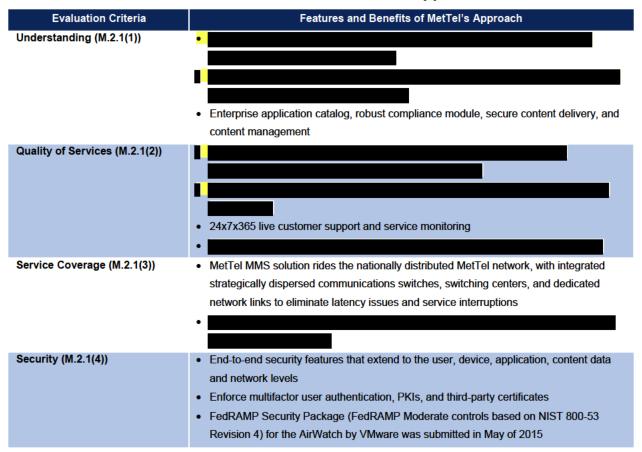


2.1.13.1 Compliance with Evaluation Criteria [L.29.2.1]

The MetTel MMS solution fulfills the mandatory service requirements for MMS C.2.8.6. This section presents a technical description of our offering, demonstrating our capabilities in Standards, Connectivity, Technical Capabilities, Features, Performance Metrics, and Security. **Exhibit 2.1.13-1** highlights some key strengths and benefits of our MMS solution.



Exhibit 2.1.13-1. Features and Benefits of Approach to MMS



2.1.13.1.1 Service and Functional Description [L.29.2.1, C.2.8.6.1, C.2.8.6.1.1]

MMS helps Agencies transition to a more complex mobile computing and communications environment by supporting security, network services, and software and hardware management for mobile handheld devices. This is especially important as many Agencies focus more on BYOD initiatives and advanced wireless computing.

MMS is a core capability for effectively scaling the secure deployment and management of mobile applications, enterprise data on mobile devices, and management of the devices and mobile platforms. The optimal balance between security, total costs, and functionality provides the most business value to Agencies.



