The Business Case for Enterprise Smartphone Security

A White Paper

Winn Schwartau, Mobile Application Development Partners, LLC

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

www.MobileActiveDefense.com

The Smartphone Security Company

The Business Case for Enterprise Smartphone Security

The Smartphone is the new Personal Computer.

The mobile infrastructure is growing faster than any IT development in history because of the consumerization of technology and its integration into the enterprise. [1] *As a result, many high profile private and government organizations are forcing management to seriously examine how it will deploy several hundred million smartphones (iPhones, iPads, Android, Nokia Symbian and Microsoft Windows mobile devices) across their mobile infrastructures and connect with their customers.*

Executive Impact Analysis:
Smartphones as Business Enablers.

Leading business and IT executives instantly recognize the value of the emerging mobile infrastructures. They clearly see the proliferation of smartphones and mobile tablets as profoundly business enabling and an opportunity that cannot be missed.

- Globally, companies are demanding more flexibility and functionality from their mobile workforces. Despite its lower overhead, the mobile enterprise requires just as much security as its fixed network counterparts.
- Corporate users are demanding more than BlackBerrys. From Board members, to company Presidents and C-Level executives and through the workforce ranks, iPhones/iPads and Android driven smartphones and tablets are the mobile platforms of choice.
- Corporate stakeholders understand the vast business-enabling power of a mobile enterprise.
- Companies in all industries are developing mobile Intranets using non-Blackberry custom 'apps' to meet both their internal and customer-facing needs.
- Rogue (unregistered and non-controlled) mobile devices are connecting to enterprises, creating extraordinary security risks. Organizations are falling out of compliance, substantially increasing the risk of both criminal and civil data breaches and privacy violations.
- Enterprises must also contend with nearly four billion users (2013) who want to conduct business with them from their smartphones and laptops. *"Access to mobile banking is growing so rapidly that a substantial percentage of users (39%) are accessing their mobile accounts from home on their Smartphones and handsets rather than their PCs at home."* [2]
- Highly skilled professional criminals are already exploiting mobile technology at an unprecedented rate and will continue to do so with increased vigor.

[1] 1.82 billion smartphones and 1.72 billion mobile PCs by 2013. Gartner

[2] ComScore Mobile Financial Services Market report, July 2009

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)
www.MobileActiveDefense.com
The Smartphone Security Company

- The CISO, CTO and associates stakeholders do not enjoy the luxury of time as they have in the past. The mobile enterprise is here to stay.

Corporate leaders understand that the mobile space offers unprecedented opportunity as well as risk. They also know that privacy, security and compliance are critical to the success of their operations in the U.S. and around the world.

M.A.D. Partners Mobile Enterprise Compliance and Security (MECS) Server is a comprehensive, policy driven solution that enables the enterprise to securely build its mobile enterprise capabilities and outreach, while still maintaining compliance. It provides the same kinds of lock downs and controls organizations apply to their BlackBerry and laptop populations, but extends centralized management over iPhones, iPads, Android, Symbian and Microsoft Mobile platforms. The MECS Solution provides powerful controls across these multiple mobile platforms, thereby enabling the organization to compliantly enable its mobile workforce and business applications, both internal and customer facing.

- Export your existing security, privacy and compliance policies.
- Use Certificates of Authority (CA) based provisioning for mobile devices.
- Install in hours, not weeks or months.

This paper will outline the business case for mobile security, privacy and compliance as a business-enabling technology and a mitigation mechanism for corporate risk.

Market Impact Analysis:

Mobile enterprise management, control, security compliance and reporting.

Many enterprises have resigned themselves to permitting and authorizing users to only use BlackBerry smartphones on their networks, given the nature of the inherent BES security and moreover, policy control. However, many IT, IS Directors and otherwise compliant organizations are plagued with countless rogue mobile devices connecting to and roving on their enterprise, with no visibility, security measures or control and policies. Thus, their well-earned and auditable security and governance is effectively erased.

In fact, as we have been told in more cases than not, enterprise management and their directors actively want to embrace the iPhone/iPad and similar smartphone, but these devices must offer the organization the same breadth of control, reporting, security and compliance as the BlackBerry. Surprisingly, countless organizations permit 'personally liable' (or employee owned) smartphones on their network – regardless of the potential liabilities involved. [3]

[3] As reported by Aberdeen in a recent survey titled "Enterprise Mobility Strategies 2010: More Mobility, Same Budget." - more than two-thirds (73 percent) of respondents indicated that some or all employees were permitted to use personal-liable mobile devices for corporate use.

