

Securing Information to the Edge

AFCEA/GMU Panel Discussion

3:00 – 4:30

Participants

- Dr. Rocky Young – Moderator
- Panelists:
 - Mr. Mark Norton – DoD
 - Mr. Kevin Cox – DoJ
 - Mr. Gary Bode – Army
 - Mr. Daniel Ford – Fixmo
 - Mr. Daniel Taylor – Microsoft
 - Mr. Brian Hajost – SteelCloud

The image features a background of thin, vertical, light blue lines on a light gray gradient. A solid teal horizontal bar spans the width of the image, containing the text. Below the teal bar is a thin yellow line, and at the very bottom is a gray gradient bar.

Mr. Mark Norton – DoD

mark.norton@osd.mil

DoD Mobile Enterprise



Mark Norton
DoD CIO, C4IIC
May 23, 2013





Strategic Mobility Vision Established



Goal 1

- Advance and Evolve the DoD Information Enterprise Infrastructure to support Mobile Devices

Goal 2

- Institute Mobile Device Policies and Standards

Goal 3

- Promote the development and Use of DoD Mobile and Web-Enabled Applications

Goal 4

- Develop an enterprise Mobility service for Classified and Unclassified capabilities

Successful execution relies on the cooperation and collaboration of all DoD Components and on partnerships with federal, intelligence, academia, and commercial communities. With your support, we will equip our forces with the capability to **quickly access relevant information whenever and wherever needed.**

Vision: Secure Access to Data Anywhere, Anytime

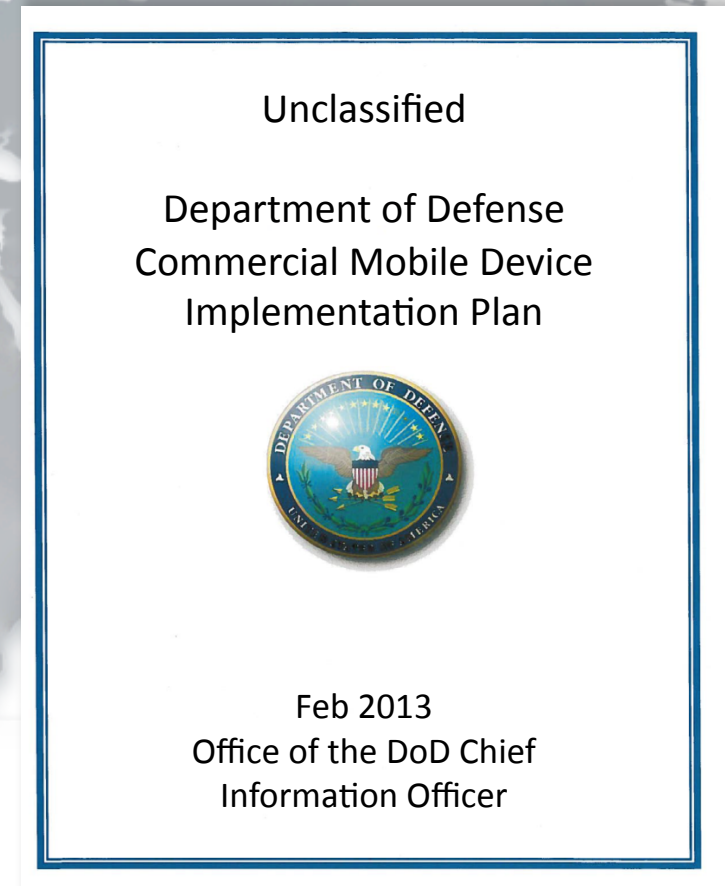


DoD Enterprise Benefits:

- Efficient; Cost Savings
- Consistent Security
- Rapid Technology Insertion
- Shared Applications extend capabilities to all users

DISA to roll out in multiple phases:

- UNCLASS
 - April 2013, 1,500 devices
 - Sept 2013, 5,000 devices
 - FY14, up to 100,000 devices
- CLASS
 - Mar 2013, 500 devices at SECRET
 - Sept 2013, 1,500 devices at TOP SECRET
 - FY14, enterprise capability





DoD CIO

Mobility Big Picture

DoD Migration from Wired to Wireless



Mobile Device Management

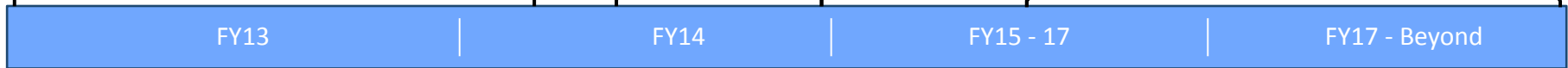


Apps/Cloud

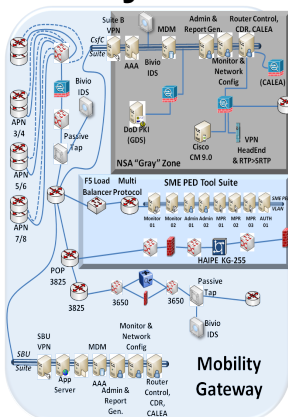


PIV 201-2 Integration

Technology Insertion
Near Field Communications?
Biometrics?



Implement CONUS Mobility Gateway



Global Expansion of Mobility Gateways



Phase-out of SME PED



Primary Communication for ROUTINE DoD Users is Wireless



SUPPORT THE WARFIGHTER



DoD Mobile Classified Evolution



QSEC-800

QSEC-2700

SME PED

Droid Pro

Razr Maxx

Capabilities:

- Secure phone calls to DMCC, DRSN, ECVoIP, VoSIP, SCIP devices
- 4G LTE /CONUS
- Access to Secure DoD Enterprise Email



Looking Ahead with Industry

- **Improve user experience**
- **Mobile Application Management**
- **Over the Air (OTA) device management; device auditing; and device provisioning**
- **Physical Layer Limitations (Spectrum/AJ)**



Must deliver mobile solutions that leverage commercial off-the-shelf products, improve functionality, decrease cost, and enable increased personal productivity

The image features a background of thin, vertical, light blue lines on a light gray gradient. A solid teal horizontal bar spans the width of the image, containing the text. Below the teal bar is a thin yellow line, and at the very bottom is a gray gradient bar.

Mr. Kevin Cox – DoJ

kevin.cox@usdoj.gov

DIGITAL GOVERNMENT STRATEGY UPDATE

#	Owner(s)	Milestone Actions	Timeframe (months)			
			1	3	6	12
9.1	DHS / DOD / NIST	Develop government-wide mobile and wireless security baseline (includes security reference architectures.).				.

