Lookout

Whitepaper

Lookout for Federal agencies

Compliance considerations for mobile devices

Lookout for Federal agencies

Compliance considerations for mobile devices

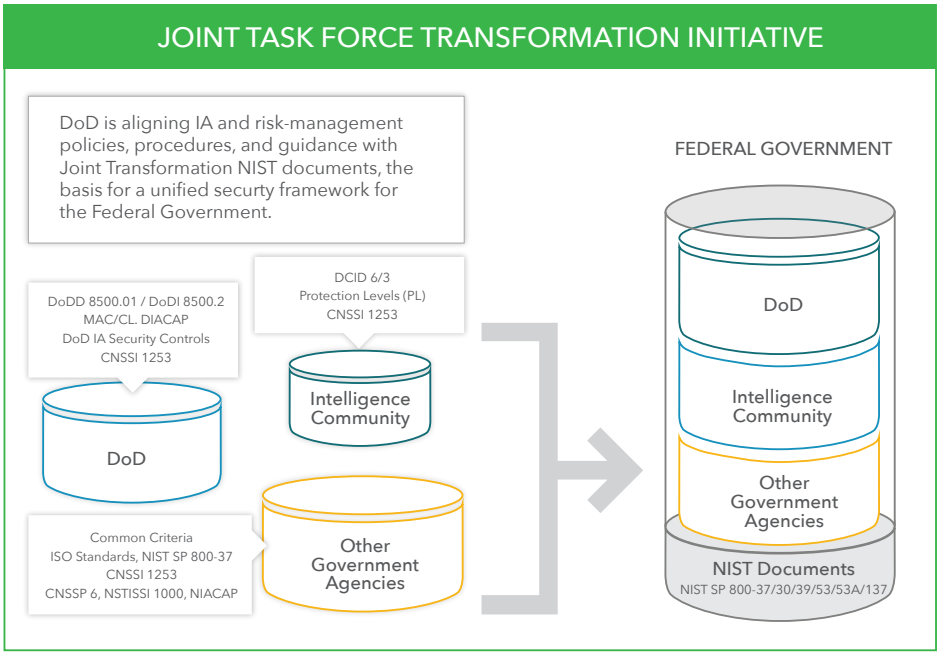
Federal agencies are now creating formal mobility programs as employees increasingly rely on their mobile devices for everyday life. Restricting mobile devices from the workplace also runs the risk of "Shadow BYOD", whereby employees find ways to access work documents on their mobile devices despite restrictions. In fact, a recent survey conducted by Lookout revealed that for employees at Federal agencies with rules prohibiting smartphones at work, 40% said those rules had no impact on their behavior .[1]

This move towards a mobile-enabled Federal workplace has prompted new standards and guidelines for securing data on these devices. In this document, we review the latest guidelines related to securing mobility and how Lookout helps Federal agencies stay compliant with these new guidelines.

Quick overview of Federal information security

Information security at federal agencies is driven by key mandates, including the Federal Information Security Management ACT of 2002, or FISMA. FISMA created a framework of security requirements based on continuously evolving standards, and federal agencies must comply with these rules and report on the effectiveness of their IT security programs to the OMB and Congress.

The Department of Defense also requires all DoD-owned or controlled information systems to submit to the Defense Information Assurance Certification and Accreditation Process (DIACAP). However, DIACAP has recently been replaced by the "Risk Management Framework (RMF) for DoD Information Technology (IT)". This dynamic process requires DoD agencies and commands to review and update their information assurance posture annually. The DoD RMF aligns with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF).



[1] "Feds: You have a BYOD program whether you like it or not", Lookout 2015

Standards and Guidelines related to securing mobile devices

NIST 800-53

Overview:

The purpose of NIST Special Publication 800-53 is to provide guidelines for selecting security controls for information systems supporting federal agencies. The guidelines apply to all components of an information system that process, store or transmit federal information.

Who does NIST 800-53 apply to?

The catalog of security controls outlined in NIST 800-53 applies to all U.S. federal information systems except those related to national security.

Are there specific guidelines related to mobile devices?	
ID	**Key Quotes**
SI-3	The organization employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code. Entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices
SI-7	The organization employs integrity verification tools to detect unauthorized changes to software (including operating systems) and firmware

How does Lookout help with NIST 800-53 compliance?

MALICIOUS CODE PROTECTION: NIST requests that malicious code protection mechanisms exist at information system entry and exit points, specifically noting mobile devices. Lookout protects against malicious code targeting mobile devices such as smartphones and tablets.