Aberdeen Group - "Enterprise Mobility Strategies 2010: More Mobility, Same Budget."

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

It is exactly the dual-use capabilities of the smartphone which concerns enterprises that must care about security, privacy and compliance for myriad reasons.

The average employee has multiple email accounts on their smartphone – most of which are not under corporate management, compliance control or accountability. Millions of mobile smartphones connect to corporate equipment and information, potentially exposing companies to threats like phishing, malware, SPAM, and viruses. Depending upon the study, between 67-97% of emails are unwanted and potentially dangerous.

On the other hand, the enhanced flexibility, functionality and open development platforms of the iPhone and Android devices are driving an immediate need for the enterprise to rapidly – and securely – build their mobile infrastructure, sooner than later. As we have learned, the enterprise already fully comprehends the business enabling capability of a secure mobile infrastructure. Building custom applications for the iPhone/iPad and Android platforms offers a simple means to build out both a mobile Intranet and powerful customer experience.

But, most every industry segment that wishes to deploy their unique applications must also adhere to one or more U.S. and international regulatory guideline. See Appendix D for a complete list of U.S. and international compliance guidelines, laws and regulations.

- Internal and external mobile banking, stock trading and other financial transactions. (GLBA)
- Sharing private health data between nurses, doctors, surgeons, radiologists, testing labs, EMTs, hospitals offers incredible enhancement of the medical field. (HIPAA)
- MAD Mobile Enterprise Compliance and Security (MECS) Server supports the critical NIST 800-53 U.S. Federal Government guidance for access control and media storage for mobile devices.
- International standards ISO/IEC 27002 are the basis for countless country and region specific privacy and compliance regulations that mirror those in the U.S. The MECS Solution clearly maps across this highly established set of standards. See Appendix C.
- The retail customer experience is profoundly changing. Clothiers dress virtual shoppers on their tablets within the store and take payment. (PCI)
- Government applications across all disciplines. (FISMA)
- All U.S. publicly traded companies. (SOX)
- Education records. (FERPA)

The IT industry is only in the early life-cycle development stage of the mobile enterprise and how the capabilities discussed will transform the enterprise and the customer experience. Just as we could not have made specific prediction in 1994 on how profoundly the web would transform business, all we can predict about the mobile market today is two facts:

1. The changes will be deep, fast and unpredictable.
2. Any shift to mobility must include strong security, privacy and compliance as an integral part of any deployment.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Mobile Active Defense's MECS (Mobile Enterprise Compliance and Security) Server is a 'compliance umbrella' or 'halo' that was developed with best practices from around the world as our benchmark for features and flexibility. While regulatory bodies and laws have countless nuances and specifics, they all have the same fundamental goal: to protect data, afford privacy and protect the public.

The MECS Server implementation and flexibility allows the administrator of any organization which is subject to one or more compliance regulations, to interpret those rules and enforce them as they see fit. Organizations can then, effectively map existing policy and legal guidelines across the spectrum of the MECS server and define and adjust granularity enforcement across multiple global regions to effect appropriate controls.

Some organizations, however, may not be subject to any specific regulatory compliance guidelines. They, may have, however, already chosen to protect themselves, their employees and clients from intrusion or compromise within their fixed enterprise. Our experience has shown us that the SMB often fits into this middle ground where compliance is not mandated, yet security and privacy are of paramount concern.

Mobile Active Defense and the MECS Server allow the organization to deploy the level of security it chooses, but perhaps more importantly, MECS provides hidden benefits, each with their own non-obvious ROI benefits.

- No one knows when a regulatory body will extend its influence. The SME can find itself suddenly in the position of having to meet stringent guidelines. Instead of additional expense and rearchitecting, Mobile Active Defense prepares the company for most if not all compliance contingencies, especially since MECS Server feature sets will be continuously upgraded as needed.
- When companies grow in size, certain laws and regulations that had not previously affected the security posture of the company, will come into play. Corporate executives that are planning for the future can well prepare their company by using MECS Servers, the best in class mobile enterprise solution, making IT and security or compliance growth painless. The company can then concentrate on its core business.
- In an era of M&A (Mergers and Acquisitions), the security aware organization that has planned for security contingencies and its potential M or A, makes itself a more valuable entity. Integrating IT departments can be an excruciating exercise, but if a standards and compliance guidelines based company has planned for its future, the costs associated with corporate mergers decreases, thereby increasing its financial value. Mobile Active Defense allows the rapid scaling and integration of disparate operating groups into its centralized management platform.