May 2013

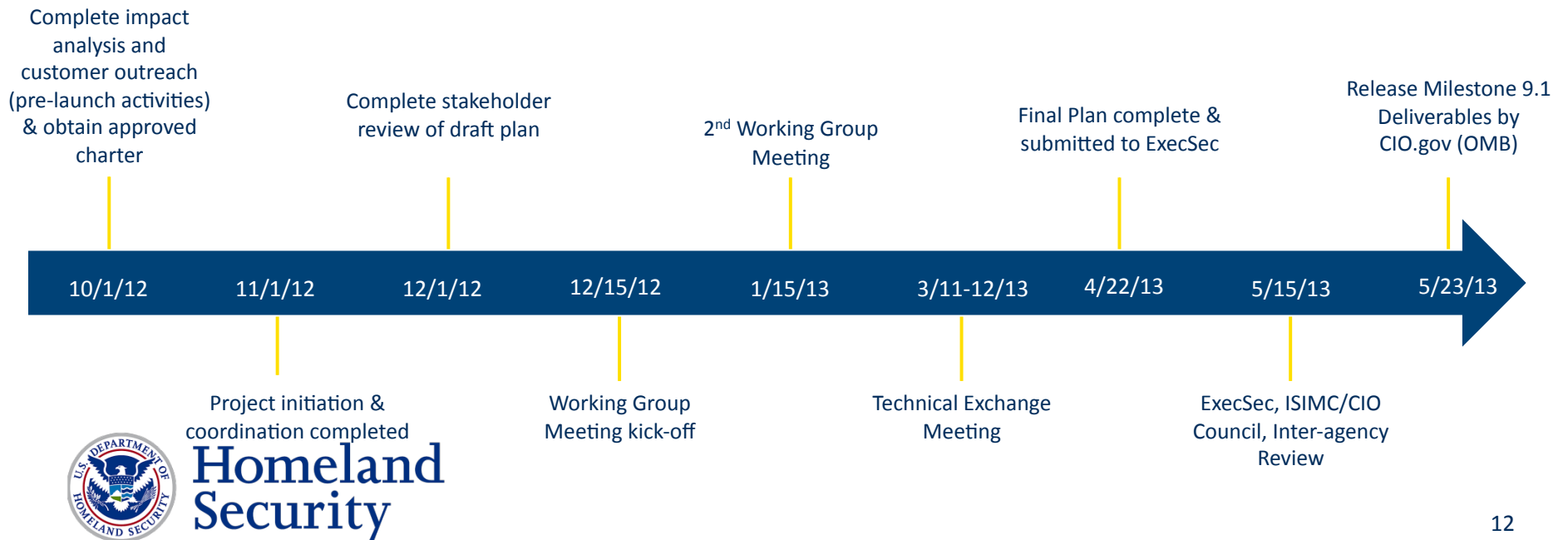


**Homeland
Security**

Deliver Government-wide mobile and wireless security baseline which includes a reference security architecture.

DHS will lead a six month reference architecture tiger team

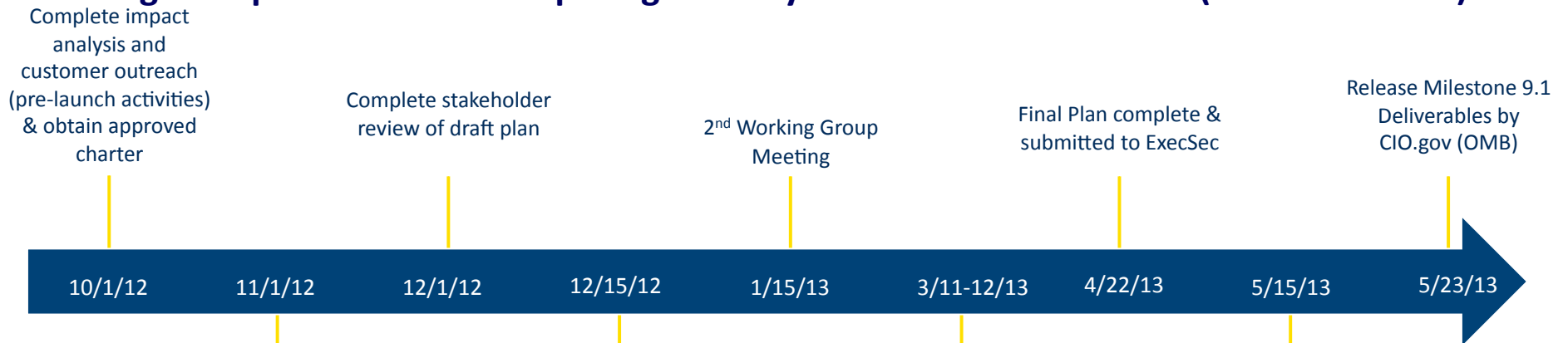
- **Phase 1:** Develop Use Case Requirements (Completed)
- **Phase 2:** Establish Baseline Security Requirements (In Progress)
- **Phase 3:** Integrate and Update Mobile Security Reference Architecture (In Progress)
- **Phase 4:** Submission and Review



On-Going Activities for DGS Milestone 9.1

On-going Key Activities :

- **Mobile Computing Baseline Working Group:** DHS, DoD, DOJ, GSA, NIST establishing IA Mobile Overlay(s)
- **Development of the Mobile Computing Decision Framework**
- **Federal Mobile Technical Exchange Meeting:** Solicit input & feedback for DGS Milestone 9.1
- **Federal Mobile Security Baseline:** Narrative focusing on MCDF, Federal Employee Usecase, and Mobile Security Overlays.
- **Align & Update Mobile Computing Security Reference Architecture (DHS NPPD FNR)**



Homeland Security

Milestone 9.1

#	Owner(s)	Milestone Actions	Timeframe (months)			
			1	3	6	12
9.1	DHS / DOD / NIST	Develop government-wide mobile and wireless security baseline (includes security reference architectures.).				•



DELIVERABLE
Enterprise Overlay for Mobile Security (Moderate)



