

# Mobile First Government

MobileIron enables the federal government to support an increasingly mobile workforce. With MobileIron, government agencies can ensure protection of sensitive data on agency-issued and employee-owned mobile devices while enhancing the productivity of their workforce and ultimately becoming more responsive to the citizen community. MobileIron enables government agencies to use mobile technologies to support their forward-facing missions and optimize their operations.

Mobility plays an increasingly important role in today's federal government agencies. The always-available access to mobility and the overflow of work into personal lives have pushed mobile devices to the forefront. Enabling email alone is no longer enough; full productivity depends on real-time access to applications and files and the ability to share data or collaborate anywhere at any time.

To empower the mobile workforce, government agencies are moving towards mobile computing and telework, which helps them to shift work to the optimal location, time and resource. As workplace mobility increases, many agency employees are now using mobile devices such as smartphones and tablets to complete their work.

MobileIron helps government agencies proactively create an agile and secure infrastructure that supports a multi-device multi-OS environment. Ensuring security and compliance is paramount for any federal agency, and MobileIron helps them build a secure infrastructure that will enable them to become both Mobile First and Cloud First.

## Secure Agency Devices

The days when Blackberry was the only device used by government employees are long gone. Now workers use both agency-owned and personal devices to access government/agency email, which is causing a shift in agency attitudes toward mobility. But as employees leverage workarounds such as free file sharing services to accomplish a mission or improve productivity, they unknowingly put their agencies at risk for a cyber attack or data breach. Therefore, device security must be at the heart of any federal enterprise mobility strategy. Left unmanaged and unsecured, an agency's fleet of mobile devices becomes an open gateway to its network and most sensitive data.

MobileIron helps federal agencies secure and manage data on any device across multiple operating systems such as iOS, Android and Windows Phone. MobileIron technology secures corporate email and email attachments by providing automatic device configuration, certificate-based security, and selective wipe of enterprise data for both corporate and user-owned devices. With secure email, application and content delivery, agencies can deliver the right resources to users securely while preserving the device's native user experience.

## Benefits:

- Securely access agency email on any device with a native experience
- Secure ruggedized devices
- Enable field operations, including front-line missions
- Reduce asset costs by supporting employee-owned devices
- Securely push government apps to all employee devices
- Securely collaborate among team members
- Support government regulations, including CJIS, NSA Commercial Solutions for Classified Program Components List (CSfC), NIAP MDM-PP, FIPS 140-2 (3PAO certified), HIPAA, SOC2 Type 2 and Government Records Initiative

*“ Mobility Vision: A highly mobile workforce equipped with secure access to information and computing power anywhere at anytime for greater mission effectiveness.”*

[DoD Mobile Device Strategy](#)

## Secure Sensitive Apps and Content

All government agencies are required to meet various federal mandates regarding security, mobility and high availability. As new mobile workflows are introduced to meet these mandates, devices and access points need to be tightly managed to ensure that government data remains secure. Any security breach attracts heavy fines, in addition to compromising citizen and sensitive data.

While delivering email through a secure client with a native experience is a start, it is not enough. MobileIron helps federal agencies not only manage devices and deliver email securely, it also provides secure access to sensitive data. In addition, MobileIron's Content Security Service, ensures that agencies can provide document-level security across multiple business and personal cloud content repositories, which in turn assures greater compliance to regulations such as HIPAA etc. Built-in activity tracking and compliance tools ensure that agencies stay in compliance with the Government Records Directive, which requires agencies to capture and record all audit trails.

## Mobilize Field Operations

Mobile devices enable all types of field workers, from field census workers to FEMA employees to military personnel in front-line missions, access applications seamlessly and improve productivity, response time and reporting from the field. But without a robust solution to ensure that security is not compromised, adoption of mobility will be difficult.

MobileIron helps government agencies empower their field workforce to do their jobs more effectively. In addition to providing a comprehensive security solution, MobileIron also provides workflow enhancement features such multi-user support, which can be used to save on asset costs in the field, as well as innovate new business workflows. For example, federal aviation departments can employ secure tablets managed by MobileIron to access flight book information, which not only reduces air carrier weight, but also enables the agency to provide real-time updates to the devices.

## Bring Your Own Device (BYOD)

Beyond government mandates and directives, many federal agencies are looking at BYOD as a means to achieve capex savings and reduce IT support costs while giving their employees choice in selecting their mobile devices. With BYOD, agencies must ensure that mobile devices can securely access government data and applications while preserving personal content and maintaining employee privacy. To simplify management across the many operating systems and device types, agencies need a single EMM solution that will secure all their mobile devices.

MobileIron has demonstrated innovation by obtaining patents for BYOD privacy technology that allow for selective wipe and management of mobile device data in an enterprise environment. In addition, MobileIron offers zero-day support for the latest OS and related mobility updates. MobileIron's EMM platform helps federal agencies manage and support all device types in their organization, giving employees choice and freedom while giving IT confidence that sensitive data will be secure. With its containerized approach to delivering applications and content across multiple mobile OS vendors, MobileIron ensures that personal data is left untouched, while agency/government data is never compromised.

“*With MobileIron's secure, scalable platform the USDA can move ahead with its mobility initiatives confident that its mobile apps, data, and devices are secure.*”

Jay Sunny Bajaj, Founder and CEO, DMI

## About MobileIron

MobileIron enables federal agencies to create an agile and secure infrastructure that supports a multi-device, multi-OS environment. MobileIron is the first company in the world to receive [Common Criteria certification](#) against Version 2.0 of the Mobile Device Management Protection Profile (MDMPP V2.0 and MDMPP Agent V2.0) from the National Information Assurance Partnership (NIAP). In August, the MobileIron Core platform received [Security Technical Implementation Guide \(STIG\)](#) approval from the Defense Information Systems Agency (DISA). MobileIron was also the only mobility specialist to be recognized by Government CIO Outlook as one of the [Top 20 Homeland Security Solution Providers 2016](#).

MobileIron's FIPS 140-2 cryptographic libraries are certified by a third-party Cryptographic and Security (CST) laboratory to be in full compliance with the Cryptographic Module Validation Program (CVMP). MobileIron has also partnered with Entrust Datacard to support Derived Credentials on the mobile device to help support secure login while accessing sensitive information from their mobile device. MobileIron enables agencies to build a secure infrastructure that will help them create a Mobile First and Cloud First government agency.

**For More Information**, please visit  
[www.mobileiron.com/government](http://www.mobileiron.com/government)  
or contact us at  
[globalsales@mobileiron.com](mailto:globalsales@mobileiron.com)