Each of these growth path decisions will generate its own ROI based upon size of enterprise, sense of security and privacy, and growth plans.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Technical Impact Analysis:

The threats are real.

The threat landscape is vastly different than when prior generations of technology were introduced. The mobile threats are of direct and immediate concern to any security-aware and compliance driven organization, regardless of industry sector.

Today's hostile actors are sophisticated, well financed, highly technical and patient. Through two decades of effective and profitable hostile acts and experience, organized crime around the world is a very real threat to the enterprise in its fixed locations, but more so to the emerging mobile infrastructure. These risks to the privacy, security and compliance of the enterprise are even more profound to its mobile components, especially since too many companies allow rogue, non-compliant smartphones to connect, store, communicate and process proprietary and regulated data.

The threats to the mobile enterprise are largely reduced to two primary vectors.

1. Email. Attachments are well-known infection carriers, regardless of the targeted platform. Phishing, spam and scams attract and encourage poor behavior on the part of the user, thus permitting other paths of infection and corporate data breaches. As smartphones connected to the enterprise have potentially several personal and uncontrolled email accounts in addition to one or more corporate accounts, the threat of an unsecure path to company networks has substantially increased. Smartphones do not scan adequately for viruses, malware, phishing attacks, adware and spam. They do not differentiate between the sensitivity of the data in personal and business accounts, nor do they provide isolation, discretionary access control, filtering or monitoring. These risks have been clearly demonstrated over the past twenty years to be unacceptable to the CISO, CTO or risk adverse management.

2. Apps are the greatest hostile software delivery system invented by man. Without appropriate controls, smartphone users may choose to download apps from iTunes or from other open-source third party app stores. As of today, there is no means to implement code review and evaluation of the efficacy of the underlying and hidden operation of the app. Apple evaluates 'advertised function' and does not implement security-driven code review. Other third part app stores are worse, with an estimated 20% of all apps already containing hostile or unwanted software. The compliant enterprise cannot permit such an egregious security lapse to exist in either its fixed or mobile enterprise, and thus is compliance-required to control mobile app download, deployment and usage.

- The first mobile 'botnet' was discovered in July 2009 by researchers at security firm, Trend Micro.
- By the first half of 2009, one in 63 smartphones was infected with mobile spyware and malware, according to a July, 2009 study of nearly 2,000 smartphone users.
- More and more people are being tricked into going to malicious web sites with their smartphone browsers, as well as being scammed directly on their phones[4].

[4] Fierce Mobile Content, Jan 2010

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

- The iPad has already been rooted (taken over by hostile code).[5]
- "Smartphones are essentially becoming regular computers," says Vinod Ganapathy, computing professor at Rutgers University in New Jersey. "They run the same class of operating systems as desktop and laptop computers, so they are just as vulnerable to attack by malware."[6]
- OSX and Android are a bonanza for hackers and malicious software engineers.[7]
- An Australian student created an experimental worm that hop-scotched across "jailbroken" iPhones, which are phones altered to run software Apple has not authorized.[8]
- Infecting a business network can be achieved when a user syncs an infected smartphone to his desktop or business laptop computer which is connected to an enterprise network. Such security breaches violate policy, compliance and regulatory guidelines and create the very real risk of data breaches through another path.

MECS Servers solve such unacceptable risks by instituting mobile enterprise controls and network security measures that first and foremost 'lock down' the phone under enterprise management and control. Using CA-based authentication at the MECS Server, all smartphone traffic is routed over encrypted tunnels to the MECS enterprise-grade management and control system. All data is scanned, reviewed according to enterprise policy and remediated as required. To enforce policy to the greatest extent possible, especially to echo existing security posture, the MECS granular firewall offers a familiar suite of controls and interface, thereby eliminating the need for complex programming or administrative learning curves. The smartphone becomes 'invisible' to the Internet, creating a secure, private and compliant mobile intranet.

With the inherent limitations of single user, non-multi-tasking and non-auto-start mobile environments, security cannot be pushed to the iPhone as it done on traditional computing devices using Windows, OS X or Linux. With M.A.D., the 'lock down' of the iPhone and other mobile devices is so strong that the user cannot escape or turn off the trusted shell it is locked into. All data is directed through the MECS Server so the company is in complete control of the device and the data.