DELIVERABLE
Milestone 9.1 Federal Mobile Security Baseline



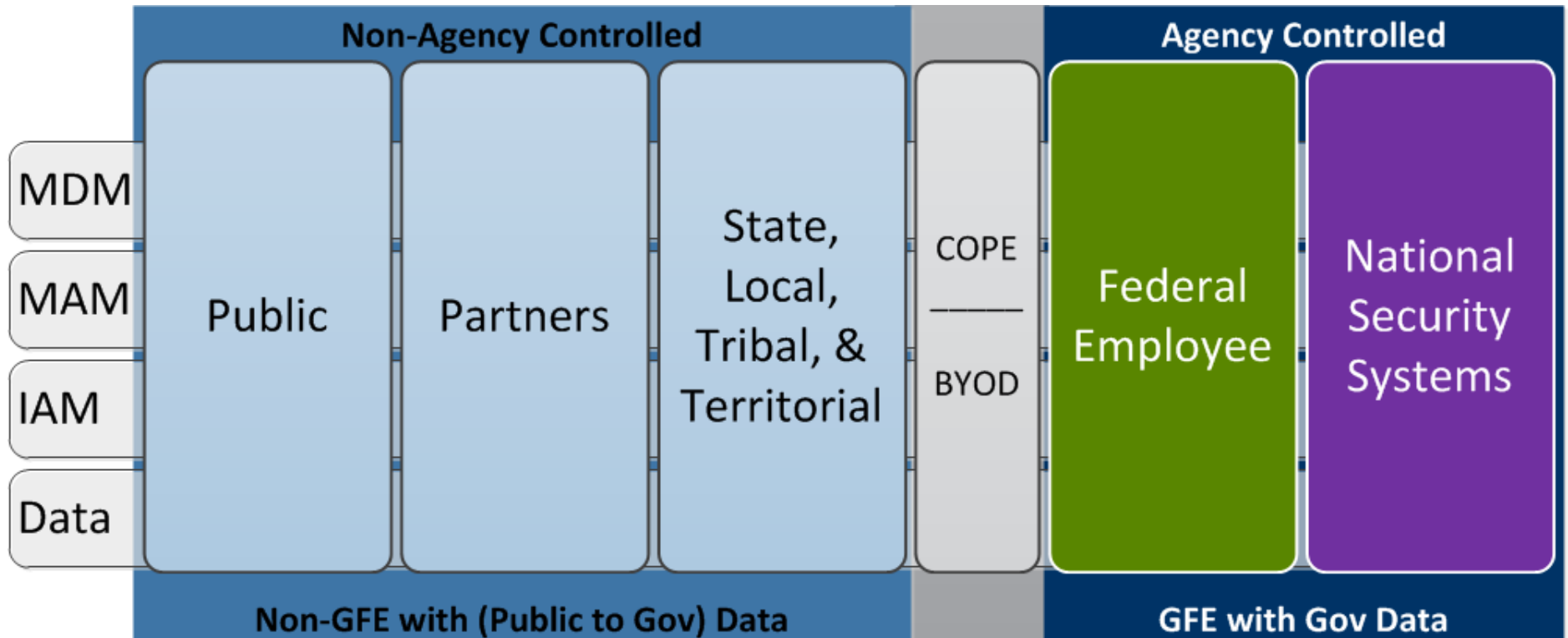
DELIVERABLE
Mobile Security Reference Architecture (Appendix: Mobile Computing Decision Framework)



Intersection of Top Challenges

Non-Agency Controlled				Agency Controlled	
Public	Partners	State, Local, Tribal, & Territorial	COPE BYOD	Federal Employee	National Security Systems
Mobile Device Management (MDM)					
Mobile Application Management (MAM)					
Identity & Access Management (IAM)					
Data Standards (Data)					
Non-GFE with (Public to Gov) Data				GFE with Gov Data	

Intersection of Mobile Challenge Areas and Use Cases



Mobile Computing Decision Framework

Four Stages

Mission Requirement



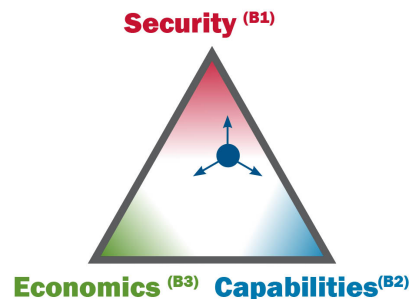
Input: Mission request for mobile computing

Steps: Define mobile business case:

- Users
- Data sources and sensitivity
- Location of use

Output: Preliminary assessment of mission impact

Decision Balancing



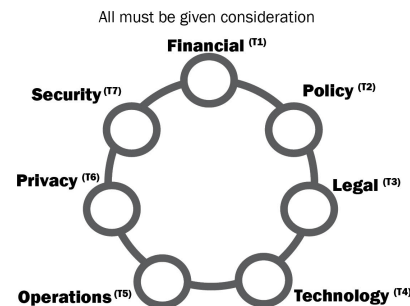
Input: Approved business case

Steps: Choose starting point (primary factor)
Determine tradeoffs:

- Security
- Capabilities
- Economics

Output: Balance point that most effectively supports mission

Risk-Based Tailoring



Input: Balance of security, capabilities, economics

Steps: Apply security baseline and risk management method:

- Assess risk in each area
- Determine mitigations
- Examine remaining risk

Output: Acceptable risk in all areas –or– repeat Decision Balancing

Results

Application (R1)

Device (R2)

Infrastructure (R3)

Input: Mission business case, balanced considerations, acceptable risk

Steps: Translate mission requirement, risk and mitigations to high level requirements

Output: Description of:

- Devices (OS, type)
- Applications (internal, external) and services
- Infrastructure: MDM, MAM, IAM, access gateways, firewalls, encryption



Homeland Security

Security Baseline and Overlays

- **Security Baseline:** Set of minimum security and privacy controls for federal information systems and organizations based on security category and impact level of information systems
 - Implemented as part of organization-wide information security and privacy risk management process
 - Mobile Computing Security Baseline starts with NIST 800-53 moderate baseline and is tailored to addresses threats and risks unique to mobile computing environment
- **Security Control Overlay:** Apply NIST or CNSSS tailoring guidance to security baseline to develop a set of controls for community-wide use for computing paradigms such as mobile or cloud computing
 - Overlay is a *fully specified set of security controls, control enhancements, and supplemental guidance*
 - Government-wide overlays will be developed for MDM, MAM, IAM and Data



Interpreting the MDM Overlay

NIST Moderate Baseline + Add/Remove Controls = MDM Overlay (Moderate)

No.	NIST 800-53 Controls Name		NIST SP 800-53	Proposed MDM	Rationale for addition or removal	Seven Types of Risk							
	ID	TITLE (NIST SP 800-53 Rev 4 FPD)				M	M	COMMENTS	Finance	Policy	Legal	Technology	Operations
#	ID	TITLE (NIST SP 800-53 Rev 4 FPD)	M	M	COMMENTS	T1	T2	T3	T4	T5	T6	T7	
1	AC-1	Access Control Policy and Procedures	X	AC-1	Controls in NIST Baseline and MDM Overlay		Policy	Legal					
2	AC-2	Account Management	X	AC-2					Technology				
3	AC-2(1)	Account Management Automated System Account Management	X	AC-2(1)		STIG ID: SRG-APP-000024-SRV				Technology			
4	AC-2(2)	Account Management Removal of Temporary / Emergency Accounts	X	(-)		No temporary accounts on the MDM server, so requirement is essentially N/A. STIG ID: SRG-APP-000024-NA				Technology			
20	AC-3(4)	Access Enforcement Discretionary Access Control		+AC-3(4)	Add only for multiple-user devices.				Technology			Security	
21	AC-3(5)	Access Enforcement Security-Relevant Information		+AC-3(5)	STIG ID: SRG-APP-000037-MDM-000220-SRV				Technology			Security	

Control Removed from NIST Baseline for MDM Overlay

Controls Added to NIST Baseline for MDM Overlay



Homeland Security

Backup Slides

BACK UP SLIDES



Homeland
Security

9.1 Milestone Playbook Highlights

	Non-Agency Controlled				Agency Controlled	
	Public	Partners	State, Local, Tribal, & Territorial	COPE BYOD	Federal Employee	National Security Systems
MDM		?	?	?	✓	✓ +
MAM	?	?	?	?	✓	✓ +
IAM	?	?	?	?	✓	✓ +
Data	?	?	?	?	✓	✓ +
	Non-GFE with (Public to Gov) Data					GFE with Gov Data



The image features a background of thin, vertical, light blue lines on a light gray gradient. A solid teal horizontal bar spans the width of the image, containing the text. A thin yellow line is positioned above and below the teal bar.