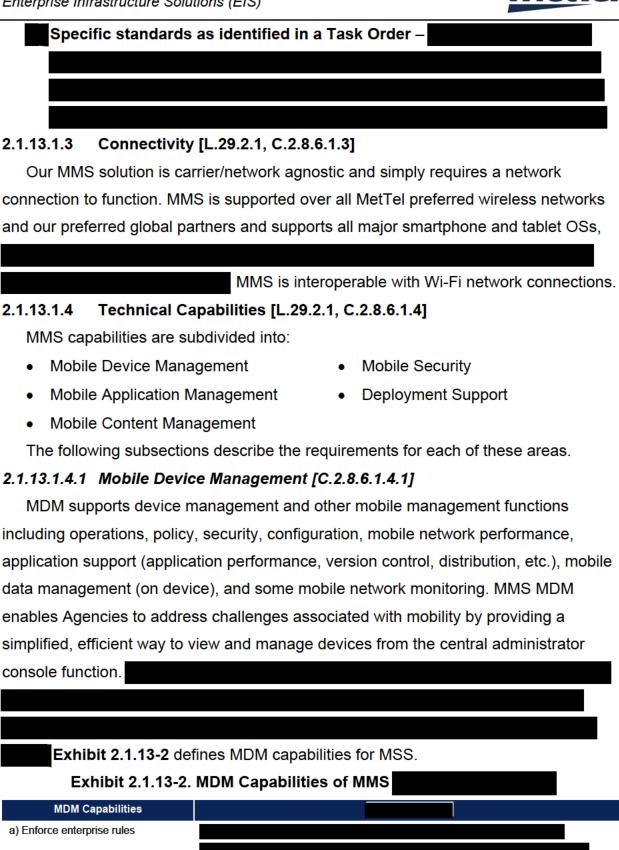


Functional Description

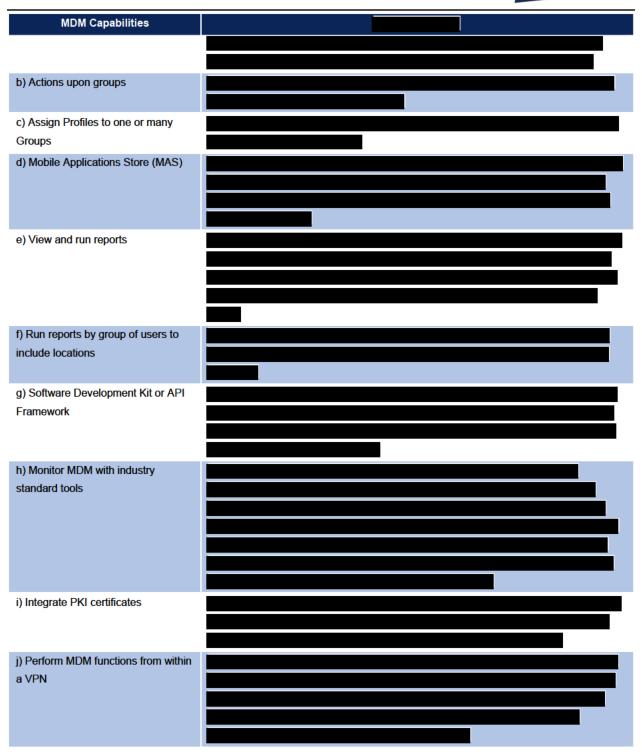
MMS supports mobile computing by allowing Agency-owned and personal mobile handheld devices (smartphones and tablets, based on smartphone OSs) to access Agency networks and applications in accordance with the Agency's IT security policy. MMS supports Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM), mobile security, and deployment support.

(IVIAIVI),	, Mobile Content Management (MCM), mobile security, and deployment support.
• /	Agencies configure MMS in conformance to security policies, ensuring the
ı	mobile device fleet is compliant regardless of device ownership (i.e., BYOD)
_	
• [MMS makes it easy to deploy secure MDM, MAM, MCM solutions for the entire
	Agency device fleet
2.1.13.	1.2 Standards [L.29.2.1, C.2.8.6.1.2]
Met	tTel MMS complies with all the following standards:
	FISMA Moderate Impact level standards –
Ī	
2.	NIST 800-53 – The MetTel MMS Information Security Program is modeled using
	NIST 800-53 – The MetTel MMS Information Security Program is modeled using industry best practices and regulatory standards, including NIST SP 800-53
i	industry best practices and regulatory standards, including NIST SP 800-53
i 	industry best practices and regulatory standards, including NIST SP 800-53 which typically aligns with customer policies and programs.
i 	industry best practices and regulatory standards, including NIST SP 800-53
i 	industry best practices and regulatory standards, including NIST SP 800-53 which typically aligns with customer policies and programs.
i \ 	industry best practices and regulatory standards, including NIST SP 800-53 which typically aligns with customer policies and programs.









Device enrollment is a key capability to ensure the MMS enforces Agency policies. **Exhibit 2.1.13-3** identifies the elements available when adding a device to the MDM management domain in the MMS.



Exhibit 2.1.13-3. MDM Device Enrollment Capabilities

Capabilities	Compliant	
a) Set a Target Platform	Yes	
b) Use a Target Device Model for profile	Yes	
c) Specify minimum OS version	Yes	
d) Target Device Ownership	Yes	
e) Allow a user to edit any field for a "live" or "active" profile	Yes	
f) Allow a user to self-enroll an Agency GFP or BYOD device	Yes	
g) Centrally manage multiple devices	Yes	
h) Support different policies or grouping for multiple devices under one user	Yes	
i) Apply multiple policies to devices simultaneously	Yes	
j) Use external directory service repository for enrollment.	Yes	
k) Use federated and multi-factor authentication for enrollment	Yes	
Set support email and phone information for registration messages	Yes	
m) Redirect users to a URL upon successful enrollment	Yes	
n) Edit an enrollment activation notification message to user	Yes	
o) Set a default Device Ownership type upon enrollment for different groups	Yes	
p) Use an internal user list for enrollment for different groups	Yes	
 q) Set support email and phone information for registration messages for different groups 	Yes	
r) Edit an enrollment activation notification message to the user or group of users	Yes	

Vol. 1 Technical

RFP No. QTA0015THA3003



Exhibit

Capabilities	Compliant	
s) Send a user or group an activation	Yes	
enrollment message		

Device profiles define users and group capabilities in the MMS and are key to enforcing Agency policies.