M.A.D also gives the administrator a range of remediation options to handle security, privacy and compliance exception events. Jailbreaking of an iPhone/iPad on a corporate network, for example, is detected by M.A.D.'s controls, enabling the administrator to pick a remediation path within minutes.

It is critical for the reader to understand that Mobile Active Defense and the MECS Server is unique in its ability to truly lock down devices to the extent required by the security-aware and compliance regulated organization – while not changing the user experience or causing any noticeable latency whatsoever.

There are a number of companies who claim to offer 'device management' and this has become exceedingly misleading to the CISO and CTO. Apple's iOS4 (operating system for the iPhone and iPad) includes MDM,

[5] http://www.theregister.co.uk/2010/02/23/smartphone_rootkits_demoed/
[6] http://www.theregister.co.uk/2010/02/24/mobile_network_security_threats/
[7] http://247wallst.com/?s=Hackers+To+Hit+Apple+iPhone%2C+Google+Android+Handsets+Next+Year
[8] http://www.emailsecuritymatters.com/site/blog/email-security/anti-spam-hacking-and-virus-security-how-will-smartphones-survive/

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)
www.MobileActiveDefense.com
The Smartphone Security Company

Mobile Device Management. In combination with Active Sync, a small set of device management tools is included:[9]

- Password management
- PIN/password lock
- Remote wipe
- Active Sync
- Device Encryption

Device management is not security, does not provide privacy nor does it begin to approach the controls needed for compliance. Google offers a simple free version with a managed user interface for Apple's MDM, while Good, Trust Digital (McAfee) and MobileIron offer fee-based versions with marginally more functionality. Customer feedback is that these approaches are substantially less than adequate for even minimal protection, notably because Apple's design explicitly allows the user to turn off MDM, thereby obviating any device management at all.

We at M.A.D. Partners, LLC can confidently say that at this juncture, there is no other solution or approach to the mobile enterprise compliance problem. For a company to settle for such an anemic approach to data protection, they would also need to be willing to turn off all security controls from their BlackBerrys and their laptops. How many CISOs will sign off on that?

Operational Impact Analysis:

So what if?

Information security and information technology is always a delicate balancing act between ease of use, functionality, business need, risk and of course cost/benefit. So, what if you could finally have your secure mobile enterprise cake and eat it, too? The following scenarios are based upon real-life experiences.

- **Scenario 1**
    - You are a BlackBerry shop, have rogue iPhones (and other smartphones) that are invisible to your network, thus you have no control over them. Personal email use by employees on those devices is also outside of your control.
    - As a corporation, you want to offer employees the option of using smartphones, but they must be secured, controlled and owned by the organization
    - M.A.D.'s advantages are compliance through granular role based policy control, security, compliance and visibility, just like BlackBerry's BES. A single management console for all other platforms.

[9] See Mobile Enterprise ActiveSync/iPhone Product Comparison data sheet. www.MobileActiveDefense.Com

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

- **Scenario 2**
    - You allow employees to access company email from their own smartphones. As a result, you have little or no visibility of the devices, nor control over their security or usage, thus you now have a violation of company policy.
    - Rogue mobile devices are connecting to your networks with no controls in place over the device or the data.
    - To manage risk, limit breach and privacy breaches and for budgetary reasons, you want to keep your current policy of letting employees use their own smartphones. You also recognize the need for policy control and security because those devices and data communicate with your network
- **Scenario 3**
    - You are primarily a BlackBerry shop and have discovered a population of rogue iPhones (and other smartphones) on your network. You recognize you need some control over them, but you do not want to provide company owned devices.
    - This is the 'If you can't beat them, join them' scenario. You cannot stop this behavior, but you need to manage your risk by including these devices in a policy-controlled environment – just as you enjoy with BES now.
- **Scenario 4**
    - Your company is highly mobile and you require sharing of data (email, company and or customer information) between your mobile and fixed networks. You understand that this increases the risk of breach and falling out of compliance.
    - This is the real world today and you understand that the devices and data must be controlled in similar manners throughout your organization.
- **Scenario 5**
    - Your company is developing unique mobile applications for internal and/or external use. To make these applications useful and business enabling, they must have access to and manipulate sensitive information.
    - Most industries must adhere to compliance regulations over data flow and protection, thus requiring both the devices and the information to meet those guidelines.
- **Scenario 6**
    - Your company has controls in place to handle security events, breaches and other incidents within your fixed infrastructure.
    - You also know you need to have similar event detection, notification, escalation and remediation throughout your mobile enterprise.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Each of the above scenarios is real, and many organizations are currently challenged by more than one of them. In each case, you will notice both the problems and solutions approaches overlap and are highly intertwined.