Mr. Gary Bode – Army

gary.bode@us.army.mil



DCGS-A

Distributed Common Ground System - Army

DCGS-A Information Sharing Across Domains and Organizations

*AFCEA-GMU C4I Center Symposium – Critical Issues
in C4I*

May 22nd, 2013

COL Charles A. Wells
Project Manager, DCGS-A
dcgsa.apg.army.mil
pmo@dcgsa.us

Gary A. Bode, MA, MS, CISSP-ISSEP
Senior Test Engineer (Security)
gary.bode@us.army.mil





What Does Distributed Common Ground Systems – Army (DCGS-A) Deliver ?



- ◆ **Historically, every sensor had its own, unique ground system to receive, store, and process data.**
 - Created intelligence-sharing challenges
 - Focus on analyzing intelligence related to a single Intelligence discipline (Signal Intelligence, Imagery, etc.)

- ◆ **DCGS-A Changes The Paradigm!**
 - *Single system receives data from all sensors*
 - National – Aerial – Terrestrial – The Soldier
 - Intelligence easily shared
 - Army-wide – Jointly – with Coalition Partners
 - Multi-disciplined Intelligence Analysis
 - Signal – Imagery – Human Intelligence
 - Fuse into a common product to support analysis

***Better Analysis – Increased Collaboration
Timely, Informed Critical Command Decisions***





DCGS-A Technology Focus Areas

- **Ease of use**
 - Single Common Baseline
 - Intuitive user interfaces
 - Streamlined workflow based upon analytic process
 - Training
(Computer Based Training / Embedded Training)
- **Actionable intelligence to the edge**
- **Node to node (cloud) data synchronization / content management**
- **Knowledge management**
- **Entity extraction from unstructured information (entities, activities, relationships between them)**
- **F3EAD**
(Find, Fix, Finish, Exploit, Analyze, Disseminate)
 - Aided target recognition (technology and TTP)
 - Combat assessment





DCGS-A Engagement with Industry

- ◆ **DCGS-A has partnered with both OGAs and Industry in the Ozone Widget Development by:**
 - Making the DCGS-A Ozone Development environment available as a free download on DISA's Forge.mil:
 - <https://project.forge.mil/sf/projects/dcgsaozone>
 - Making all of the common infrastructure (help, query, results, map, and DIB) widgets freely available to the DoD enterprise through the Forge.mil site
 - Holding Training classes that have included both DCGS-A Staff, OGA Staff, and Industry Partners
 - Supporting the Forge.mil site and Ozone Google Group with insight into our implementation
 - Participating in the Government Open Source Software (GOSS) meetings for steering the overall Ozone Roadmap

- ◆ **DCGS-A Standard Cloud architecture supports an open integration environment:**
 - Designed around a Modular Open Systems Architecture (MOSA) to allow industry to easily integrate capabilities without relying on stove pipe approaches
 - Includes all manner of integration from core infrastructure, data integration, analytical tools, and visualization.

- ◆ **The Tactical Cloud Integration Lab (TCIL) effort has been stood up as a "proving ground" for new Cloud/Ozone capabilities targeted for inclusion in the DCGS-A Standard Cloud (DSC). This includes:**
 - Providing public meetings for understanding DSC's Cloud Architecture
 - Inviting Industry Partners to both propose and integrate capabilities onto the DSC Reference Hardware available in the TCIL
 - Providing a public website with technical information on the TCIL and DSC efforts
 - Plans are in place to stand up a TCIL Cloud node on an unclassified domain and provide VPN access to external parties





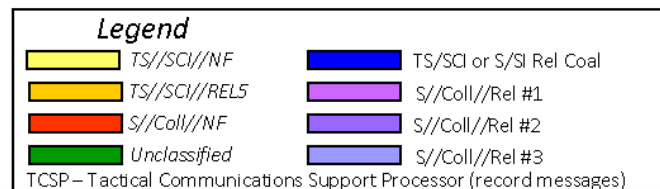
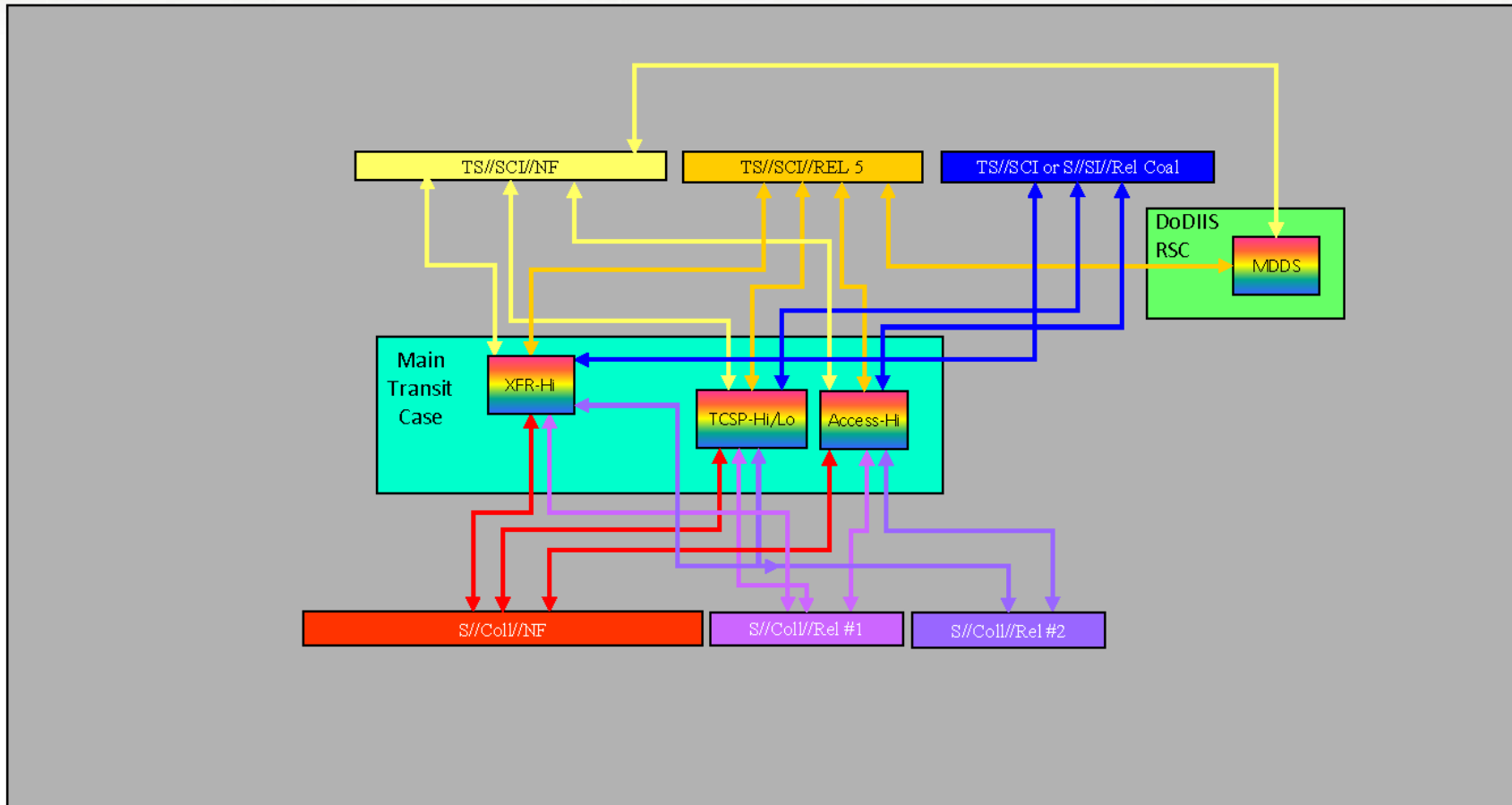
DCGS-A Cross Domain Solution Selection Criteria