As mobile devices increasingly become a productivity tool for employees, the amount of sensitive data passing through these endpoints is on the rise, with attackers increasingly targeting these devices with malicious code.

Lookout protects both iOS and Android devices against the rise of app-based threats including trojans, spyware, and sideloaded applications. Lookout also protects against network-based attacks that attempt to access encrypted data-in-transit by executing a “man-in-the-middle attack.” As mobile devices increasingly connect to unverified Wi-Fi access points at home and abroad, Lookout helps agencies stay compliant by providing network protection on mobile devices that aren’t addressed by VPNs.

DETECTION OF TAMPERING WITH OPERATING SYSTEMS AND FIRMWARE: Lookout detects anomalies within the operating system and firmware to determine if any tampering has taken place that could indicate either a malicious attack (such as Android threats that root the device) or user-initiated tampering (such as jailbreaking their device).

DOD Instruction 8500.2

Overview:

Outlines the controls from the DoD Information Assurance Certification and Accreditation Process (DIACAP), which is a United States Department of Defense (DoD) process that means to ensure that companies and organizations apply risk management to information systems.

Who does DoD Instruction 8500.2 apply to?

The catalog of security controls outlined here apply to agencies within the Department of Defense.

Are there specific guidelines related to mobile devices?	
ID	**Key Quotes**
ECVP-1	"All Servers, workstations and mobile computing devices (i.e. laptop, PDAs) implement virus protection that includes a capability for automatic updates"
ECAT-2	An automated, continuous on-line monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential IA implications, and with a user configurable capability to automatically disable the system if serious IA violations are detected.

How does Lookout help with DoD Instruction 8500.2 compliance?

VIRUS PROTECTION: This instruction requires virus protection on all "all servers, workstations, and mobile computing devices" that have the capability for automatic updates.

Lookout protects both iOS and Android devices against the rise of app-based threats including trojans, spyware, and rootkits. Attacks targeting mobile devices are on the rise, with Android devices seeing a strong increase in malware that auto-roots the devices to gain escalated privileges. On iOS, malware can be easily distributed as a sideloaded app that bypasses Apple's App Store review. Attackers can distribute these apps via SMS messages, phishing emails, or websites to coerce users to trust and install the app on their devices, allowing the apps to use private APIs that Apple wouldn't normally allow. Occasionally, malware has made it passed Apple's review into the App Store, however this is relatively rare.

Lookout also pushes automatic updates over the air (OTA) to devices to ensure that the security on the device is updated with the latest threat information from Lookout's cloud-based security platform.

CONTINUOUS MONITORING: This instruction also requires "continuous on-line monitoring" for threats with the capability to immediately alert personnel and "automatically disable the system if serious IA violations are detected".

Lookout addresses this instruction by providing continuous protection against threats, notifying both the end user and IT admins in real time if threats are detected. Moreover, through our integration with leading EMM solutions, agencies can automatically quarantine the mobile device if serious threats are detected.

NIST 800-163 Vetting the Security of Mobile Applications

Overview:

Published Jan. 26, 2015, NIST Special Publication 800-163, "Vetting the Security of Mobile Applications", provides federal and other government agencies and private businesses with direction on how to:

- Plan the implementation of a mobile app vetting process
- Develop app security requirements
- Understand the types of app vulnerabilities and the testing methods used to detect those vulnerabilities, and
- Determine if an app is acceptable for deployment on the organization's mobile devices

Who does NIST 800-163 apply to?

All federal agencies and organizations looking to use mobile applications to enhance employee productivity. Note that this publication provides guidance, rather than specific compliance requirements.

Are there specific guidelines related to threats and data leakage?	
ID	**Key Quotes**
3.1 General Requirements	Preventing unauthorized functionality: Unauthorized functionality, such as data exfiltration performed by malware, must not be supported Limiting permissions: Apps should have only the minimum permissions necessary and should only grant other applications the necessary permissions Protecting sensitive data: Apps that collect, store, and transmit sensitive data should protect the confidentiality and integrity of this data. This category includes preserving privacy, such as asking permission to use personal information and using it only for authorized purposes. Securing app code dependencies: The app must use any dependencies, such as on libraries, in a reasonable manner and not for malicious reasons
3.1.2 Preventing Unauthorized Functionality	Malware detection and analysis tools can identify both known and new forms of malware. These tools can be incorporated as part of an organization's enterprise mobile device management (MDM) solution, organization's app store, or app vetting process.
3.1.3 Limiting Permissions	Some apps have permissions that are not consistent with EULAs, app permissions, app descriptions, in program notifications, or other expected behaviors and would not be considered to exhibit secure behavior. An example is a wallpaper app that collects and stores sensitive information, such as passwords or PII, or accesses the camera and microphone.
3.2.3 Static Versus Dynamic Analysis	Malware increasingly detects the use of emulators as a testing platform and changes its behavior accordingly to avoid detection. Therefore, it is recommended that analyzers use a combination of emulated and physical mobile devices so as to avoid false negatives from malware that employs anti-detection techniques.