Each of the above scenarios is solved by the rapid application of the MECS Server across the organization's mobile population.

- Rogue phones are immediately taken off the network.
- The Administrator will register only those phones the company wants connected.
- The level of security provided by BES will be effectively duplicated across the rest of your smartphone population.
- Your company will enjoy the immediate creation of a secure, private and compliant mobile intranet.
- Your unique mobile apps will operate under compliant controls and management.
- You will be able to detect and remediate security threats and breaches by high-speed detection and notification, including jailbreaking (iPhone/iPad).

Financial Impact Analysis:

What is all of this really costing you now? TCO, risk and cost benefit?

According to a recent Gartner study, managed mobile devices have significantly lower TCO (by 53% to 63%) than unmanaged devices.[10] Enterprise resources often end up supporting employees who are using unsanctioned and rogue mobile devices. The time, effort and costs associated with this 'out of band' and unbudgeted assistance are significant as planning, procedures, training and tools are not in place to help an enterprise IT support team properly address issues.

- If it costs $500 per year to handle an unmanaged population of 500 phones, ($250,000), the company can enjoy a savings of between $132,500 and $157,500 by choosing to implement M.A.D. and the MECS Solution for its mobile population.

Conversely, when IT Managers are able to provide proper mobile device management, they can predict what resources, skill sets, procedures, policy and infrastructure are needed to ensure proper service levels and security compliance - within their budgets. Smartphones must be treated as another computing device or TCO will soar. As Strategy Analytics puts it "Mobility management in the enterprise must encompass a life-cycle approach, mimicking a traditional IT computing strategy."[11]

[10] Four TCO Profiles for Smartphones and PDAs: 2009 Update - 19 October 2009 Federica Troni, Ken Dulaney Gartner RAS Core Research Note G00171705

[11] Measuring the Value of Mobile Device Management – Philippe Winthrop, Strategy Analytics, 30, November 2009

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Enterprises also are able to enjoy substantial operational savings in the mobile space in distinction to the fixed environment. The cost per seat – overhead – is substantially less when exporting existing policy to a mobile workforce than by attempting to create and manage unique policies.

- Examine existing fixed enterprise device control costs. Mobile device control and management costs will be less because the company has already developed and deployed a policy.
- M.A.D. and the MECS Server is the only cost.
- The administrator exports existing policy that is immediately deployed across the registered phone population.

In evaluating risks of deploying a mobile enterprise, the organization has sufficient data to make proper decisions that will positively affect the company instead of creating substantial risk. The cost to the enterprise of falling out of compliance by allowing rogue devices or choosing not to implement proper controls can be extreme as is evidenced by the crackdown by regulatory bodies.

The enterprise needs to identify its compliance requirements for devices and data under its purview – and thus, its control. Many enterprises have already performed an extensive and costly review of the risks associated with:

- 1st generation mobile phone, vis a vis, the BlackBerry.
- Laptops running Windows, OS X and Linux.

In both cases, the results of such analyses were the same: the mobile devices must meet certain levels of security and privacy to meet compliance guidelines and not violate the laws of their particular jurisdiction. See Appendix D for a detailed list of U.S. and international privacy, security and compliance guidelines.)

The enterprise, therefore, does not have to conduct a new risk and financial impact analysis. It has already been done. The organization need only ask one question: *"Are we willing to accept the risk and place non-compliant devices into our mobile enterprise, even though our BlackBerrys and laptops are properly controlled?"*

M.A.D. and the MECS Server allow the enterprise the luxury of, almost overnight, extending the same level of security and compliance their BES provides, across the other four major smartphone platforms.

Appendix A, the Mobile Enterprise Compliance and Privacy Chart, allows the company to compare its current security posture to its growing mobile one.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Solutions Impact Analysis:

It's not only BlackBerry anymore

Recognizing the organizational need for BlackBerry-like control over iPhones, all other smartphones and the mobile enterprise, Mobile Active Defense and the MECS Server is a unique technology that solves the problems outlined herein.

Traditional PC/laptop security approaches require substantial resource utilization; processes, cycles, RAM and storage, straining performance and often creating operational conflicts. With Mobile Active Defense, a Zero Footprint on the mobile device pushes all of the security and compliance controls to a centrally managed console requiring no day-to-day intervention or participation on the part of the user.