- Must be on the UDCMO Baseline List (currently ~30 CDS of all types – most are transfer)
- Open architecture – non-proprietary OS, i.e., an OS that runs on multiple h/w platforms, e.g., Solaris x86, RH SE Linux
- Operates on current CHS equipment set (X86)
- Tactical Friendly (able to operate in bandwidth constrained scenarios and support RT/NRT transfers)
- Meets DCGS-A Specific Requirements
 - multiple document type transfer capability
 - bi-directional
 - certified for TSABI and SABI
 - ease of use
 - sustainable (current OEM, CM, dev planned)





Cross Domain Solution Suite Logical Data Flow



The image features a background of thin, vertical, light blue lines on a light gray gradient. A solid teal horizontal bar spans the width of the image, containing the text. Below the teal bar is a thin yellow line, and at the very bottom is a gray gradient bar.

Mr. Daniel Ford – Fixmo

daniel.ford@fixmo.com

Fixmo

The Mobile Risk Management Company

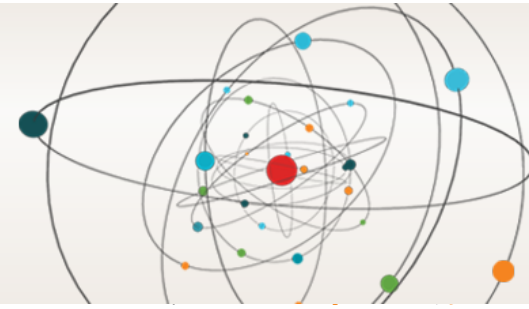


**Go Ahead.
Let Them Bring
Their Own Devices.**

**Defense-grade mobile security,
risk management, and compliance.**

We should talk.

Introduction



Contact Informaton:

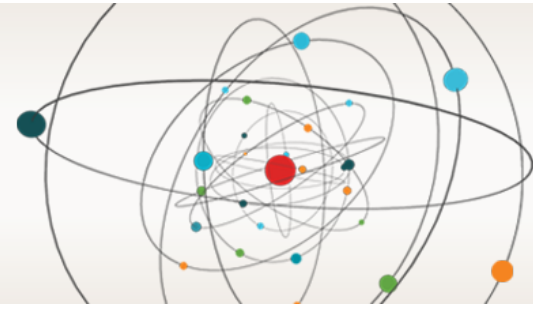
Twitter: @netsecrex

SMTP: daniel.ford@fixmo.com

Blogs:

- www.netsecrex.com
- www.fixmo.com/blog
- <http://www.enterprisecioforum.com/en/users/netsecrex>

Introduction

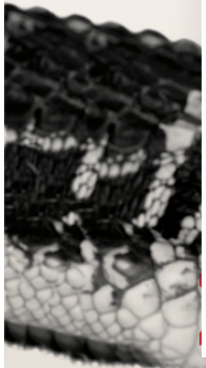


Agenda at a Glance

1. Removing the FUD
2. Vulnerabilities
3. Mobile Risk Factors and Considerations

Objective:

Provide a better understanding of the security risks related to smartdevices.



Removing FUD



February 21, 2013: Android represents 97% of mobile malware market



March 7, 2013: Android accounted for 79% of all mobile malware in 2012; 96% in Q4 alone.



March 26, 2013: iPhone more vulnerable than Android, BB, and WP combined



May 14, 2013: Mobile malware continues to rise; Android now at 91.3% of mobile malware market.

Mobile Risk Considerations: Removing the FUD



TOTAL CVE
210



TOTAL CVE
24



TOTAL CVE
11

SourceFire Report on Mobile Vulnerabilities:

http://www.phonearena.com/news/iPhone-more-vulnerable-than-Android-BB-and-WP-combined_id41258

