MOBILE POLICY
SECURITY REQUIREMENTS GUIDE (SRG)
OVERVIEW

Version 1, Release 2

26 July 2013

Developed by DISA for the DoD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DISA FSO or any non-Federal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

LIST OF TABLES

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

This Mobile Policy Security Requirements Guide (SRG) Overview, along with the associated Technology SRGs, provides the security policies and requirements for applying security concepts to mobile systems. This SRG also supports the design, implementation, and management of wireless devices and networks that are used to provide information technology (IT) services to mobile workers in the DoD, in addition to providing policy guidance for DoD Directive (DoDD) 8100.02 and other DoD policies related to wireless systems.

The Mobile Policy SRG is one in a family of SRGs addressing mobility solutions. Other mobility SRGs include the Mobile Operating System (MOS) SRG, Mobile Applications SRG, and the Mobile Device Management (MDM) SRG. The Mobile Policy SRG provides non-technical requirements (policy, training, and operating procedures, for example) for mobile devices operated in the DoD while the other mobility SRGs provide technical requirements. Organizations designing or implementing mobile solutions should review all of the SRGs to ensure compliance.

1.1.1 Security Requirements Guides

SRGs are collections of requirements applicable to a given technology family. SRGs represent an intermediate step between Control Correlation Identifiers (CCIs) and STIGs. CCIs represent discrete, measurable, and actionable items sourced from Information Assurance (IA) controls defined in policy, such as those originating in Department of Defense Instruction (DoDI) 8500.2 and National Institute of Standards and Technology (NIST) Special Publication 800-53. STIGs provide product-specific information for validating and attaining compliance with requirements defined in the SRG for that product’s technology area.

There are four core SRGs: Applications, Network Infrastructure, Operating Systems, and Policy. Each addresses the applicable CCIs in the context of the technology family. Subordinate to the core SRGs, there are Technology SRGs developed to address the technologies at a more granular level.

The Mobile Policy SRG is based on current mobile policy tied to CCIs rather than the Policy (Core) SRG. This Mobile Policy SRG contains non-technical check and fix information and should be utilized by organizations to implement mobile policy.

The STIGs based on this SRG will provide the product specific technical implementation guidance for that product. The STIG will contain the specific check and fix information for the product it covers.

SRG Hierarchy example:

Application SRG
 |__ *Database SRG*
  |__ *MS SQL Server 2005 STIG*

The SRG relationship and structure provides the ability to identify requirements that may be considered not applicable for a given technology family and provide appropriate justification. It also provides the structure to identify variations in specific values based on the technology family. These variations will be captured once and will propagate down to the Technology SRGs and then to the STIGs. This will eliminate the need for each product specific STIG to address things that are not applicable. The "Not Applicable" items will be identified with via the STIGID and Group Title naming and will utilize the Vulnerability Discussion to document the justification.

1.1.2 SRG Naming Standards

In an effort to establish consistency across the SRGs, a naming standard for the Group Title and STIGIDs has been established.

Technology SRG Naming Standards

For Technology SRG Group Title and STIGIDs the following applies:

{Core SRG value}+-{*Technology SRG*}-{*6 digit numeric sequence number* or *NA* flag}

Examples:

SRG-NET-000001-RTR-000001
SRG-APP-000001-COL-000001
SRG-OS-000001-UNIX-000001

Example for the non applicable:

SRG-NET-000001-ROUTER-NA
SRG-APP-000001-DB-NA

Checks/Fixes will be included at this level in a general form. These checks and fixes will apply for any STIGs that are created for products that do not have product specific check and fix guidance.

1.2 Authority

DoD Directive (DoDD) 8500.1 requires that “all IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines” and tasks Defense Information Systems Agency (DISA) to “develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA”. This document is provided under the authority of DoDD 8500.1.

Although the use of the principles and guidelines in these STIGs provide an environment that contributes to the security requirements of DoD systems operating at Mission Assurance Categories (MACs) I through III, applicable SP 800-53 IA controls need to be applied to all systems and architectures.

The Information Operations Condition (INFOCON) for the DoD recommends actions during periods when a heightened defensive posture is required to protect DoD computer networks from attack. The Information Assurance Officer (IAO) will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance.

Initially, these directives are discussed and released as Warning Orders (WARNORDs) and feedback is encouraged. These may then upgrade these orders to directives; they are then called Communication Tasking Orders (CTOs). It is each organization's responsibility to take action by complying with the CTOs and reporting compliance via their respective Computer Network Defense Service Provider (CNDSP).