In addition, all security controls, profiles and filters are updated 100 times every day, yet there is no bandwidth consumed in the last mile or resources used on the mobile device. This ensures that the mobile workforce always has the latest protection available against the newest threats and remains in compliance at all times. Breach detection results in immediate remediation capability on the part of the administrator. Between native Active Sync and MDM communicating with the centralized policy enforcement capabilities of the MECS Server, jailbreaking and other violations can be detected in less than a minute and remediated by the administrator.

With M.A.D.'s Managed Security Service, small to medium enterprises can outsource the hosting and management of their mobile enterprise knowing that the risks are being mitigated constantly. Some organizations, however, will prefer to house their own MECS Sever and Enterprise Compliance and Enforcement Management Console within their own networks. In either case, M.A.D. will be protecting their mobile enterprise in just a few hours.

We do the rest.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Appendix A

Mobile Enterprise Compliance and Privacy Chart

The following chart will clearly show the enterprise the mapping between their existing secure and compliant network and their proposed mobile one. Organizations with whom we have spoken are not willing to take the risk of criminal or civil compliance or privacy violations at any point in their enterprise. Thus, they have been routinely rejecting the minimal management capabilities of Good or Mobile Iron. Good is simply not good enough for the enterprise.

Enterprises have determined that the only appropriate way to build out a mobile enterprise on both a business and risk level is to mirror their current capabilities. M.A.D. and the MECS Server is the most potent and capable solution at their disposal.

	What is the posture of your existing network?	What is the posture of your existing network?	What is the posture of your existing network?		What would you like in your Mobile Network?	What would you like in your Mobile Network?
	Fixed/Internal	Laptop/Mobile	Blackberry-BES		iPhone/iPad	All Other Smart Phones
COMPLIANCE						
What are your commpliance requirements? (HIPAA, PCI, etc.)						
Do you meet them?						
Are you subject to regulatory reviews? When is your next one?						
Is compliance reviewed by internal, external reviews or both?						
Do you want to maintain compliance for this portion of your networks?						
	Yes/No?	**Yes/No?**	**Yes/No?**		**Yes/No?**	**Yes/No?**
VPN on at all times?						
CA Based?						
Policy Driven Controls in Place						
Stateful Inspection Firewall to manage each device?						
Anti-virus scanning?						
Malware and phishing detection and removal?						
Spam removal?						
Blacklisting URLs?						
Whitelisting URLs?						
Content Filtering?						
Controls Dual Homing?						
Role Based Controls?						
Can Users Bypass Security Controls?						
How many security updates are performed daily?						
Block unauthorized devices?						

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

www.MobileActiveDefense.com

The Smartphone Security Company

Appendix B

(MECS) Compliance with United States Federal Government Guidelines NIST 800-53

NIST 800-53

MAD Mobile Enterprise Compliance and Security (MECS) Server supports the critical 800-53 guidance's for access control and media storage for mobile devices.

ACCESS CONTROL SETTINGS:

- Restrict the use of writable, removable media in organizational information systems.
- Prohibits the use of personally owned, removable media in organizational information systems.
- Prohibits the use of removable media in organizational information systems when the media has no identifiable owner
- Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting classified information:
    - Connection of unclassified mobile devices to classified information systems is prohibited;
    - Connection of unclassified mobile devices to unclassified information systems requires approval from the appropriate authorizing official(s);
    - Use of internal or external modems or wireless interfaces within the mobile devices is prohibited

MEDIA STORAGE

- Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MEDIA TRANSPORT

- Maintains accountability for information system media during transport outside of controlled areas; and
- Restricts the activities associated with transport of such media to authorized personnel.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Appendix C
M.A.D. Enterprise Compliance and Security Server (MECS)
ISO 27001 Controls

ISO 27001 CONTROLS
MAD Mobile Enterprise Compliance and Security Server (MECS) support the critical ISO 27001 access control guidance for mobile devices, and maps directly to both PCI and SOX.

ACCESS CONTROL SETTINGS:
- Restrict the use of writable, removable media in organizational information systems.
- Prohibits the use of personally owned, removable media in organizational information systems.
- Prohibits the use of removable media in organizational information systems when the media has no identifiable owner
- Enforces the following restrictions on individuals permitted to use mobile devices in facilities containing information systems processing, storing, or transmitting confidential information:
    - Connection of mobile devices to classified information systems is prohibited

MEDIA STORAGE
- Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

MEDIA TRANSPORT
- Maintains accountability for information system media during transport outside of controlled areas; and
- Restricts the activities associated with transport of such media to authorized personnel.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

Appendix D

International Laws

The following list contains a number of international privacy related laws by country and region. Wherever possible, these hyperlinks reference an English translation of the law. See also our list of U.S. Privacy Laws.