Mobile Risk Considerations: Vulnerabilities



TOTAL CVE
243



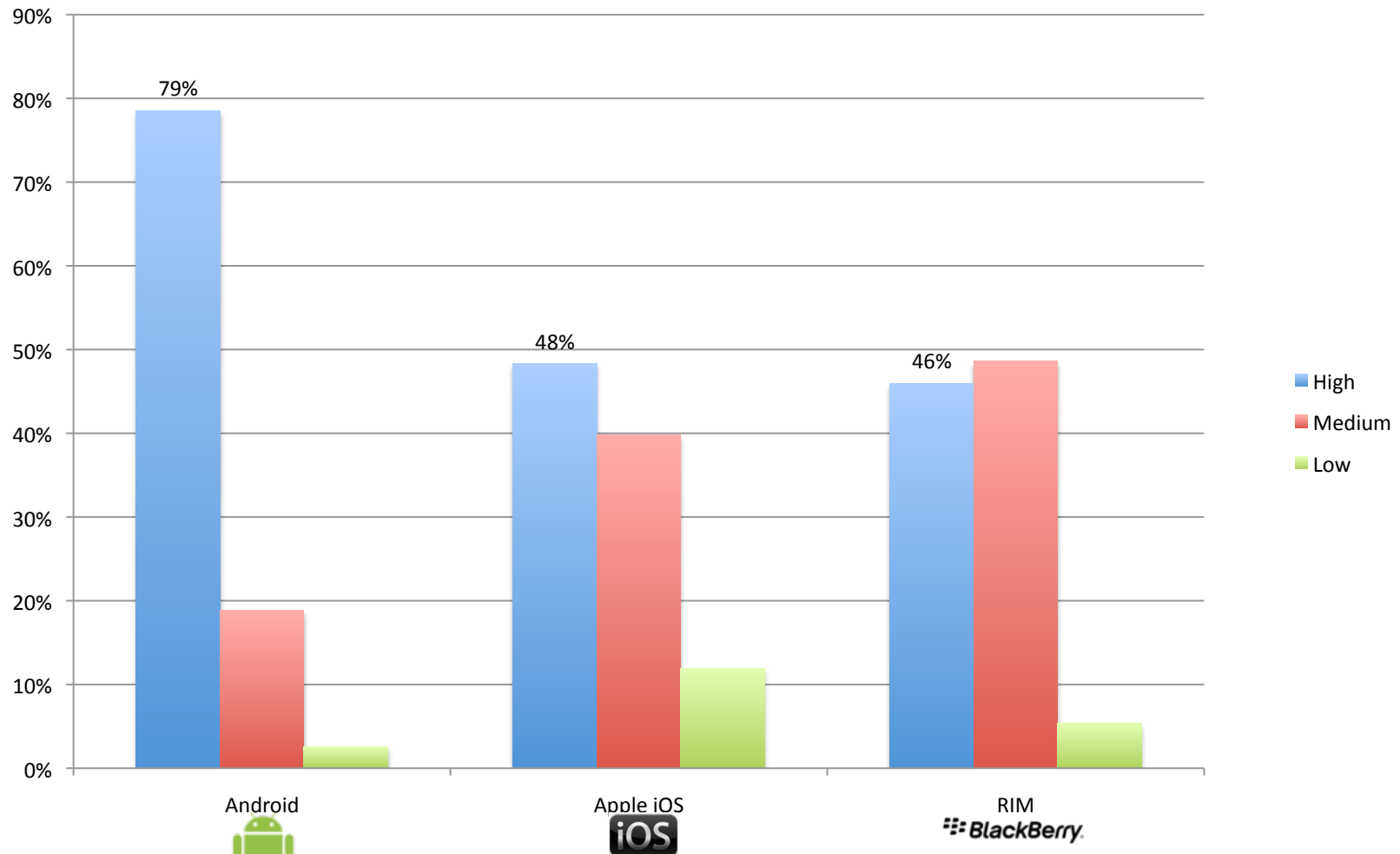
TOTAL CVE
194



TOTAL CVE
58

Patch Early, Patch Often...

Mobile Risk Considerations: Vulnerabilities (Another Look)





Backup Slides

1. Forensic/iOS Keychain

Case Study 2: iOS KeyChain Study



The Team

- Dan Ford (Fixmo)
- Amanda Hartle-Fennell (Symantec)



Goals

- Capture Data in Forensically Sound Method
 - Capture Enterprise Data: WiFi, VPN, Email authentication credentials
 - Capture Commonly Used Data From Private Apps
-

Case Study 2: Why look at the KeyChain?



iOS Keychain Weakness FAQ

Further Information on
iOS Password Protection

Jens Heider, Rachid El Khayari

Fraunhofer Institute for
Secure Information Technology (SIT)

July 16, 2012

Updated versions can be found at:
<http://sit4.me/ios-keychain-faq>

Versions Included:

- 4.3.3
- 4.3.5
- 5.0
- 5.0.1
- 5.1.1 (Last Update July 2012)

Case Study 2: Why look at the KeyChain?



Entry Description	Secret Type	kSecAttrAccessible
AOL Email	Password	AfterFirstUnlock
Apple ID	Private Keys	WhenUnlocked
Apple ID Authentication Password	Token	AfterFirstUnlock-ThisDeviceOnly
Apple Push	Token	AlwaysThisDeviceOnly
Apple Ubiquity (iCloud)	Certificates + Private Keys	AlwaysThisDeviceOnly
Apple-token-sync	Token	Always
Apps using default class	depends on App	WhenUnlocked
APSCIdentity	Certificate	AlwaysThisDeviceOnly
Backup Password	Password	WhenUnlocked-ThisDeviceOnly
Bluetooth Link Key	Key	AlwaysThisDeviceOnly
CardDAV	Password	AfterFirstUnlock
CalDAV	Password	AfterFirstUnlock
GMail Account	Password	AfterFirstUnlock
iChat message-prot.-key	Key	AlwaysThisDeviceOnly
Identity Certificate (e.g. VPN)	Certificate + Private Key	AlwaysThisDeviceOnly
ids Identity (probably iChat/iMessage)	Certificate + Private Key	AlwaysThisDeviceOnly
IMAP	Password	AfterFirstUnlock
iMessage Encryption Key	Key	AlwaysThisDeviceOnly

Entry Description	Secret Type	kSecAttrAccessible
iMessage Signing Key	Key	AlwaysThisDeviceOnly
iPhone Configuraton Utility	CA Certificates + Private Key	AlwaysThisDeviceOnly
LDAP	Password	WhenUnlocked
Lockdown-Identity	Certificate + Private Key	AlwaysThisDeviceOnly
MCEmail Account (probably created by IPCU profile)	plist with IMAP password	AlwaysThisDeviceOnly
MS Exchange	Password	AfterFirstUnlock
Passcode policy settings	plist with hashes of old passcodes	WhenUnlocked-ThisDeviceOnly
Passwords saved in Safari	Password	WhenUnlocked
SIM PIN	PIN	AlwaysThisDeviceOnly
SMTP	Password	AfterFirstUnlock
Subscribed Calendars	Password	AfterFirstUnlock
Visual Voicemail	Password	Always
VPN Passwords	Password	AfterFirstUnlock
VPN Certificates	Certificate + Private Key	AlwaysThisDeviceOnly
WiFi	Password	Always-ThisDeviceOnly* AfterFirstUnlock**
Yahoo Email	Token	AfterFirstUnlock

* If configured via iPhone Configuration Utility

** If configured on device

Case Study 2: Results



Enter your Exchange account information

Cancel Exchange Next

Email email@company.com

Domain Optional

Username Required

Password Required

Description My Exchange Account

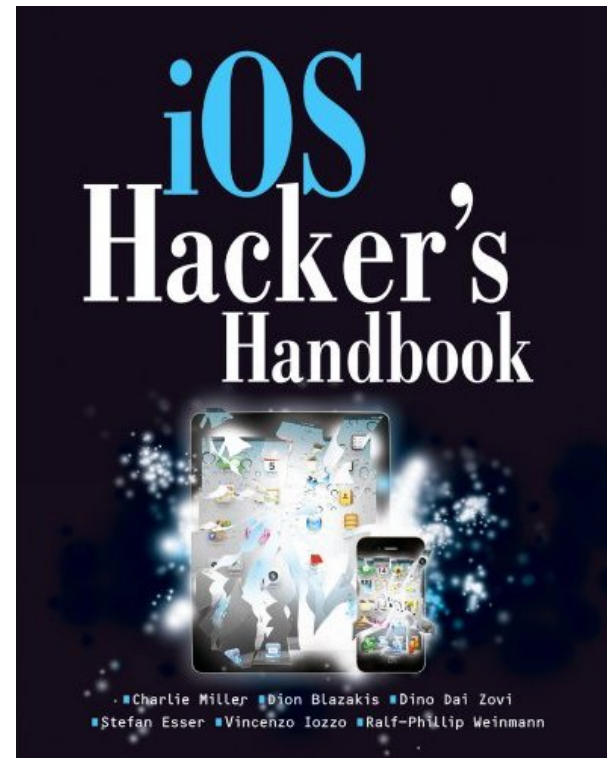
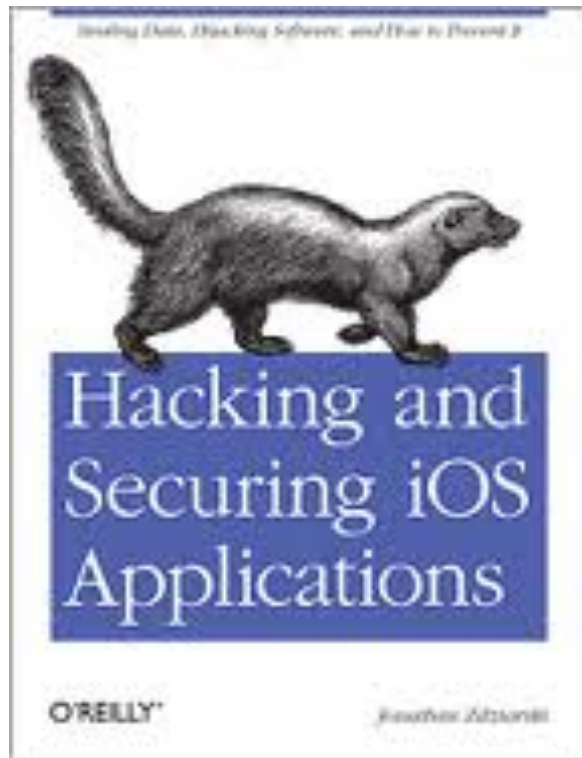


