TASK ORDER REQUEST (TOR)

GSC-QFOB-XX-XXXX

Managed Mobility Service

in support of:

X Federal Agency

Issued to:
all contractors under the Alliant
Government Wide Acquisition Contract

Issued by:
General Services Administration or Local Contracting Office
Address xxx

November 2013

Project Number XXXXXXX

NOTE: The section numbers in this Task Order (TO) correspond to the section numbers in the Alliant Contract. Section B of the contractor's Alliant Contract is applicable to this TO and is hereby incorporated by reference. (A draft modification for Section B was issued by GSA Alliant 9/11/13 and will need to be incorporated here.) In addition, the following applies:

SECTION B - SUPPLIES OR SERVICES AND PRICES/COSTS

B.1 GENERAL

The work shall be performed in accordance with all sections of this TO and the contractor's Basic Contract, under which the resulting TO will be placed.

B.5 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is ¾ % (i.e., (.0075)) of the total price/cost of contractor performance. Each TO issued under this contract shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award. The following access fee applies to TO issued under this contract.

GSA-Issued Task Orders:

Orders in excess of $13.3 million are capped at $100,000 per order year.

B.6 ORDER TYPES

The contractor shall perform the effort required by this TO on a Firm-Fixed-Price (FFP) basis

B.7 ORDER PRICING (ALL ORDER TYPES)

Long distance travel is defined as travel over 50 miles. Local travel will not be reimbursed.

The following abbreviations are used in this price schedule:

FFP	Firm-Fixed-Price
ODC	Other Direct Cost

[Note: Section B.7.1.1 offers three separate CLIN structures: Cloud, On-Prem, and Hybrid.]

B.7.1.1 CLINS:

[Use the following section if the requirement is for a Cloud delivery model]

MANDATORY CLOUD CLINs

CLIN	Description	QTY	Unit	**Total Firm Fixed Price**
0001	Implementation/Setup (Task 1)	X	Months	$_____
0002	Managed Mobility Service (Task 2,3)	12	Months	$_____

OPTIONAL CLOUD CLINs

CLIN	Description	QTY	Unit	**Total Firm Fixed Price**
0003	Additional Users (Task 1)	X	ea	$_____

[Use the following section if the requirement is for On-Premise delivery model]

ON-PREMISE CLINs:

MDM Software/Solution CLINs

CLIN	Description	QTY	Unit	**Total Annual Firm Fixed Price**
000X	MDM Perpetual License	##	ea	$_____
000X	MDM Monthly Subscription License	##	Per User/Month	$_____

MDM Professional Service CLINs

CLIN	Description	QTY	Unit	**Total Annual Firm Fixed Price**
000X	Set-up Fee	##	ea	$_____
	Installation	##	ea	$_____
	Training	##	ea	$_____
	Support and Maintenance	##	ea	$_____
	Service Desk Support	##	Per User/Month	$_____

Hardware CLINs

CLIN	Description	QTY	Unit	**Total Annual Firm Fixed Price**
000X	Hardware Appliance (Server)	XX	ea	$_____

ODC CLINs

CLIN	Description	QTY	Unit	**Not To Exceed**
000X	Travel is TBD at Task Order Level			$_____

[Use the following section if the requirement is for a Hybrid delivery model]

HYBRID CLINs:
MANDATORY CLINs

Hybrid - For the purposes of this request a Hybrid solution is a solution where the components are distributed across federal Government data centers and the respondent's cloud data center. It is anticipated that the respondent will provide all required hardware to the network edge of their cloud data center. The respondent would be responsible for all aspects of system and software performance for solution components within their cloud data center.