2.1.13-4 defines the requirements for device profiles and MetTel's response.

Exhibit 2.1.13-4. MMS Device Profiles

	Capabilities	Compliant
a) Cr	reate a profile template	Yes
b) Co	ppy profiles	Yes
c) Ed	dit a "live" or "active" profile	Yes
d) Se	et profile removal permissions	Yes
e) Se	et Profile Start Date	Yes
f) Se	et Profile End Date	Yes
cu	utomatically update a device that irrently has a profile when editing that ofile	Yes
h) Pu	ısh a profile to an individual device	Yes
de	utomatically remove profiles from evices whose state changes from alifying to not-qualifying	Yes
as	upport multiple profiles being applied to single device (most restrictive rules oply)	Yes
k) De	elete a profile from the MDM system	Yes
I) Se	et a description for a profile	Yes
m)Ma	anage the following via a profile:	
İ.	Install applications	Yes
ii.	Control use of camera	Yes
iii.	Control use of installed applications, including default applications	Yes
İV.	Allow multiple Wi-Fi configurations for a single profile	Yes
V.	Manage device Wi-Fi settings via a MDM policy	Yes
vi.	Control Wi-Fi Security Type	Yes



	Capabilities	Compliant	
Vii.	Multiple VPN configurations for a single profile	Yes	
Viii.	VPN Connection (or Policy) Type	Yes	
ix.	VPN Connection Proxy for a VPN configuration	Yes	
X .	Multiple email/calendar/contact configurations per profile	Yes	
Xİ.	Multiple Web Clip / Web Shortcut configurations per profile	Yes	

Device feature management provides control of the features in devices and the flexibility to enable or disable specific features. **Exhibit 2.1.13-5** defines the required set of device feature management capabilities.

Exhibit 2.1.13-5. MMS Device Feature Management Capabilities

	Capabilities	Compliant	
-	ulti-OS support – Manage multiple OS vices	Yes	
	evice passcode enforcement omplexity, length, presence)	Yes	
c) Ins	stallation of applications (See MAM)	Yes	
d) Ca	nmera (enable/disable)	Yes	
e) Co	ontrol radios/communications	Yes	
İ.	Wi-Fi (enable/disable)	Yes	
ii.	Bluetooth (enable/disable)	Yes	
iii.	Enable or disable specific hardware component and uses	Yes	
iv.	Near Field Communications (NFC) (enable/disable)	Yes	_
V.	Enable/disable GPS	Yes	
vi.	Store Enterprise/Agency data to removable media (disable)	Yes	

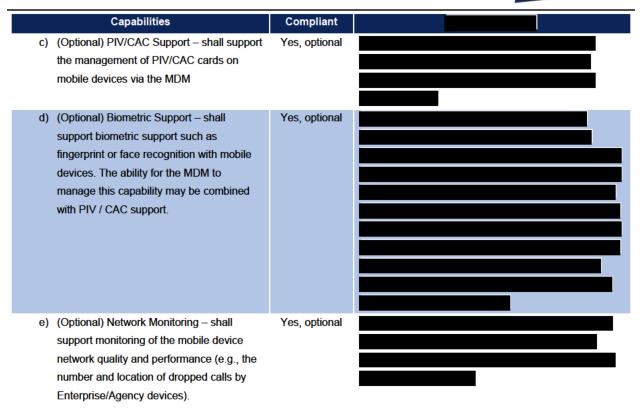


MDM provides a robust set of additional management capabilities for an Agency to control the mobile fleet as required to meet operational requirements. **Exhibit 2.1.13-6** provides the MetTel response to the required MDM capabilities.