WELLS FARGO

Case Study 2: Partially Owned



Case Study 2: iOS KeyChain Study



Case Study 2: iOS KeyChain Study



Key	Type	Value
DKey	String	62585dd9962f42b0cb4a114b27c5c6b38429edb5
EMF	String	d25e427d4361882586de2f05152aa9dc45409727
KeyBagKeys	Data	<44415441 000004e4 56455253 00000004 0000
btMac	String	70:56:81:0e:27:8e
▶ classKeys	Diction...	(10 items)
dataVolumeOffset	Number	138240
dataVolumeUUID	String	721f3743bd40c67a
hwModel	String	N81AP
key835	String	65462658bf09d958e25d27d26d243d34
key89B	String	e11fd08cc6f88ac714a2b137db050058
lockers	Data	<6b4c3400 31474142 31474142 a9d62745 0399
passcode	String	0001
passcodeKey	String	b6eb808d7784ce221dee80cdfd5ee99511655864;
salt	String	f80f65a09fd8c6970fd2485f24279ae59cb96408
serialNumber	String	CCQHLQ85DNQW
udid	String	b607a4a1618917a3380dde5083ac179785e54ba2
uuid	String	c00976dcc49a47fdb90119caf00ae456
wifiMac	String	70:56:81:0a:d4:39

Case Study 2: iOS KeyChain Study



Keybag unlocked with passcode key
Keychain version : 5

----- Passwords -----

Service : AirPort
Account : mattress
Password : Ross!ditechedgolf
Agrp : apple

Service : ids
Account : identity-rsa-public-key
Password : <binary data> :
3082010a0282010100db560930ea89cb53e380fea64d9f0368f1ff5b71872-
ba5666ec346f3815f2f1615642a1209c36994f4e934313a287382d8d78e6b-
8eb7ee1d41c74138b44fda2fe3d934353ff290e07cf1ad8ff55f350203010
Agrp : apple

Service : AirPort
Account : Fixmo Network
Password : D0nt\$3ttle4good
Agrp : apple

Service : com.facebook.datr
Account :
Password : SqfYT-A587sxlKem_zWb02Z7
Agrp : T84QZS65DQ.platformFamily

Service : 45607F97-8620-48B5-8116-5D9020CE33A6.XAUTH
Account : VPN_Corp_Test
Password : Pwnd?
Agrp : apple

Service : MProfileRemovalPasscode
Account : 532D4A12-64A5-4446-8CE7-B629516A2FD2
Password : test123
Agrp : apple

Server : imap.gmail.com:143
Account : rschwalm@gmail.com
Password : M@tresse5

Server : smtp.gmail.com:25
Account : rschwalm@gmail.com
Password : M@tresse5

Server : :0
Account : DataAccess-52D50EBB-5DF2-4FEF-B6FD-B4873013F8A
Password : @mAnd@_3mAi!

Evidence that mobile threat looming



- Weakness in the iOS Keychain
- *Application Developers*
- *CVEs in iOS/Android/RIM*
- *Malicious Apps*



About Fixmo



Founded in 2009 with a focus on **Mobile Security and Risk Management**

“Enabling trusted and compliant mobile computing without compromise”



Focus on Security & Compliance

Help organizations protect the **integrity, privacy and compliance** of their mobile devices and corporate data
Security and compliance as an **enabler** for true mobility



Next Generation Mobile Security

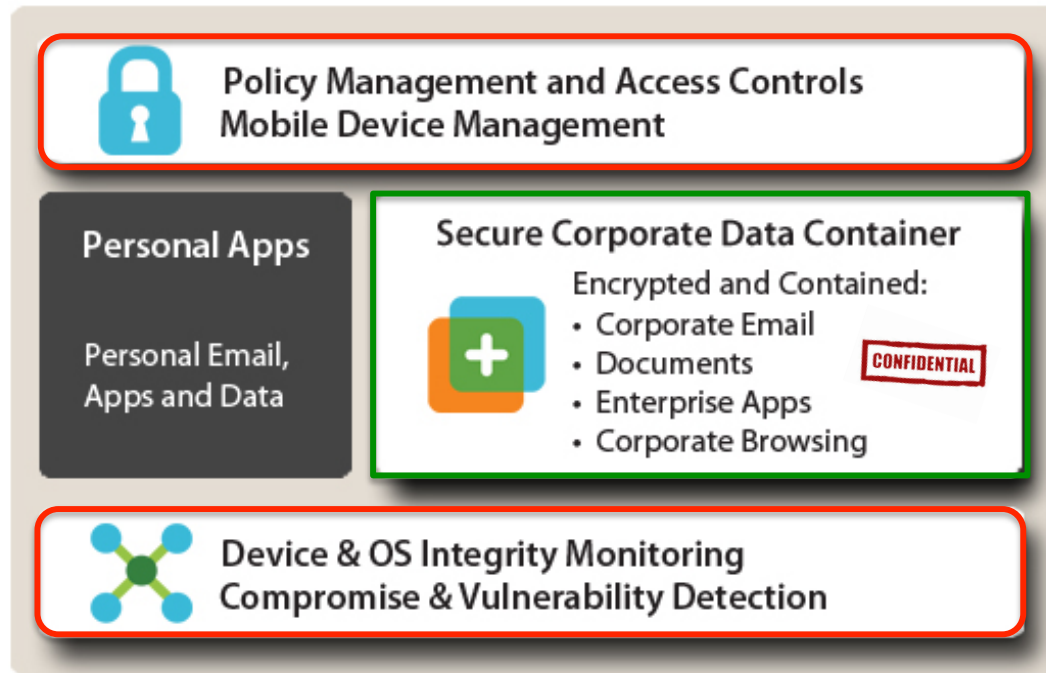
Designed for emerging risks of mobile computing and the realities of **bring-your-own-device (BYOD)**