- **Argentina:** Personal Data Protection Act of 2000 (aka Habeas Data)
- **Austria:** Data Protection Act 2000, Austrian Federal Law Gazette part I No. 165/1999 (Datenschutzgesetz 2000 or DSG 2000).
- **Australia:** Privacy Act of 1988
- **Belgium:** Belgium Data Protection Law and Belgian Data Privacy Commission Privacy Blog
- **Brazil:** Privacy currently governed by Article 5 of the 1988 Constitution.
- **Bulgaria:** The Bulgarian Personal Data Protection Act, was adopted on December 21, 2001 and entered into force on January 1, 2002. More information at the Bugarian Data Protection Authority
- **Canada:** The Privacy Act - July 1983
  Personal Information Protection and Electronic Data Act (PIPEDA) of 2000 (Bill C-6)
- **Chile:** Act on the Protection of Personal Data, August 1998
- **Colombia:** Two laws affecting data privacy - Law 1266 of 2008: (in Spanish) and Law 1273 of 2009 (in Spanish) Also, the constitution provides any person the right to update their personal information
- **Czech Republic:** Act on Protection of Personal Data (April 2000) No. 101
- **Denmark:** Act on Processing of Personal Data, Act No. 429, May 2000.
- **Estonia:** Personal Data Protection Act of 2003. June 1996, Consolidated July 2002.
- **European Union:** European Union Data Protection Directive of 1998
- EU Internet Privacy Law of 2002 (DIRECTIVE 2002/58/EC) With a discussion here.
- **Finland:** Act on the Amedment of the Personal Data Act (986) 2000.
- **France:** Data Protection Act of 1978 (revised in 2004)
- **Germany:** Federal Data Protection Act of 2001
- **Greece:** Law No.2472 on the Protection of Individuals with Regard to the Processing of Personal Data, April 1997.
- **Guernsey:** Data Protection (Bailiwick of Guernsey) Law of 2001
- **Hong Kong:** Personal Data Ordinance (The "Ordinance")
- **Hungary:** Act LXIII of 1992 on the Protection of Personal Data and the Publicity of Data of Public Interests (excerpts in English).
- **Iceland:** Act of Protection of Individual; Processing Personal Data (Jan 2000)
- **Ireland:** Data Protection (Amendment) Act, Number 6 of 2003
- **India:** Information Technology Act of 2000
- **Italy:** Data Protection Code of 2003
  Italy: Processing of Personal Data Act, January 1997
- **Japan:** Personal Information Protection Law (Act) (Official English Translation)
  Law Summary from Jonesday Publishing
- **Japan:** Law for the Protection of Computer Processed Data Held by Administrative Organs, December 1988.
- **Korea** - Act on Personal Information Protection of Public Agencies Act on Information and Communication Network Usage
- **Latvia:** Personal Data Protection Law, March 23, 2000.
- **Lithuania:** Law on Legal Protection of Personal Data (June 1996)

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)

- **Luxembourg:** Law of 2 August 2002 on the Protection of Persons with Regard to the Processing of Personal Data.
- **Malaysia** - Common Law principle of confidentiality Draft Personal data Protection Bill (Not finalized) Banking and Financial Institutions Act of 1989 privacy provisions.
- **Malta:** Data Protection Act (Act XXVI of 2001), Amended March 22, 2002, November 15, 2002 and July 15, 2003
- **Morroco:** Data Protection Act
- **Netherlands:** Personal Data Protection Act 2000
- **New Zealand:** Privacy Act, May 1993; Privacy Amendment Act, 1993; Privacy Amendment Act, 1994
- **Norway:** Personal Data Act (April 2000) - Act of 14 April 2000 No. 31 Relating to the Processing of Personal Data (Personal Data Act)
- Philippines: No general data protection law, but there is a recognized right of privacy in civil law.
- **Romania:** Law No. 677/2001 for the Protection of Persons concerning the Processing of Personal Data and the Free Circulation of Such Data
- **Poland:** Act of the Protection of Personal Data (August 1997)
- **Portugal:** Act on the Protection of Personal Data (Law 67/98 of 26 October)
- **Singapore** - The E-commerce Code for the Protection of Personal Information and Communications of Consumers of Internet Commerce. Other related Singapore Laws and E-commerce Laws .
- **Slovak Republic:** Act No. 428 of 3 July 2002 on Personal Data Protection.
- **Slovenia:** Personal Data Protection Act , RS No. 55/99.
- **South Korea:** The Act on Promotion of Information and Communications Network Utilization and Data Protection of 2000
- **Spain:** ORGANIC LAW 15/1999 of 13 December on the Protection of Personal Data
- **Switzerland:** The Federal Law on Data Protection of 1992
- **Sweden:** Personal Data Protection Act (1998:204), October 24, 1998
- **Taiwan:** Computer Processed Personal data Protection Law - applies only to public institutions.
- **Thailand:** Official Information Act (1997) for state agencies. (Personal data Protection bill under consideration.)
- **United Kingdom:** UK Data Protection Act 1998
  Privacy and Electronic Communications (EC Directive) Regulations 2003 official text, and a consumer oriented site at the Information Commissioner's Office.
- **Vietnam:** The Law on Electronic Transactions 2008