Exhibit 2.1.13-6. Additional MDM Capabilities

	Comphilities	Campliant
_	Capabilities	Compliant
5.	Data Management – read, write, transmit, and	Yes
	receive data on mobile devices as well as with	
	backend systems/repositories	V
a) File Management – to secure data, files, and	Yes
	applications (e.g., pdf files or Word docs) on a mobile device	
L.		Vee
) Personal Information Management	Yes
6.	NIST SP 800-126 Security Content	Yes
	Automation Protocol (SCAP) support for the	
	server-side components, including asset	
	management, configuration management,	
	patch management, and remediation	
	capabilities	
7 [Device Inventory Management and Reports	Yes
8. 5	System Performance Reports	Yes
	ADM Consuit (Consultance Depot	V
9. N	ADM Security/Compliance Reports	Yes
10	Capabilities that may be defined in the Task	
Ord		
		Voc optional
	 a) (Optional) Quality of Service (QoS) – shall support QoS capabilities to prioritize real- 	Yes, optional
	time or latency-sensitive application data	
	• • • • • • • • • • • • • • • • • • • •	
	where appropriate (e.g., VoIP, video, real-	
	time chat). It shall be possible to enforce and exclude QoS priority by application or	
	protocol to prevent non-real-time	
	applications from inappropriately increasing	
	their traffic priority.	
		Voc antional
	b) (Optional) Classified Data – shall support	Yes, optional
	access classified data up to the SECRET level via mobile devices.	
	level via filobile devices.	





2.1.13.1.4.2 Mobile Application Management [C.2.8.6.1.4.2]

Mobile applications are changing the way people work. Mobile users demand applications that connect them to enterprise resources, increase their productivity, and promote collaboration with colleagues.

MAM capabilities include Application Deployment, MAS, Application Security, and some optional capabilities that may be defined at the Task Order level. MetTel MMS is fully compliant with these requirements. **Exhibit 2.1.13-7** through **Exhibit 2.1.13-10** define the MetTel response to MAM capabilities.

Exhibit 2.1.13-7. Application Deployment

Capabilities	Compliant	
a) Commercial Application Store	Yes	Sta
b) Reporting of installed applications	Yes	
c) Block Application Purchase	Yes	
d) Application Whitelisting/Blacklisting	Yes	
e) Staged/controlled application	Yes	
deployment.		



The MAM provides the user the ability to select private enterprise or Agency applications for installation on managed devices. MAS is integrated into the MDM on the MetTel EIS Portal and allows application provisioning by group policy and mandatory application deployment. MAS supports the capabilities defined in **Exhibit 2.1.13-8**.

Exhibit 2.1.13-8. Mobile Application Store

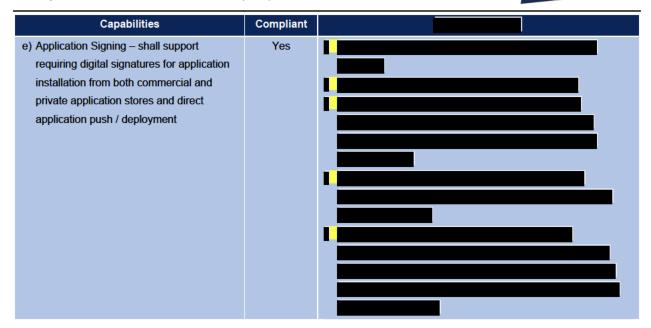
	Capabilities	Compliant	
i.	Add/update an application from a Commercial Application Store to the MAS	Yes	
ii.	Add additional metadata to and report on metadata on any application added to the MAS (name, description, version, OS, keywords, etc.)	Yes	
iii.	Add/update an enterprise/Agency application to the MAS via a web GUI	Yes	
iv.	Specify the effective date for an Agency internal application	Yes	
٧.	Specify the expiration date for an Agency internal application	Yes	
vi.	Specify the minimum operating system and model for an Agency internal application	Yes	
vii.	Download Agency internal and public applications from MAS	Yes	
viii.	Categorize, group, or tag applications (e.g., business applications, scientific applications, etc.)	Yes	

Application Security provides the capability to approve applications for operation and protect the applications on the wireless device as a key element of the overall MAM. **Exhibit 2.1.13-9** lists MDM Application Security capabilities.