Government Heritage

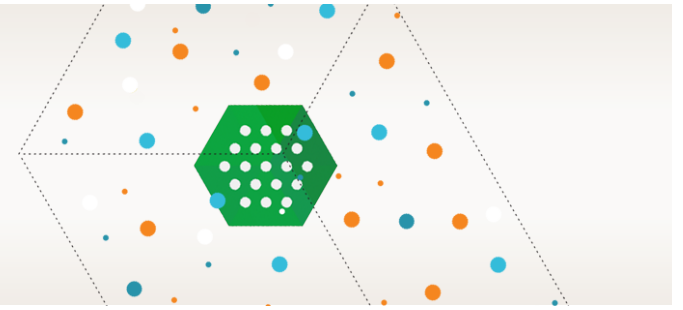
Core technology developed through a **Technology Transfer Program (TTP)** and CRADA with the **U.S. NSA**

Fixmo Mobile Security & Risk Management



Fixmo SafeZone Advantage

What makes our Secure Container unique?



- ✓ Designed as a Comprehensive Secure Workspace Environment with Email/PIM, Documents, Browsing and Apps – All in One
 - ✓ Fully Extensible to Custom Apps and 3rd Party Apps
-
- ✓ Defense-Grade Security Built on a “No-NOC” Architecture
 - ✓ FIPS 140-2 Encryption for all Corporate Data-at-rest and in-transit
-
- ✓ Support for S/MIME and Two-Factor Authentication
 - ✓ Deployable Independent of MDM Solution

Fixmo

The Mobile Risk Management Company



Dan Ford
Chief Security Officer, Fixmo

Daniel.ford@fixmo.com

@NetSecrex

The image features a background of thin, vertical, light blue lines on a light gray gradient. A solid teal horizontal bar spans the width of the image, containing the text. Below the teal bar is a thin yellow line, and at the very bottom is a gray gradient bar.

Mr. Daniel Taylor – Microsoft

danielta@microsoft.com


The image features a background of thin, vertical, light blue lines on a light gray gradient. A solid teal horizontal bar spans the width of the image, containing the text. Below the teal bar is a thin yellow line, and at the very bottom is a gray gradient bar.

Mr. Brian Hajost – SteelCloud

bhajost@steelcloud.com



“Industry Involvement in Process Acceleration”



Brian Hajost
President & CEO
M: 703-926-8291
bhajost@steelcloud.com

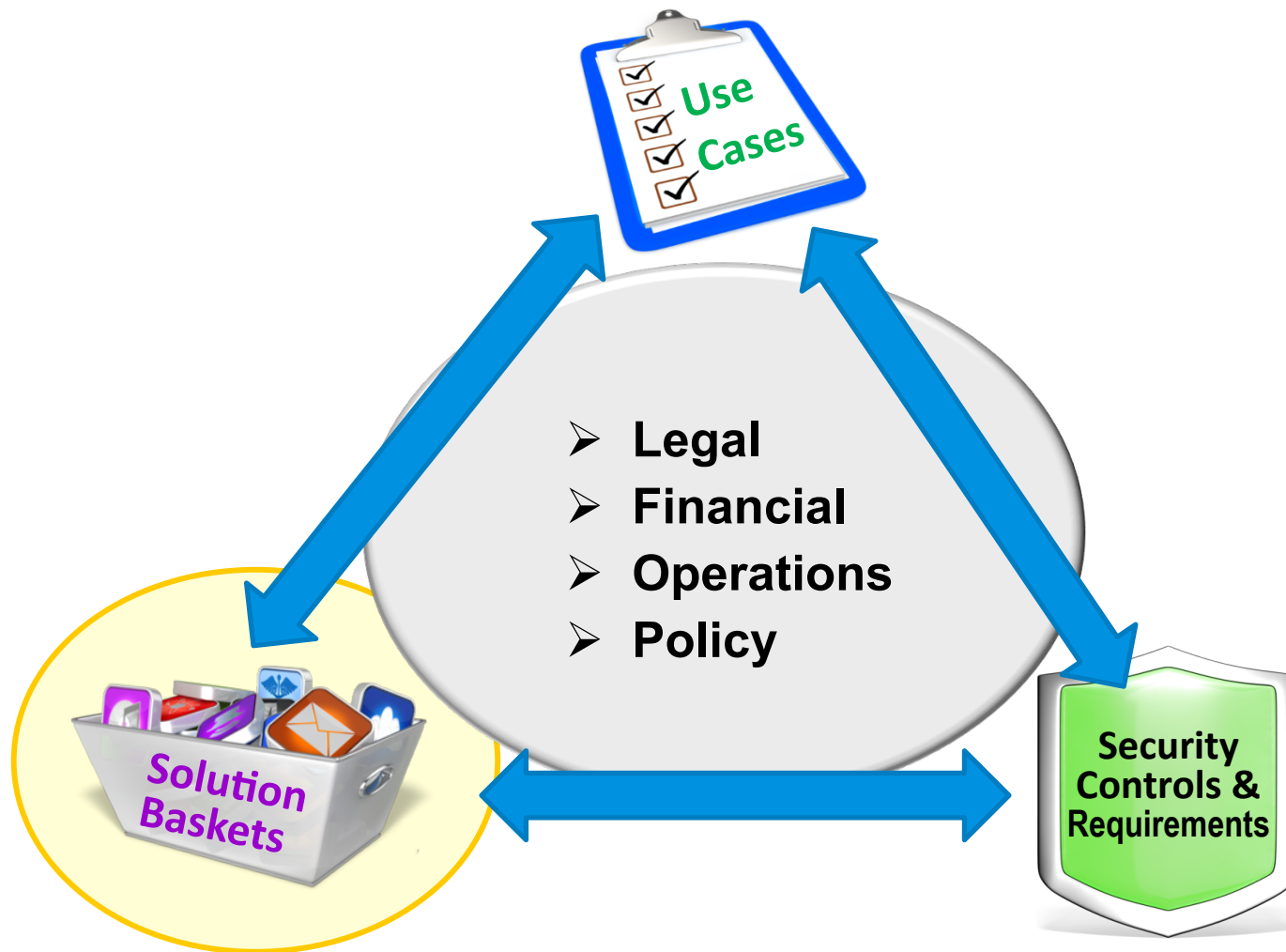


Traditional Process

Defining Requirements



ACFEA DC MWG Initiative – *Helping the Process*



ACFEA DC MWG Initiative – *In Action*

Agency/Component Use Cases



*User
Questionnaire*



Solution Baskets

Open Forum

Ask your all
your questions
now.

Dr. Rocky Young
robert.young@osd.mil

Mr. Mark Norton
mark.norton@osd.mil

Mr. Kevin Cox
kevin.cox@usdoj.gov

Mr. Gary Bode
gary.bode@us.army.mil

Mr. Daniel Ford
daniel.ford@fixmo.com

Mr. Daniel Taylor
danielta@microsoft.com

Mr. Brian Hajost
bhajost@steelcloud.com