2.1.13 Managed Mobility Service [C.2.8.6]

[redacted]

- Satisfies strict Government security standards and FISMA compliance
- FIPS 140-2 and AES 256 compliant
- Flexible deployment options built to scale with growing Agency requirements
- Containerized solutions to protect Government data, applications, email, and browsing on employee-owned devices (BYOD)

[redacted] Our management solutions enable organizations to securely manage large-scale deployments of mobile devices, [redacted], from a single web-based console.

[redacted] Combined with the extensive inventory and telecommunications expense management capabilities of the MetTel EIS Portal, the Agency has all the information necessary to effectively and efficiently manage the complete network, wireline and wireless.

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

Evaluation Criteria	Features and Benefits of MetTel's Approach
Understanding (M.2.1(1))	• [redacted] • Enterprise application catalog, robust compliance module, secure content delivery, and content management
Quality of Services (M.2.1(2))	• [redacted] • 24x7x365 live customer support and service monitoring • [redacted]
Service Coverage (M.2.1(3))	• MetTel MMS solution rides the nationally distributed MetTel network, with integrated strategically dispersed communications switches, switching centers, and dedicated network links to eliminate latency issues and service interruptions • [redacted]
Security (M.2.1(4))	• End-to-end security features that extend to the user, device, application, content data and network levels • Enforce multifactor user authentication, PKIs, and third-party certificates • FedRAMP Security Package (FedRAMP Moderate controls based on NIST 800-53 Revision 4) for the AirWatch by VMware was submitted in May of 2015

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.

[redacted]

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.

- Agencies **configure MMS** in conformance to security policies, ensuring the 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]

MetTel MMS complies with all the following standards:

FISMA Moderate Impact level standards –

2. **NIST 800-53** – The MetTel MMS Information Security Program is modeled using industry best practices and regulatory standards, including NIST SP 800-53 which typically aligns with customer policies and programs.

FIPS-140-2 – MMS is fully FIPS 140-2 compliant,

4. **IPv4 and IPv6** – MMS supports both IPv4 and IPv6 addressing.

Specific standards as identified in a Task Order –

2.1.13.1.3 Connectivity [L.29.2.1, C.2.8.6.1.3]

Our MMS solution is carrier/network agnostic and simply requires a network connection to function. MMS is supported over all MetTel preferred wireless networks and our preferred global partners and supports all major smartphone and tablet OSs, MMS is interoperable with Wi-Fi network connections.

2.1.13.1.4 Technical Capabilities [L.29.2.1, C.2.8.6.1.4]

MMS capabilities are subdivided into:

- Mobile Device Management
- Mobile Application Management
- Mobile Content Management
- Mobile Security
- Deployment Support

The following subsections describe the requirements for each of these areas.

2.1.13.1.4.1 Mobile Device Management [C.2.8.6.1.4.1]

MDM supports device management and other mobile management functions including operations, policy, security, configuration, mobile network performance, application support (application performance, version control, distribution, etc.), mobile data management (on device), and some mobile network monitoring. MMS MDM enables Agencies to address challenges associated with mobility by providing a simplified, efficient way to view and manage devices from the central administrator console function.

Exhibit 2.1.13-2 defines MDM capabilities for MSS.

Exhibit 2.1.13-2. MDM Capabilities of MMS

MDM Capabilities	
a) Enforce enterprise rules	

MDM Capabilities	[redacted]
	[redacted]
b) Actions upon groups	[redacted]
c) Assign Profiles to one or many Groups	[redacted]
d) Mobile Applications Store (MAS)	[redacted]
e) View and run reports	[redacted]
f) Run reports by group of users to include locations	[redacted]
g) Software Development Kit or API Framework	[redacted]
h) Monitor MDM with industry standard tools	[redacted]
i) Integrate PKI certificates	[redacted]
j) Perform MDM functions from within a VPN	[redacted]

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

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

Device profiles define users and group capabilities in the MMS and are key to enforcing Agency policies. [redacted] **Exhibit 2.1.13-4** defines the requirements for device profiles and MetTel's response.

Exhibit 2.1.13-4. MMS Device Profiles

Capabilities	Compliant	[redacted]
a) Create a profile template	Yes	[redacted]
b) Copy profiles	Yes	[redacted]
c) Edit a "live" or "active" profile	Yes	[redacted]
d) Set profile removal permissions	Yes	[redacted]
e) Set Profile Start Date	Yes	[redacted]
f) Set Profile End Date	Yes	[redacted]
g) Automatically update a device that currently has a profile when editing that profile	Yes	[redacted]
h) Push a profile to an individual device	Yes	[redacted]
i) Automatically remove profiles from devices whose state changes from qualifying to not-qualifying	Yes	[redacted]
j) Support multiple profiles being applied to a single device (most restrictive rules apply)	Yes	[redacted]
k) Delete a profile from the MDM system	Yes	[redacted]
l) Set a description for a profile	Yes	[redacted]
m)Manage the following via a profile:		
i. Install applications	Yes	[redacted]
ii. Control use of camera	Yes	[redacted]
iii. Control use of installed applications, including default applications	Yes	[redacted]
iv. Allow multiple Wi-Fi configurations for a single profile	Yes	[redacted]
v. Manage device Wi-Fi settings via a MDM policy	Yes	[redacted]
vi. Control Wi-Fi Security Type	Yes	[redacted]

