devices for **[AGENCY NAME]** issuance and approve the types of personally owned devices that will be used.
b. Assure that **[AGENCY NAME]** issued mobile IT devices are available for staff members with job functions that are mission critical to **[AGENCY NAME]** operations, or that protect the safety and security of **[AGENCY NAME]** staff or Volunteers.
c. Provide for the distribution, operation, and administrative support of issued mobile IT devices.
d. Maintain an inventory of **[AGENCY NAME]** mobile IT devices by serial number, user's office, user's name, and service start/end dates.
e. Maintain an inventory of licenses for **[AGENCY NAME]** owned software installed on each personally owned and **[AGENCY NAME]** owned mobile IT device.
f. Establish and maintain security configurations for all issued mobile IT devices, including patching and upgrading of software/firmware.
g. Log and monitor the activity on all issued devices for compliance with the Rules of Behavior for General Users.
h. Develop the **[AGENCY NAME]** Remote Access and Mobile Information Technology User Guide.

4.2 Supervisors

Supervisors of **[AGENCY NAME]** staff who have applied for, or have been issued, mobile IT devices or wish to use personal mobile IT devices to conduct **[AGENCY NAME]** business must:

a. Ensure compliance with managerial requirements as described in the **[AGENCY NAME]** Remote Access and Mobile Information Technology Guide.
b. Sign and approve the Mobile IT Device User Agreement Form for each user that they supervise.
c. Report the lost, stolen, damaged, destroyed, compromised or non-functional **[AGENCY NAME]** issued mobile device to the **[PROPER AUTHORITY]**.
d. Confirm that the lost, stolen, damaged, destroyed, compromised, or non-functional IT device has been reported to the **[AGENCY NAME]** Service Desk by the user.

4.3 Users

Users who conduct official **[AGENCY NAME]** business on a mobile IT device must:

a. Sign the Remote Access and Mobile IT Device User Agreement Form.
b. Operate the device in compliance with this policy, all applicable federal requirements, and the **[AGENCY NAME]** Remote Access and Mobile Information Technology Guide.
c. Not process or access Classified information on the device.
d. Use only approved and authorized **[AGENCY NAME]** owned devices to physically attach to **[AGENCY NAME]** IT systems.
e. Store only the minimum amount, if any, of Personally Identifiable Information (PII) and electronic Protected Health Information (ePHI) necessary to do one's work, and immediately delete the PII or ePHI when no longer needed. Users shall receive written approval from their supervisor before accessing, processing, transmitting, or storing **[AGENCY NAME]** Sensitive Information such as PII or ePHI.
f. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
g. Immediately contact the **[AGENCY NAME]** Service Desk and their immediate supervisor if the IT device is lost, stolen, damaged, destroyed, compromised, or non-functional.
h. Abide by all federal and local laws for using the device while operating a motor vehicle (e.g. users are banned from text messaging while driving federally owned vehicles, and text messaging to conduct **[AGENCY NAME]** business while driving non-government vehicles).

Users who are issued a **[AGENCY NAME]** owned mobile IT device must also:

a. Comply with **[AGENCY TECHNOLOGY POLICY]**.
b. Not disable or alter security features on the device.
c. Only use the **[AGENCY NAME]** owned device for official government use and limited personal use.
d. Reimburse the OCIO for any personal charges incurred that are above the established fixed cost for the Agency's use of the device (e.g. roaming charges incurred for personal calls).
e. Be required to reimburse the **[AGENCY NAME]** if the mobile IT device is lost, stolen, damaged or destroyed as a result of negligence, improper use, or willful action on the employee's part and if determined by the **[PROPER AUTHORITY]**.

5.0 Effective Date

The effective date is the date of issuance.

Sample #4: Wireless Communication Reimbursement Program

POLICY STATEMENT

Beginning **[DATE]**, the **[AGENCY NAME]** will initiate a program aimed at reducing the number of government-owned wireless communication devices (i.e. cellular

phones, PDAs, portable devices, etc). The intended benefits of this program are twofold: Many employees carry personal devices in addition to the government-issued device. With the advances in technology, efficiencies can be gained through the combination of these devices. In addition to end-user efficiency, combining devices means significant savings for the government.

Employees whose job duties require the frequent need for a cell phone or portable device as determined by their supervisor may receive a monthly voice/data plan reimbursement to cover the costs of government-related business. Only in extenuating circumstances will further reimbursement for voice/data plan costs be available to employees who participate. All other employees may submit infrequent business-related cell phone expenses for individual reimbursement.

USE OF PERSONAL CELL PHONE/PORTABLE DEVICE FOR BUSINESS PURPOSES

Determining Employee Eligibility: Employees with job duties that require the frequent need to use a cell phone/PDA for business purpose are eligible, typically including:

- Employees with 24/7 response requirements.
- Employees available for emergency contact (e.g., duties require them to be contacted anywhere/anytime).
- Employees on the road or in the field (typically out of the office on business **[XX]** or more days annually) who are required to remain in touch with others.