CLIN	Description	QTY	On-Prem	Cloud	Unit	**Total Firm Fixed Price**
000X	Implementation/Setup	X		X	Months	$_____
000X	Managed Mobility Service	12		X	Months	$_____

CLIN	Description	QTY	On-Prem	Cloud	Unit	**Total Firm Fixed Price**
000X	Additional Users	X		X	Each	$_____

CLIN	Description	QTY	On-Prem	Cloud	Unit	**Total Firm Fixed Price**
000X	MDM Perpetual License	##	X		Each	$_____
000X	MDM Monthly Subscription License	##	X		Per User /Month	$_____

CLIN	Description	QTY	On-Prem	Cloud	Unit	**Total Firm Fixed Price**
000X	Set-up Fee	##	X		Each	$_____
	Installation	##	X		Each	$_____
	Training	##	X		Each	$_____
	Support and Maintenance	##	X		Each	$_____
	Service Desk Support	##	X		Per User /Month	$_____

CLIN	Description	QTY	On-Prem	Cloud	Unit	**Total Firm Fixed Price**
000X	Hardware Appliance (Server)	XX	X		Each	$_____

CLIN	Description	QTY	On-Prem	Cloud	Unit	**Not To Exceed**
000X	Travel is TBD at Task Order Level					$_____

The respondent will clearly describe all HW/SW components in the table below that will be in the federal Government data center and those components within the respondent's cloud data center.

List the Hardware or Software, a brief description and where it will reside – Federal Government Data Center or the Cloud Data center. (Provide an attachment if required for additional information.)

Hardware / Software	Description	Fed. Govt. Data Center	Cloud Data Center

SECTION C - PERFORMANCE-BASED STATEMENT OF WORK

C.1 DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

<Agency-Specific background. Include not only MDM/MAM positioning but also Mobile strategy.>

C.1.1 PURPOSE

The government's mobility management challenge must address the customer agency's mission needs in a secure, cost-effective manner. This objective is driven by the Digital Government Strategy requirement 5.5, which seeks to "Set up a government-wide mobile device management platform" (http://www.whitehouse.gov/sites/default/files/omb/egov/digital-government/digital-government.html). Managed Mobility 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 themselves. The optimal balance between security, total costs and functionality will provide the most business value to the agencies.

C.1.2 AGENCY MISSION

<Agency-specific mission and how mobile supports that mission. Should include overall vision for how mobile will support agency mission>

C.1.3 BACKGROUND

C.1.4 CURRENT MOBILE ENVIRONMENT

Agency-specific description of current environment to include:

- Number and type of devices
- How devices are currently managed
- How email is currently accessed from devices
- Enterprise Applications and data currently accessed from devices
- Corporate owned/personally owned device information
- Locations from where devices typically operate (e.g. within government premise, via provisioned cellular service, via ad hoc WiFi hotspots)
- Penetration of agency owned vs. byod devices
- Other?

C.2 SCOPE

The scope of the TO includes …

C.3 OBJECTIVE

The objective of the TO is to provide:

C.4 TASKS

The contractor shall perform the following tasks under the TO.

Task 1 – Life Cycle Management

Task 2 – Provide High Level Architecture

Task 3 – Provide Mobile Device Management

Task 4 – Provide Mobile Application Management

C.4.1 TASK 1 – LIFE CYCLE MANAGEMENT

- Project Management
- Implementation
- Training
- Support

Mobility Life Cycle Management	All Required	Section	Use Case Reference
1. Project Management: Does the proposed solution clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements? (Y/N)	Required	C.4.1.1.1	
2. Professional Services: Does the respondent clearly describe how they provide initial deployment support services including installation, configuration, and the certification of initial solutions, as well as for additional professional services to support specific agency related integrations or customizations? (Y/N)	Required	C.4.1.1.2	
3. Enterprise System Integration: Does the respondent demonstrate experience in providing the steps necessary for deploying, integrating, and securing a mobility solution into an enterprise-wide environment? (Y/N)	Required	C.4.1.1.3	
4. Training: Does the respondent demonstrate how they can be responsible for developing and updating the MDM-MAS Training Material content, as well as providing prepackaged online training and associated materials described in the Training Plan? (Y/N)	Required	C.4.1.1.4	
5. Operations Support: Does the respondent/solution provide access to help desk support that meets the identified criteria? (Y/N) Does the respondent indicate the location of their help desk support? (Y/N)	Required	C.4.1.2	