United States Laws

The following list contains a number of United States federal and state laws that have provisions for data privacy. Also see our list of International Privacy Laws. Organizations can save time and money maintaining compliance these privacy regulations using the Privacy Management Toolkit.

PCI: The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits the merchant. Just one TJX violation cost the company $880,000.

HIPAA: HIPAA calls for civil and criminal penalties for privacy and security violations, including: -- fines up to $25K for multiple violations of the same standard in a calendar year - fines up to $250K and/or imprisonment up to 10 years for knowing misuse of individually identifiable health information. Providence Health and Services was fined $100,000 in 2008. The California Department of Public Health has fined five hospitals a total of $675,000 for failing to prevent unauthorized access to confidential patient medical information.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)
www.MobileActiveDefense.com
The Smartphone Security Company

GLBA: Non-compliance of GLBA can result in a variety of fines and up to 5 years imprisonment for each violation. "The financial institution shall be subject to a civil penalty of not more than $100,000 for each such violation," and "the officers and directors of the financial institution shall be subject to, and shall be personally liable for, a civil penalty of not more than $10,000 for each such violation." Kaiser Permanente Bellflower was fined $250,000 for one violation alone.

SOX: Can be fined and be imprisoned for not more than 20 years. Ford was fined $20M in 2005 as one example of SOX violation enforcement.

- Americans with Disabilities Act (ADA) - Primer for business.
- Cable Communications Policy Act of 1984 (Cable Act)
- California Senate Bill 1386 (SB 1386) - Chaptered version.
- Children's Internet Protection Act of 2001 (CIPA)
- Children's Online Privacy Protection Act of 1998 (COPPA)
- Communications Assistance for Law Enforcement Act of 1994 (CALEA) - Official CALEA website.
- Computer Fraud and Abuse Act of 1986 (CFAA) law summary. Full text at Cornell
- Computer Security Act of 1987 - (Superseded by the Federal Information Security Management Act (FISMA)
- Consumer Credit Reporting Reform Act of 1996 (CCRRA) - Modifies the Fair Credit Reporting Act (FCRA).
- Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003 law overview. Text of law at Cornell library
- Electronic Funds Transfer Act (EFTA) Summary
- Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Fair Credit Reporting Act (Full Text).
- Federal Information Security Management Act (FISMA)
- Federal Trade Commission Act (FTCA)
- Driver's Privacy Protection Act of 1994 . Text of law at Cornell
- Electronic Communications Privacy Act of 1986 (ECPA)
- Electronic Freedom of Information Act of 1996 (E-FOIA) Discussion as it related to the Freedom of Information Act.
- Fair Credit Reporting Act of 1999 (FCRA)
- Family Education Rights and Privacy Act of 1974 (FERPA; also know as the Buckley Amendment)
- Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA)
- Privacy Act of 1974 - including U.S. Department of Justice Overview
- Privacy Protection Act of 1980 (PPA) - Additional discussion at http://www.epic.org/privacy/ppa/.
- Right to Financial Privacy Act of 1978 (RFPA)
- Telecommunications Act of 1996
- Telephone Consumer Protection Act of 1991 (TCPA) - Text of law at http://www.law.cornell.edu/uscode/47/227.html
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)
- Video Privacy Protection Act of 1988 discussion and overview. Text of law at: Cornell Law Library.

3399 Peachtree Road NE · Suite 400
Atlanta, GA 30326 · USA
1.877.halo.mad (425.6623)