How does Lookout help with NIST 800-163 compliance?

Lookout provides visibility into app-based malware and data leakage, both of which represent high security concerns as discussed in NIST 800-163.

MALWARE DETECTION: Lookout provides protection against app-based malware, such as trojans, spyware, and rootkits. These threats can lead to data exfiltration and have been identified on both Android and iOS (iOS malware rarely found in the App Store, but can be found on 3rd party app stores).

CONTROLLING DATA LEAKAGE: Lookout uses a combination of static and dynamic analysis to identify the app capabilities on the device, allowing the organization to view and restrict apps that violate their security policy. For example, Lookout can identify a wallpaper app that collects and stores sensitive information, such as passwords or PII, or accesses the camera and microphone.

MDM INTEGRATION: Through Lookout's integration with leading MDM solutions, agencies can automatically quarantine the mobile device if serious threats are detected.

NIAP Requirements for Vetting Mobile Apps

Overview:

The National Information Assurance Partnership (NIAP) is responsible for U.S. implementation of the Common Criteria including management of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) validation body. The principal objective of the Validation Body is to ensure the provision of competent IT security evaluation and validation services for both government and industry. NIAP manages a national program for developing Protection Profiles, evaluation methodologies, and policies that will ensure achievable, repeatable, and testable requirements.

This specific document presents functional and assurance requirements for vetting mobile apps outside formal Common Criteria evaluations. Common Criteria evaluation is required for IA and IA-enabled products in National Security Systems. However, even apps without IA functionality may pose some security risks, and concern about these risks has motivated the vetting of such apps in government and industry.

Who does NIAP apply to?

Organizations both in government and industry that are participating in the process of IT security evaluation within the CCEVS.

Are there specific guidelines related to threats and data leakage?	
ID	**Key Quotes**
FDP_DEC_EXT.1.1 FDP_DEC_EXT.1.2	The application shall restrict its access to some: 1) hardware resources: network connectivity, camera, microphone, location services, NFC, USB, Bluetooth 2) sensitive information repositories: address book, calendar, call lists, system logs
FPT_API_EXT.1.1	The application shall use only documented platform APIs
FPT_API_EXT.1.1	The application shall encrypt all transmitted sensitive data with at least one of: HTTPS, TLS, DTLS, SSH

How does Lookout help with NIAP compliance for App Vetting?

Lookout provides visibility into app capabilities that access sensitive information, sideloaded applications that may be using undocumented APIs, and protection against attacks on encrypted data in transit.

VISIBILITY TO APPS THAT ACCESS SENSATIVE INFORMATION: Lookout uses a combination of static and dynamic analysis to identify the app capabilities on the device, allowing the organization to view and restrict apps that violate their security policy. For example, Lookout can identify a wallpaper app that collects and stores sensitive information, such as passwords or PII, or accesses the camera and microphone.

DETECTION OF SIDELOADED APPS THAT MAY USE UNDOCUMENTED APIs: Users are increasingly turning to 3rd party app stores to get apps for free (such as gaming apps). Downloading these onto your non-jailbroken iPhone or non-rooted Android device is simple, yet these apps bypass official App Store review and can use undocumented APIs. With Lookout, admins get alerted to any sideloaded apps that have been installed on mobile devices that may violate an organization's compliance policies.

PROTECTION FROM NETWORK ATTACKS ON ENCRYPTED DATA IN TRANSIT: Lookout protects against network-based attacks that attempt to access encrypted data-in-transit by executing a "man-in-the-middle attack". As mobile devices increasingly connect to unverified Wi-Fi access points at home and abroad, Lookout helps agencies stay compliant by providing network protection on mobile devices that aren't addressed by VPNs.

Embracing mobility while staying compliant

Progressive organizations are embracing smartphones and tablets in the workplace to enable more productivity from employees. As more sensitive data flows through these endpoints, Federal agencies are looking to solutions that provide visibility into emerging risks on this platform to comply regulatory and organizational security policies.

To learn how Lookout can help your agency stay compliant while enabling mobility within your organization, contact us at info@lookout.com