Mobility Life Cycle Management	All Required	Section	Use Case Reference
6. Demonstration Platform: Does the proposed solution possess a fully functional and secure demonstration platform with associated mobile devices to educate potential customers on the use, benefits and technical specification of the solution, and will it provide access to the portal for the purpose of sampling and demonstrations that will be connected to the respondent's site through a federal website? (Y/N)	Required	C.4.1.1.5	
7. Past Performance: Has the respondent provided past performance with references that include solution installations that are similar to the solution being offered within this RFP/SOW? If other partner solutions are being used to fulfill the requirement identified in the RFP/SOW, has the respondent described how the solution has been tested and sold to other government agencies? (Y/N)	Required	C.4.1.3	
8. Enterprise Configuration: Does the respondent demonstrate the non-core integration services as indicated? (Y/N)	Optional	C.4.1.4.1	
9. Integration with Federal Strategic Sourcing Initiaitve (FSSI) Wireless Portal: Does the respondent demonstrate how to integrate their proposed solution with the FSSI Wireless portal to automatically retrieve asset and plan data, and return relevant data to the FSSI portal?	Optional	C.4.1.4.2	
10. Pilot: The proposed solution will be delivered within the pre-production pilot timelines and installation dates identified in this RFP and agreed to in the SOW.	Optional	C.4.1.4.3	

C.4.1.1 SUBTASK 1 IMPLEMENTATION / INSTALLATION

C.4.1.1.1 Project Management

The respondent must clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements.

C.4.1.1.2 Deployment / Migration / Transition

The respondent must clearly describe how they provide initial deployment support services. These services are expected for installing, configuring, and certifying the initial deployment of the MDM, MAM and/or Container solutions, as well as the ability to support specific agency related integrations or customizations. The respondent would assist the agency with achieving

accreditation and authorization (compliance) objectives by producing supporting documentation and/or modifications to the solution to reach compliance.

The respondent must submit a Transition Plan that details how devices previously supported by the respondent will transition from existing service in a quick, reliable, and accurate manner to the offered solution. Staffing requirements (contractor and government) for this Transition Plan must also be identified. The proposed solution will receive additional consideration if example transition plans from previous MDM deployments are supplied.

The respondent must provide an example of a previous successful on-boarding of 10,000 or more devices. The example must include a high-level timeline, staffing required, and a summary walk-through of the process (1 page maximum for summary walk-through).

The Contractor must also provide an example of an exit transition plan that describes how, in case termination for any reason, delivered data conforms to an industry standard format capable of being transported to other systems.

C.4.1.1.3 Enterprise Systems Integration

The respondent must show how they can be responsible for providing steps necessary for deploying, integrating, and securing their Mobility Solution into the enterprise-wide environment. This includes such systems as enterprise email, directories, trouble-ticketing, etc. The steps included are expected to vary dependent upon whether the solution is on-premise or a cloud solution.

C.4.1.1.4 Training

The Government requires that all users of the MDM-MAM system, which includes end users, administrators and developers, be trained to correctly utilize the system. The respondent must demonstrate how they can be responsible for developing and updating the MDM-MAM Training Material content (Enterprise, User, Administration levels), as well as providing prepackaged online training, training classes, and associated materials described in the Training Plan. The online training may be hosted by the government or the contractor, and the contractor must provide the required content.

C.4.1.1.5 Demonstration Platform

The respondent must possess a demonstration platform to educate potential customers on the use, benefits and technical specification of the solution. The demonstration platform must be fully functional and secure with associated mobile devices to educate potential customers on the use, benefits and technical specification of the solution. Respondents shall provide access to the portal for the purpose of sampling and demonstrations that will be connected to the respondent's site through a federal website.