Exhibit 2.1.13-9. MAM Application Security

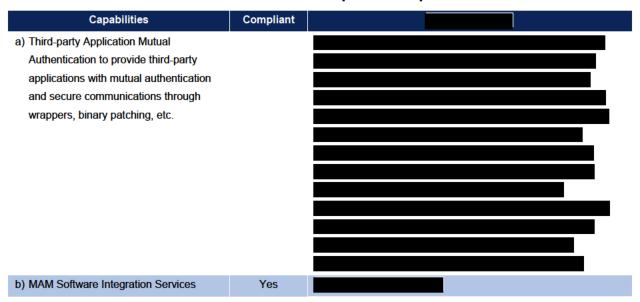
	Capabilities	Compliant
a) M	utual Authentication	Yes
b) Ap	oplication Installation Control	Yes
c) Bl	acklisting / Whitelisting	Yes
de	oplication Environment Requirements – etect and enforce device environment enditions such as:	Yes
i.	Minimum or specific operating system versions	Yes
ii.	Required presence or absence of other applications	Yes
iii.	Absence of privilege escalation ("rooting" or "jai breaking")	Yes





An Agency may define optional capabilities in a Task Order. **Exhibit 2.1.13-10** defines MAM optional capabilities.

Exhibit 2.1.13-10. MAM Optional Capabilities



2.1.13.1.4.3 Mobile Content Management [C.2.8.6.1.4.3]





Accessible, round-the-clock mobile connectivity drives modern enterprise productivity. The proliferation of consumer mobility drives demand for a simple and ubiquitous content collaboration solution.

These

integrated solutions empower the mobile workforce and provide unprecedented innovation and networking without compromising data security and granular control.

MCM enables secure mobile access to content anytime, anywhere, and on any device. MCM protects sensitive content and provides a central application to securely access, store, update, and distribute documents. Mobile Security and Deployment Support are the key elements of MCM and are defined in the following sections.

2.1.13.1.4.4 Mobile Security [C.2.8.6.1.4.4]

Exhibit 2.1.13-11 provides the MetTel response to the requirements for Mobile Security defined in EIS RFP Section C.2.8.6.1.4.4. The MetTel MMS solution complies with all mobile security requirements in this section.

Exhibit 2.1.13-11. Mobile Security Capabilities of MMS

Capabilities	Compliant	
Enroll a device before applying any policy (null Policy)	Yes	
Create Whitelists/Blacklists for device enrollment to include OS versions and device models	Yes	
 Allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise as individuals or to groups under the MDM 	Yes	
Use an existing MDM user attribute repository for enrollment to the new MDM system	Yes	
5. Take action based on compliance rules	Yes	
6. Block the device or erase (wipe) only the managed data on a device under the following conditions:		
a) Blacklisted	Yes	
b) Exceed a set number of failed login attempts	Yes	
c) Exceed defined interval for contacting MDM (policy based)	Yes	
 d) Detection of OS jailbreaking or application tampering (policy based) 	Yes	
e) Any other policy violation	Yes	



Capabilities	Compliant	
f) Remote instruction from MDM (manual)	Yes	
7. Password policy enforcement:		
a) Minimum complexity (length, composition, common words, etc.)	Yes	
b) Password lifetime limit	Yes	
c) Password re-use limits	Yes	
d) Password inactivity timeout	Yes	
e) Report password failures beyond threshold to MDM	Yes	
f) Maximum password attempts before lock or wipe	Yes	
8. Mask passwords when they appear in the Management GUI	Yes	
Determine which administrative user made a configuration change in the MDM administrative environment	Yes	
 Determine which device user made a configuration change in the MDM console (self-service logging) 	Yes	
11. Installation and configuration (update, revocation checking) of individual and group authentication certificates for the following purposes:	Yes	
a) Email (S/MIME) signing and encryption	Yes	
b) Wi-Fi Configuration	Yes	
c) VPN Configuration	Yes	
12. Send/receive (encrypt and sign, decrypt and verify)	Yes	
 Restrict downloading attachments, copying of data to/from removable media 	Yes	
(Optional) View the current GPS location of a device or logical grouping of devices on a map	Yes	
15. Encrypt the data in transit between the MDM and the device in accordance with FIPS 140-2	Yes	
16. Data at rest on a mobile device	Yes	
17. User Authentication shall support PIN or password authentication for the managed applications and optionally multifactor authentication with any two of the following three authentication types:	Yes	
a) Shared Secret	Yes	