1.3 Scope

The security requirements contained within the SRGs are applicable to all DoD-administered systems and all systems connected to DoD networks. The SRG provides requirements to reduce the security vulnerabilities of systems. These requirements are designed to assist Security Managers (SMs), Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) with configuring and maintaining security controls.

1.3.1 Relationship to STIGs

The SRG defines the requirements for various technology families and the STIGs are the technical implementation guidelines for specific products. The STIGs are not a superset of other DISA STIGs that may be applicable to a given system, which may include but are not limited to Database, Web Server, and Domain Name System (DNS) STIGs. Compliance with all STIGs applicable to a system is required.

1.4 Vulnerability Severity Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Code of CAT I, II, or III.

Table 1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines	Examples of DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately, result in loss of Confidentiality, Availability, or Integrity.	Includes **BUT NOT LIMITED** to the following examples of direct and immediate loss: 1. May result in loss of life, loss of facilities, or equipment, which would result in mission failure. 2. Allows unauthorized access to security or administrator level resources or privileges. 3. Allows unauthorized disclosure of, or access to, classified data or materials. 4. Allows unauthorized access to classified facilities. 5. Allows denial of service or denial of access, which will result in mission failure. 6. Prevents auditing or monitoring of cyber or physical environments. 7. Operation of a system/capability which has not been approved by the appropriate Designated Accrediting Authority (DAA). 8. Unsupported software where there is no documented acceptance of DAA risk.

	DISA Category Code Guidelines	Examples of DISA Category Code Guidelines
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.	Includes **BUT NOT LIMITED** to the following examples that have a potential to result in loss: 1. Allows access to information that could lead to a CAT I vulnerability. 2. Could result in personal injury, damage to facilities, or equipment which would degrade the mission. 3. Allows unauthorized access to user or application level system resources. 4. Could result in the loss or compromise of sensitive information. 5. Allows unauthorized access to Government or Contractor owned or leased facilities. 6. May result in the disruption of system or network resources degrading the ability to perform the mission. 7. Prevents a timely recovery from an attack or system outage. 8. Provides unauthorized disclosure of or access to unclassified sensitive, Personally Identifiable Information (PII), or other data or materials.

	DISA Category Code Guidelines	Examples of DISA Category Code Guidelines
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.	Includes **BUT NOT LIMITED** to the following examples that provide information which could potentially result in degradation of system information assurance measures or loss of data: 1. Allows access to information that could lead to a CAT II vulnerability. 2. Has the potential to affect the accuracy or reliability of data pertaining to personnel, resources, operations, or other sensitive information. 3. Allows the running of any applications, services or protocols that do not support mission functions. 4. Degrades a defense in depth systems security architecture. 5. Degrades the timely recovery from an attack or system outage. 6. Indicates inadequate security administration. 7. System not documented in the site's C&A Package/System Security Plan (SSP). 8. Lack of document retention by the Information Assurance Manager (IAM) (i.e., completed user agreement forms).

1.5 SRG and STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable SRGs and STIGs from the Information Assurance Support Environment (IASE) website. This site contains the latest copies of any SRG, as well as STIGs, scripts, and other related security information. The Non-classified Internet Protocol Router Network (NIPRNet) Uniform Resource Locator (URL) for the IASE website is http://iase.disa.mil/.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to: disa.letterkenny.FSO.mbx.stig-customer-support-mailbox@mail.mil.

DISA Field Security Operations (FSO) will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA FSO maintenance release schedule.

2. ASSESSMENT CONSIDERATIONS

2.1 800-53 Requirements

Only NIST SP 800-53 policy requirements specific to mobility or wireless technologies are listed in this SRG. There are a number of policy requirements derived from NIST SP 800-53 that are not defined in this SRG, as they are not unique to mobility or wireless technologies, and are therefore required of the organization, regardless of mobility implementation.

CNSSI 1253 defines the required controls for DoD systems, based on confidentiality, integrity, and availability (baseline) for all components of information systems that process, store, or transmit National Security Information (NSI). In addition, requirements currently not on a DoD baseline as defined by CNSSI 1253 are included. These are included to ensure adequate procedures exist if controls are later added as requirements due to overlays. In all cases, CNSSI 1253 along with required baselines will serve as the policy requirement for any given asset or information system.

2.2 The Mobility SRG Framework

This SRG has procedures that are intended to provide appropriate evaluation and remediation functions for a typically configured mobile system. These procedures are not product-specific and are intended for use at the organization or agency policy level.

The Mobile Policy SRG is one of a family of four Mobility SRGs that must be considered together when implementing an enterprise mobility solution within DoD.

- The Mobile Operating System (MOS) SRG addresses security for the operating system installed on mobile devices, primarily in the smartphone and tablet form factor, and maps to the IA controls in the core OS SRG.