C.4.1.2 SUBTASK 2 - OPERATIONS SUPPORT

C.4.1.2.1 Help Desk

The respondent must provide access to help desk support for their solutions. Please indicate the location of the operational help desk. They must satisfy the following criteria:

1. End User Help Desk support must be 24/7 including holidays.
2. Administrative / Management Help Desk must be available 8am-5pm in both EST and PST.
3. Help Desks must utilize a trouble-ticketing system where each request has a unique identifier for tracking purposes.
4. Help Desk interaction must support online requests / resolution, supported with email.
5. Telephone (voice) Help Desk support must be available, but can be limited to business hours.
6. (Optional) The MDM should support Help Desk remote access to the device for troubleshooting purposes.

[NOTE: need to add level 2 and level 3 support requirements]

C.4.1.3 SUBTASK 3 – PAST PERFORMANCE

Past Performance: When providing past performance, the references provided should include solution installations that are similar to the solution being offered within this RFP/SOW.

If other partner solutions are being used to fulfill the requirement identified in the RFP/SOW, describe how the solution has been tested and sold to other government agencies. Also explain if the solution working at full capacity today.

C.4.1.4 SUBTASK 4 – OPTIONAL ITEMS

C.4.1.4.1 (Optional) Enterprise Configuration

This addresses non-core integration, such as Solution connectivity with non-required components (e.g. custom portal, Telecommunications Expense Management System (TEMS) provider system, etc.). Agencies have applications that may be need to be accessed on mobile devices, but that require configuration services to enable. The respondent should describe the services they offer of this type. Each configuration service offered must be accompanied by a successful example from industry or government.

C.4.1.4.2 (Optional) Integration with FSSI Wireless Portal

The FSSI Wireless Business Portal Interface is a secure standard for agencies to interface with cellular carriers to place orders, manage plan/device inventory, and other carrier provided information. The BPI is not a GUI but merely a secure standard for exchanging data between the customer agency and the carrier. Respondents should indicate their experience and platform's ability with exchanging information with third party providers for the purpose of providing complementary services such as device ordering, logistics, configuration, replacement/refresh, disposal, and disposition reporting

C.4.1.4.3 Pilot (Optional)

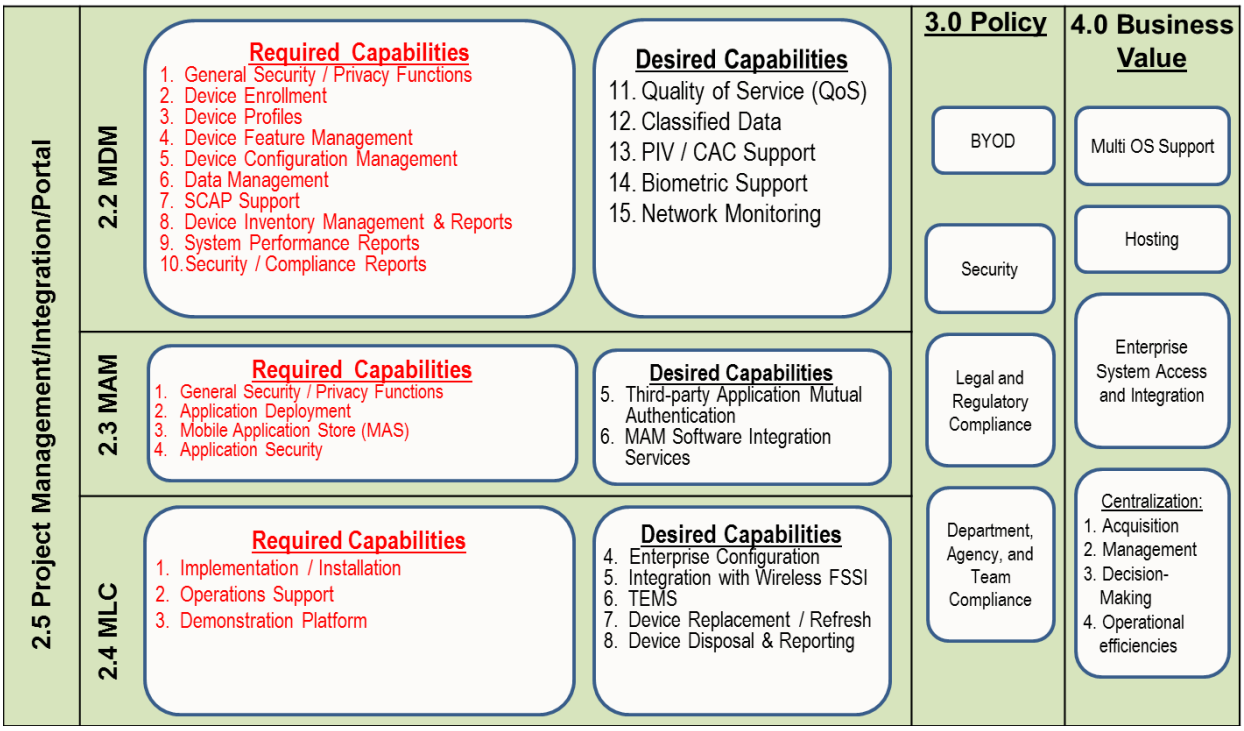
[Agency to add pilot requirements if applicable]