Dollar Amount of Reimbursement: Eligible employees will receive a reimbursement as follows:

- Voice only - $**[XX]** per month
- Data only - $**[XX]** per month
- Voice/Data - $**[XX]** per month

Establishing the Payment of Reimbursement: Complete the Mobile Device Reimbursement Request Form and submit to your supervisor for approval. Your supervisor will determine if the request meets the criteria and intent of the policy.

The reimbursement does not constitute an increase to base pay, and will not be included in the calculation of any salary adjustments.

Payment to the Employee: Payment will be made upon presentation of a completed Personal Reimbursement Form along with copies of the monthly device bill, but not more frequently than quarterly.

Use of Device: The employee must retain an active device as long as a device reimbursement is in place. The device may be used for both business and personal purposes. Extra services or equipment may be added at the employee's expense.

Users must agree to comply with **[AGENCY NAME]** security requirements for personal devices connecting to the government network. The specific requirements can be found at the following **[link]**.

Fees for Contract Changes or Cancellation: The employee is responsible for all fees to change contracts and cancellation charges.

Sample #5: Portable Wireless Network Access Device Policy

[AGENCY NAME]		
Doc Ref Number:	XXXX	**Revision Number:** XX
Document Type:	Enterprise Policy	**Page:** 39 of 43
Policy Title:	Portable Wireless Network Access Device Policy	

Synopsis:	Establish rules for the use of the portable wireless network access device and its connection to the **[AGENCY NAME]** network.		
Authority:	**LIST/CITE APPLICABLE FEDERAL/AGENCY RULES & REGULATIONS THAT ESTABLISH AUTHORITY**		
Applicability:	All users of the **[AGENCY NAME]** communications and computing resources.		
Effective Date:	**[DATE]**	**Expiration Date:**	**[DATE]**
POC for Changes:	**[AGENCY POC]**		

Approval By:	**[AGENCY APPROVING AUTHORITY]**
Approved On:	**[DATE]**

I. **Policy**

POLICY SCOPE

This policy applies to all employees of the **[AGENCY NAME]** who use portable wireless devices capable of accessing **[AGENCY NAME]** computing resources. This policy describes the handheld wireless network access system implementation, recommends guidelines for usage and lists policies and procedures that apply to its use. Portable wireless network access devices are provided to improve customer service and enhance government efficiencies and will only be provided to employees whose Managers have determined that the employee has a demonstrated need.

The purpose of this policy is to establish rules for the use of portable wireless computing devices and their connection to the **[AGENCY NAME]** network. These rules are necessary to preserve the integrity, availability and confidentiality of the **[AGENCY NAME]** network.

POLICY STATEMENT

Those employees of the **[AGENCY NAME]** who have a need for immediate notification and access to email, voice and web services while away from their office or in a mobile situation are candidates for use of a portable wireless network access device. All usage is covered by **[AGENCY NAME]**'s Acceptable Use Policy. Primary use of the portable wireless network access device is for official **[AGENCY NAME]** business. Personal use of government-owned portable wireless network access devices (for email, calendar, incoming and outgoing telephone calls) shall be limited to infrequent, incidental and/or emergency use.

POLICY PROVISIONS

Within each department, agency and/or component, the determining authority and responsibility for issuance of portable wireless network access device shall rest with the **[COMPONENT APPROVING AUTHORITY]** or similar approving authority.

Final authority and wireless activation of each new wireless network access device shall rest with the **[AGENCY NAME]** Chief Information Officer or his/her designee.

[AGENCY NAME] shall implement appropriate process and controls over the common server, infrastructure, transport services and computing resources under its control. Deployment of the portable wireless network access devices will be limited dependent on available resources.

Network security controls must not be bypassed or disabled. To the extent possible, security capabilities of the wireless device should be employed that are consistent with the **[AGENCY NAME]** Acceptable Use Policy. Use of any Cellular Telephone access shall be governed by the **[AGENCY NAME]** Cellular Telephone policy.

Violation of this policy may result in disciplinary action, loss of access privileges to the common server infrastructure, or civil and criminal prosecution.

POLICY OVERVIEW

The **[AGENCY NAME]** supports portable wireless network access as a line of service for customers. Support of full integration of e-mail, calendaring, contacts, etc. into a portable wireless network access device is provided only for those customers articulating a clear business need for their employees.

Acquisition of portable wireless network access devices by customers requires the prior written approval of their [COMPONENT APPROVING AUTHORITY] or similar approving authority. Concurrence of the [AGENCY NAME] Chief Information Officer (CIO) or designee is required for new service or transfers.

Note: Only devices provided by [AGENCY NAME] will be connected to the network and supported by [AGENCY NAME].