	Capabilities	Compliant	
	b) Token	Yes	
	c) Biometric	Yes	
18.	User Compliance:		
	a) Set up compliance rules to include custom compliance rules for profiles, devices, groups, and Whitelist/Blacklist	Yes	
	b) Activate/deactivate a compliance rule	Yes	
	c) Specify user and group rules for application	Yes	
	d) Provide enterprise-level compliance reports	Yes	
19.	Alerting – notify Agency operations staff about Agency devices:		
	a) Set up custom alerts to users and management based on various parameters	Yes	
	b) Send custom alerts to one or more user roles including administrators	Yes	
	c) Specify a creation policy for custom alerts to include having various alert severity levels		
	d) Create automated alerts for security issues such as compromised devices	Yes	
	e) Create alerts based on device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.	Yes	
	f) View alerts pending acknowledgement	Yes	
	g) Acknowledge alerts and track acknowledgements	Yes	
20.	Audit reports – as defined in a Task Order:	Yes	
	Administrator activity (i.e., actions performed, time stamps)	Yes	
	b) User access times and enrollments	Yes	
	c) Devices (i.e., number of devices by Agency and across all sub-Agencies, type, OS version)	Yes	
	d) Console logins and functions (connections to the management console, actions performed, etc.)	Yes	
	e) Policy changes and versions (policy revision control and historical changes)	Yes	
	f) Policy violations	Yes	
21.	Safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122	Yes	



Capabilities	Compliant	

2.1.13.1.4.5 Deployment Support [C.2.8.6.1.4.5]

End user experience across multiple components (i.e., laptops, tablets, and smartphones) has been difficult and disruptive in the past. As mobile technology evolves, users demand a consistent experience across all devices. Our MMS platform provides leading enterprise-grade solutions across every device, every operating system, and every mobile deployment.

Exhibit 2.1.13-12 summarizes deployment options with the MetTel MMS solution.

Exhibit 2.1.13-12. Mobile Deployment Support



The MetTel MMS solution provides deployment capabilities in full compliance with the EIS RFP stated capabilities.

1. Deployment

MetTel provides a comprehensive implementation package
Initially, our team assesses requirements,
consults on options, demonstrates capabilities, and assists with other project needs.
Whatever the mobile enterprise requirements, we provide personalized and professional
consultation services to ensure our solution addresses key mobility concerns. A
consultant works with users to build out the project plan with specific milestones and
deliverables including assisting the Agency with accreditation and authorization
(compliance) objectives. MMS supports integration with existing enterprise
infrastructures and systems.

We understand the importance of industry standards

Our due



diligence demonstrates our commitment to preserve the confidentiality, integrity, and availability of data while implementing appropriate security measures and monitoring systems. The MMS data center operations team leverages a documented methodology encompassing configuration, capacity, change, service level, availability, and incident and problem management policies and processes.

2. Enterprise System Integration

MetTel assists with deploying and integrating MMS into the Agency-wide environment. We securely integrate with Active Directory (AD) and Lightweight Directory Access Protocol (LDAP), certificate authorities, email infrastructures, and other enterprise systems in a cloud and on-premise deployment model to preserve the Agency investment in existing enterprise resources, centralize mobility management, and streamline user enablement. We integrate Trouble Ticketing with the MetTel EIS Portal to provide enterprise-wide trouble management and reporting.

3. Training

MetTel provides MDM and MAM solution training materials, online training, and additional training resources.

4. Help Desk

The MetTel EIS Help Desk provides MDM and MAM support for all EIS users and Agencies. Users initiate support for trouble request and resolution via email or telephone or by creating an online Trouble Ticket.

2.1.13.1.5 Features [L.29.2.1, C.2.8.6.2]

No features are specified for MMS.

2.1.13.1.6 Interfaces [L.29.2.1, C.2.8.6.3]

MetTel MMS supports UNIs for all smartphones and tablets running smartphone operating systems across 3G/4G Cellular Service based on CDMA, GSM, and LTE standards as required. The SRE Catalogue lists all SREs with the designation "Wireless" in the Note column.



2.1.13.1.7 Performance Metrics [L.29.2.1, C.2.8.6.4]

The MetTel EIS Portal supports the EIS Services Trouble Management System (TMS). All KPIs for MMS are met and reported through the TMS. Users can query the status of Trouble Tickets and their status against the KPIs and performance thresholds. The TMS complies with the event notification values and the severity they indicate.