The proposed solution will be delivered within the pre-production pilot timelines and installation dates identified in this RFP and agreed to in the SOW.

C.4.2 TASK 2 – PROVIDE HIGH LEVEL ARCHITECTURE

Managed Mobility is a service portfolio of mobile device management, mobile application management, and mobility lifecycle services. These are shown below and further discussed in the following subsections. Sections in red font are required capabilities, features or attributes. These requirements will be impacted in the future by the release of the Mobile Security Requirements in the Digital Government Strategy 9.1 guidance.

Managed Mobility Framework



General Managed Mobility Requirements & Past Experience (Common for All Respondents)

These characteristics represent core capabilities that must be present in order to provide Managed Mobility services to Federal Customers based on the common requirements developed by the inter-agency working group. All questions in this section require a Yes answer in order for the assessment to proceed further. Respondents should answer the questions, affirming their capability to meet the requirements, and provide a short description of how they have done so.

High Level Architecture Requirements & Respondent Capabilities/Experience	Required or Optional	Section	Use Case Reference
1. Scope/Scale: Is the respondent's solution scalable from an initial requirement of X users to the maximum requirement of Y users? (Y/N)	Required	C.4.2.1	6

High Level Architecture Requirements & Respondent Capabilities/Experience	Required or Optional	Section	Use Case Reference
2. Multi-Tenancy: Does the proposed solution support the Department's / Agency's ("tenants") hierarchical organizational structure within the solution, and support multiple configurations for each of the MDM requirements? (Y/N)	Required	C.4.2.2	
3. Solution Security: Does the proposed solution describe how they meet the 14 identified general controls/capabilities of solution security? (Y/N)	Required	C.4.2.3	
4. FISMA: Does the respondent provide evidence that the proposed solution is capable of being certified at the FISMA moderate impact level? (Y/N)	Required	C.4.2.3.2	
5. FIPS Requirements: Does the respondent provide evidence that their solution uses FIPS 140 certified cryptographic modules and continued validation? (Y/N)	Required	C.4.2.3.3	
6. Containerization: If applicable, does the respondent describe how the proposed solution meets FIPS 140-2, controlled wipe capabilities, and platform-by-platform container protection as it related to BYOD scenarios? (Y/N)	Required	C.4.2.3.4	2,3
7. IPv6 Support: Does the respondent provide evidence of either IPv6 compliance or intention to comply? (Y/N)	Required	C.4.2.3.5	
8. User Authentication: For cloud-based systems, does the respondent provide evidence of being capable of meeting authentication standards related to the portal and device, as well as 2 multifactor authentication methods? (Y/N)	Required	C.4.2.3.6	2,3,10
9. User Compliance: Does the proposed solution demonstrate the 4 items related to user compliance enablement? (Y/N)	Required	C.4.2.3.7	1,2,4,5,6,7
10. Alerting: Does the proposed solution demonstrate the 8 alert capabilities required to notify agency operations staff about devices under their management? (Y/N)	Required	C.4.2.3.8	2,6
11. Security Reporting Capabilities: Does the proposed solution demonstrate the 8 reporting capabilities, as well as the stated support functions applicable to Audit Reports? (Y/N)	Required	C.4.2.4	3,5,6,8