Deployment of wireless network access devices will be limited, and will be authorized based on the following criteria:

- Program Focus: The purpose of portable wireless network access devices are to provide continued access to resources deemed necessary for providing continued support in maintaining the functionality of their agency's program. Without such device decisions may be delayed and the effectiveness of the program shall be reduced.
- Available Resources: Funds for the purchase and monthly subscription costs for portable wireless network access devices are the responsibility of the customer. Customers seeking to deploy portable wireless network access devices should clearly articulate the source of funds to support the upfront and ongoing costs, and also demonstrate a commensurate reduction in costs for other services where applicable. (For example, to the extent that deployment of these devices obviates the need to have staff utilize other wireless services – e.g., a wireless network card for a laptop computer – customers should quantify expected savings in their written request.)
- Technology Supported: **[AGENCY NAME]** has chosen to support the portable wireless network access devices which employ the Code Division Multiple Access (CDMA) telecommunications standard and will evaluate the technology as market conditions warrant to determine the most effective options for deploying this service.

RESPONSIBILITY

The **[AGENCY NAME] [AGENCY POC]** is responsible for the development and maintenance of the procedures to implement this policy. The administration, procedural and enforcement responsibilities of this policy may be delegated to other **[AGENCY NAME]** staff.

The requestor (Customer) is responsible for using the portable device in a manner consistent with the Acceptable Use Policy in an effort to provide continued customer service and enhance Department program mandates.

PROCEDURES

ACTIVATION OF A WIRELESS SERVICE

When a **[COMPONENT APPROVING AUTHORITY]** or similar approving authority signifies a **[AGENCY NAME]** employee requires a portable wireless network access device, they may submit a written request (the **[AGENCY NAME]** Telecommunications Portable Wireless Network Access Device Request Form) to **[AGENCY NAME]**. Funds for the purchase and monthly subscription costs for the device(s), user training, upgrades and maintenance are the responsibility of the requesting component and not the **[AGENCY NAME]**.

II. Definitions

None.

III. Development and Revision History

Initial version established **[DATE]**

Reformatted version established **[DATE]**

Updated **[DATE]**

Appendix removed **[DATE]**

IV. Approval Signature Block

On File **[SIGNATURE OF AGENCY APPROVING AUTHORITY]**	
Name & Title: **[NAME & TITLE OF AGENCY APPROVING AUTHORITY]**	**Date** **[DATE]**

V. Listing of Appendices

None.

Back to top

[1] BYOD is a concept that allows employees to utilize their personally-owned technology devices to stay connected to, access data from, or complete tasks for their organizations. At a minimum, BYOD programs allow users to access employer-provided services and/or data on their personal tablets/eReaders, smartphones, and other devices. This could include laptop/desktop computers; however, since mature solutions for securing and supporting such devices already exist, this document focuses on the emerging use case of mobile devices.

[2] *NIST SP 800-124 Revision 1 (Draft), Guidelines for Managing and Securing Mobile Devices in the Enterprise*was released for comment on July 10th, 2012, and includes recommendations for securing personally-owned mobile devices. Later this year, NIST will also release for comment *NIST SP 800-114 Revision 1 (Draft), User's Guide to Telework and Bring Your Own Device (BYOD) Security* which will provide recommendations for securing BYOD devices used for telework and remote access, as well as those directly attached to the enterprise's own networks. NIST is also preparing *NIST SP 800-46 Revision 2 (Draft), Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* which will provide information on security considerations for several types of remote access solutions.

[3]Under the Federal Information Security Management Act of 2002 (FISMA) and related OMB policies and circulars, Agencies are required to follow mandatory standards and guidelines for information and information systems developed by the National Institute of Standards and Technology (NIST). These standards and guidelines should be used throughout the implementation of any BYOD program.

[4] Additional functions of MDM and MAM solutions may include: security (e.g., enforce data-in-transit encryption, data-at-rest encryption, strong authentication); network (e.g., control mobile network access, network roaming, network routing, data import/export, and use of Government gateways); system (e.g., control peripheral (dis)enablement); software (e.g., restrict application installation and force use of enterprise app stores); app store (e.g., centrally store, inspect, and manage distribution of applications); asset management and security compliance audits (e.g., routine / real-time scan of functions against enterprise policies); device jailbreak / rooting detection, system performance monitoring (e.g., processor, memory, storage, battery); peripheral status monitoring (e.g., camera, GPS, network access); device lock (e.g., timeout lock / enterprise lock); remote wipe (e.g., selective wipe / comprehensive wipe); quarantine malware / applications; device (de)activation; device configuration, restoration, or migration of profiles, services, software, policies, and files; active peripheral control (e.g. activate GPS to track lost device); enforced separation of content (e.g., personal, enterprise, classified, tactical); restricted content transfer across domains; enterprise / Web-based partitioning; over-the-air (OTA) provisioning; role/group-based access; enterprise platform integration and certification authority; help desk self-service administration; enterprise dashboard visibility, alerting, logging, troubleshooting; contract, expense, service usage management.