Capabilities	Compliant	[redacted]
vii. Multiple VPN configurations for a single profile	Yes	[redacted]
viii. VPN Connection (or Policy) Type	Yes	[redacted]
ix. VPN Connection Proxy for a VPN configuration	Yes	[redacted]
x. Multiple email/calendar/contact configurations per profile	Yes	[redacted]
xi. Multiple Web Clip / Web Shortcut configurations per profile	Yes	[redacted]

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	[redacted]
a) Multi-OS support – Manage multiple OS devices	Yes	[redacted]
b) Device passcode enforcement (complexity, length, presence)	Yes	[redacted]
c) Installation of applications (See MAM)	Yes	[redacted]
d) Camera (enable/disable)	Yes	[redacted]
e) Control radios/communications	Yes	[redacted]
i. Wi-Fi (enable/disable)	Yes	[redacted]
ii. Bluetooth (enable/disable)	Yes	[redacted]
iii. Enable or disable specific hardware component and uses	Yes	[redacted]
iv. Near Field Communications (NFC) (enable/disable)	Yes	[redacted]
v. Enable/disable GPS	Yes	[redacted]
vi. Store Enterprise/Agency data to removable media (disable)	Yes	[redacted]

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

Capabilities	Compliant	[redacted]
5. Data Management – read, write, transmit, and receive data on mobile devices as well as with backend systems/repositories	Yes	[redacted]
a) File Management – to secure data, files, and applications (e.g., pdf files or Word docs) on a mobile device	Yes	[redacted]
b) Personal Information Management	Yes	[redacted]
6. NIST SP 800-126 Security Content Automation Protocol (SCAP) support for the server-side components, including asset management, configuration management, patch management, and remediation capabilities	Yes	[redacted]
7. Device Inventory Management and Reports	Yes	[redacted]
8. System Performance Reports	Yes	[redacted]
9. MDM Security/Compliance Reports	Yes	[redacted]
10. Capabilities that may be defined in the Task Order:		
a) (Optional) Quality of Service (QoS) – shall support QoS capabilities to prioritize real-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.	Yes, optional	[redacted]
b) (Optional) Classified Data – shall support access classified data up to the SECRET level via mobile devices.	Yes, optional	[redacted]

Capabilities	Compliant	[redacted]
c) (Optional) PIV/CAC Support – shall support the management of PIV/CAC cards on mobile devices via the MDM	Yes, optional	[redacted]
d) (Optional) Biometric Support – shall support biometric support such as fingerprint or face recognition with mobile devices. The ability for the MDM to manage this capability may be combined with PIV / CAC support.	Yes, optional	[redacted]
e) (Optional) Network Monitoring – shall support monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by Enterprise/Agency devices).	Yes, optional	[redacted]

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. [redacted]

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

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

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	[redacted]
a) Mutual Authentication	Yes	[redacted]
b) Application Installation Control	Yes	[redacted]
c) Blacklisting / Whitelisting	Yes	[redacted]
d) Application Environment Requirements – detect and enforce device environment conditions such as:	Yes	[redacted]
i. Minimum or specific operating system versions	Yes	[redacted]
ii. Required presence or absence of other applications	Yes	[redacted]
iii. Absence of privilege escalation ("rooting" or "jai breaking")	Yes	[redacted]

Capabilities	Compliant	[redacted]
e) Application Signing – shall support requiring digital signatures for application installation from both commercial and private application stores and direct application push / deployment	Yes	[redacted]

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

Capabilities	Compliant	[redacted]
a) Third-party Application Mutual Authentication to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.		[redacted]
b) MAM Software Integration Services	Yes	[redacted]

2.1.13.1.4.3 Mobile Content Management [C.2.8.6.1.4.3]

[redacted]

[redacted]

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. [redacted] 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 [redacted] complies with all mobile security requirements in this section.

Exhibit 2.1.13-11. Mobile Security Capabilities of MMS

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

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

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

Capabilities	Compliant	[redacted]
		[redacted]

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. [redacted]

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

Exhibit 2.1.13-12. Mobile Deployment Support

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

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

1. Deployment

MetTel provides a comprehensive implementation package [redacted] 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 [redacted] 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. [redacted]

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.