High Level Architecture Requirements & Respondent Capabilities/Experience	Required or Optional	Section	Use Case Reference
12. Privacy: Does the proposed solution disclose privacy-impacting features that cannot be disabled? (Y/N)	Required	C.4.2.5	3
13. Service Delivery Model: Is the proposed solution delivered and (optionally) hosted by the provider as a full solution including all hardware, software, hosting, and installation services, using one or more of the following hosting models: (on premise, Cloud, Hybrid)? (Y/N)	Required	C.4.2.5.1	

C.4.2.1 SCOPE / SCALE

[This SOW is for procurement of enterprise class MDM/MAM solution scalable to 10000 devices and higher. Use the following language to specify your agency requirements.The agency should fill in the revise wording to incorporate min users and growth rquirements tailored to the agency]

The initial requirement is for the platform to support X users. The solution shall allow growth to Y users. The solution shall allow flexibility to increase the number of users in any incremental amount up to the maximum number of Y users.

C.4.2.2 MULTI-TENANCY

The proposed solution must be able to support the Department's / Agency's ("tenants") hierarchical organizational structure to apply hierarchical policy requirements within the solution, and support multiple configurations for each of the MDM requirements below. For example, each tenant may have different help desk contact information, policies, and organizational groupings and hierarchy.

C.4.2.3 SOLUTION SECURITY

Data at rest encryption, data in transit encryption (VPN), and secure applications are included in the short-term requirements for this MDM-MAM solution. These capabilities may be accomplished by separate products which are then integrated into the complete MDM-MAM solution.

C.4.2.3.1 General Security Controls

The respondent must describe how the solution meets the following general controls / capabilities.

1. Ability to enroll an authorized device and user before applying any policy (null policy)

2. Ability to create Whitelist / Blacklist for device enrollment to include OS versions and device models
3. Allow enrollment of untrusted devices and anonymous / unknown users outside the enterprise into controlled access and network isolation zones as individuals or groups under the MDM
4. Ability to use an existing user attribute repository for enrollment to the new MDM system
5. MDM has native ability with active (device scanning) and passive (on-access scanning) tools to detect, report, and alert on a compromised device (e.g.: jail broken / rooted device, malware) and take policy action based upon compliance rules
6. Ability to lock the device or to erase (wipe) ONLY the managed data on a device under the following conditions:
    - Blacklisted operating system or version (policy)
    - Exceeding a set number of failed access attempts to the device or MDM application (policy)
    - Exceeding defined interval for MDM synchronization/policy updates (policy)
    - Detection of OS jailbreaking or application tampering (policy)
    - Any other stipulated policy violation requiring stated outcome
    - Remote instruction from MDM (manual)
7. Password policy enforcement in support of HSPD-12/SP 800-53/SP 800-63 requirements in support of section C.4.2.3.6 User Authentication:
    - Minimum complexity (length, composition, common words, etc.)
    - Password lifetime limit
    - Password re-use limits
    - Password inactivity timeout (grace period) for device and MDM app
    - Report password failures beyond policy threshold to MDM
    - Maximum password attempts before lock or wipe
8. Ability to mask passwords when they appear in the Management GUI except for those administrators authorized based on RBAC authorizations.
9. Ability to determine which administrative user made a configuration change in the MDM administrative environment as well as record the change made.
10. Ability to determine which device user made a configuration change in the MDM console (self-service logging) as well as record the change made.
11. Installation and configuration (update, revocation checking, revocation) of individual and group soft and hardware-based authentication certificates for the mobile device for the following purposes:
    - Email (S/MIME) signing and encryption
    - WiFi Configuration
    - VPN Configuration
12. Ability to send/receive (Encrypt and Sign, decrypt and verify) messages that use FIPS 140 certified PKI or S/MIME encryption, where email functionality is delivered by the solution
13. Ability to restrict downloading attachments, copying of data to/from removable media, or otherwise create separate spaces or virtual containers for separating agency data and applications from personal data