- The Mobile Device Management (MDM) SRG addresses centralized management of mobile operating systems and applications. The MDM SRG also covers aspects of device integrity verification and enterprise email. The IA controls in the MDM SRG map to the IA controls in the core Applications SRG.

- The Mobile Applications SRG addresses the security of applications that run on mobile OS. The IA controls in the Mobile Applications SRG also map to the IA controls in the core Applications SRG.

- The Mobile Policy SRG addresses management, operational, personnel, and physical security controls related to mobile devices. The IA controls in the Mobile Policy SRG map to the IA controls in the core Policy SRG.

The Mobility SRGs work in conjunction with one another and there are linkages between them to form the Mobility SRG framework. For example, the technical Mobile Operating System (MOS) SRG includes requirements for Mobile Device Management (MDM) support. Additionally, many of the auditing and alerting controls that would usually apply to traditional desktop and server OS are covered under the MDM SRG in the Mobility SRG framework. This is because it is presumed that the MDM system will perform the analysis and reporting of audit logs, not the mobile OS. The Mobile Policy SRG provides the overarching policy, and non-technical requirements for all implementations.

2.3 General Procedures

The Mobile Policy SRG has procedures intended to provide appropriate evaluation and remediation functions for organizational policy. These procedures apply to organizations and the locations under their authority. Where a particular requirement applies to a limited scope, that limitation has been stated in the requirement, e.g., the site or the system.

3. COMMON CHARACTERISTICS OF MOBILE DEVICES

There are several common characteristics of mobile devices important to understand when properly implementing an IA program for Mobility.

3.1 Data Communications Interfaces

The most common data communications interfaces on mobile devices today are:

- Wi-Fi
- Bluetooth
- Cellular data communications
- Universal Serial Bus (USB)

Each interface has specific known vulnerabilities and methods for mitigating risk. The Mobile Policy SRG includes specific IA controls for Wi-Fi and Bluetooth technology and tethered USB connections. If a mobile device has an interface not listed above, it is required to be compliant with the general Mobile Policy SRG controls for data communications interfaces. For example, the next generation of mobile devices may contain an interface for near field communications (NFC) to support applications related to electronic payments and physical access control. In the interim, the general controls would apply to the NFC interface. A subsequent release of the Mobile SRGs may then include specific IA controls for that technology.

3.2 Enhanced Capabilities

One of the distinguishing features of mobile devices relative to traditional personal computers (PCs) is the inclusion of geo-location and spatial orientation sensors, cameras, and embedded microphones. Consumer applications, such as mapping and photo sharing applications that leverage these hardware capabilities, are extremely popular. DoD is currently developing applications to use these same capabilities to support the warfighter.

In most cases, the risk associated with these new capabilities is considered an operations security (OPSEC) risk rather than an IA risk. OPSEC risks are best mitigated through tactics, techniques, and procedures rather than technical controls. These mobile capabilities may be of critical value in some environments (e.g., the battlefield) but an unnecessary threat in others (e.g., a Sensitive Compartmented Information Facility (SCIF)). The Mobile Policy SRG provides a framework for requiring training, policies, and enforcement.

3.3 Non-Enterprise Activated (NEA) Mobile Devices

A non-enterprise activated (NEA) device is any DoD mobile handheld device that is not connected at any time to a DoD network or enterprise, and does not process sensitive or classified DoD data or voice communications. Sensitive data or information is defined as any DoD data or information that has not been deemed as publicly releasable by a DoD Public Affairs Officer (PAO).

This page is intentionally left blank.

APPENDIX A: ACRONYMS

Acronym	Definition
CCI	Control Correlation Identifiers
C&A	Certification and Accreditation
CMD	Commercial Mobile Device
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CONOPS	Concept of Operations
DAA	Designated Accrediting Authority
DAC	Discretionary Access Control
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
FSO	Field Security Operations
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IT	Information Technology
MAC	Mission Assurance Category
MAPP	Mobile Application
MDM	Mobile Device Management
MOS	Mobile Operating System
NEA	Non-enterprise activated
NFC	Near Field Communications
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OPSEC	Operations Security
OS	Operating System
PAO	Public Affairs Officer
PC	Personal Computer
PII	Personally Identifiable Information
SA	System Administrator
SCIF	Sensitive Compartmented Information Facility
SIPRNet	Secret Internet Protocol Router Network
SP	Special Publication
SRG	Security Requirement Guide
SM	Security Manager
STIG	Security Technical Implementation Guide

Acronym	Definition
URL	Uniform Resource Locator
USB	Universal Serial Bus
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network