14. (Optional) Ability to view the current GPS location of a device or logical grouping of devices on a map

C.4.2.3.2 FISMA or FedRAMP Requirements

The MDM solution must be certifiable at a FISMA Moderate Impact level (FIPS 199 Moderate or DoD 8500.2 MAC II) or higher. The response may include proof of certification, accreditation, or Authorization to Operate (ATO) in a federal environment, or a plan and timeline for achieving certification and/or Authority-To-Operate (ATO).

[NOTE: insert FedRAMP requirements language]

C.4.2.3.3 FIPS Requirements

The solution must protect control and management data in transit between the MDM and the device using FIPS 140 certified cryptographic modules.

The respondent must submit with their response proof of the solution's FIPS 140-2 certification for cryptographic modules. All encrypted communications must use a cryptographic module certified in accordance with a NIST Certified Cryptographic Module Validation Program under FIPS 140-2, level 1, certification. The respondent must provide evidence of the solution's NIST Certified Cryptographic Module Validation Program compliance, or that cryptographic operations in the solution rely on FIPS certified modules in the environment or operating system.

C.4.2.3.4 Containerization

If the proposed solution uses containers, respondents must describe how the container meets the following requirements:

1. FIPS 140-2 encryption of data at rest
2. Remote and local (action-triggered) secure erasure of container data without impact the rest of the device
3. Protection of container from other applications; because of varying platform capabilities, this must be described on a platform-by-platform basis

Some solutions address data control through the use of containers on the mobile device that serve to separate enterprise and personal data, and protect data from access by uncontrolled applications. This is particularly helpful for Bring Your Own Device (BYOD) scenarios, where the enterprise intends to limit interaction between agency and personal data. This approach is also used to protect data at rest if the underlying platform does not encrypt all data on the device.

C.4.2.3.5 IPv6 Support

IPv6 compliance is a goal for this request. On-premise portions of the MDM solution must support IPv6 for network communications. Controls on network communications at the device

must apply to both IPv4 and IPv6 communications, including VPNs, logging/auditing and network black/white-listing. The respondent must provide a description of the IP based components of their solution and the status (compliant or non-compliant) of the proposed solution. If the proposed solution is not compliant at time of response submission, the respondent shall provide a Program of Actions/Milestones (PoAM) signed by company official an estimated timeline to achieve IPv6 compliance.

C.4.2.3.6 User Authentication

The proposed solution for the device must support PIN or password authentication for the managed applications. Policy should also be able to enforce a device PIN as provided in Task 2, Section C.4.2.3.1-7 Password Policy Enforcement..

The respondent must include a web management portal as part of their proposed solution, and the web management portal must be capable of PIV / CAC for primary authentication as indicated in HSPD-12 standards and guidance. Password fallback for specific accounts may be configurable; however they must employ a second factor (token, SMS, voice response, etc.) to authenticate.

Respondents shall state how their proposed solution is capable of offering or supporting multi-factor authentication. Multifactor authentication involves authentication with any two of the following three authentication types:

- Shared Secret – Something the user knows, like a PIN or password
- Token – something a user possesses such as a cryptographic key such as an RSA token (soft or hard), a challenge / response token, a PIV or CAC, NFC RFID, or a key generator device like UbiKey
- Biometric – a sufficiently unique physical characteristic of the user, such as a fingerprint, iris or facial image

C.4.2.3.7 User Compliance

The respondent must demonstrate the following capabilities. The proposed solutions are required to enable the:

1. Ability to set up compliance rules to include custom compliance rules for profiles, devices, groups, and whitelist/blacklist
2. Ability to activate / deactivate a compliance rule
3. Ability to specify user and group rules for application compliance, such as required or prohibited applications on a device.
4. Ability to provide enterprise level compliance reports, including lost/wiped/inactive devices, the number of devices total, the number of devices active, how much data is sent/received by devices, connection type
5. Support hierarchical policy enforcement as stipulated in section C.4.2.2: Multi-tenancy

C.4.2.3.8 Alerting

The following alert capabilities are required to notify agency operations staff via console display as well as appropriately via email and/or text message about devices under their management. The solution must demonstrate the following capabilities:

1. Ability to set up custom alerts to users and management based upon various parameters
2. Ability to send custom alerts to one or more user roles including administrators
3. Ability to specify a creation policy for custom alerts to include having various alert severity levels
4. Ability to have automated alerts for security issues such as compromised devices
5. Ability to create alerts based upon device status such as battery low, device roaming, equipment down (not responding), device inactive, etc.
6. Ability to view alerts pending acknowledgement
7. Ability to acknowledge alerts and track acknowledgement
8. Ability to search and run reports on alerts

C.4.2.4 REPORTING

The solution must demonstrate the following capabilities:

1. Ability to run reports by device, profile, provision details, or compliance status
2. Ability to subscribe to a Report (automatic generation and delivery on a schedule)
3. Ability to schedule a Report (Monthly, weekly, daily, etc.)
4. Ability to print a Report using a printer
5. Ability to print a Report to a file
6. Ability to report on devices that haven't communicated with the MDM in a period of time
7. Ability to report all policy compliance status details of devices under MDM management
8. Ability to view reports in HTML5 dashboards from tablets or mobile devices.

The solution must be able produce the following types of reports:

C.4.2.4.1 Audit reports

Audit reports provide data necessary to monitor, reconcile, and audit system processing and reconciliation activities. Audit reports will be run as needed, exportable and will support the following filters:

1. Administrator activity (admin actions performed, time stamps, etc.)
2. User access times and enrollments
3. Participating Agencies (number of devices by Agency and across all Agencies)
4. Devices (number of devices, type, OS version, etc.)

5. Console logins and functions (connections to the management console, actions performed, etc.)
6. Policy changes and versions (policy revision control and historical changes)

C.4.2.5 PRIVACY

[The agency should define the PII requirements applicable to the agency from the guidance in this section]

The proposed solution must not display advertisements to end users of the Information System as part of its business model (i.e. not an advertising-based model).

The proposed solution must safeguard any Personally Identifiable Information (PII), including directory data stored in the information system in accordance with NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)" and in accordance with M-06-16: Protection of Sensitive Agency Information http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-16.pdf and M-07-16: Safeguarding Against and Responding to the Breach of Personally Identifiable Information http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf. An Ordering Activity will determine what data elements constitute PII according to OMB Policy, NIST Guidance and Ordering Activity policy. An Ordering Activity may request that PII be kept within U.S. Data Centers.

The solution provider must disclose privacy-impacting features that cannot be disabled.

C.4.2.5.1 Service Delivery Model

The MDM Solution must be delivered by the Contractor as a full solution including all hardware, software, hosting, and installation services, using one a [Select one on premise, Cloud, Hybrid] model as follows::

[The agency should decide which delivery model they want before issuing the RFP. Choose one of the follosing paragraphs and delete the other two]

1. Cloud Based - For the purposes of this request a Cloud Only solution is a solution that has all HW/SW components of the solution will running in the a non-government hosted cloud data center. The respondent must show how they provide all required hardware to the network edge of their cloud data center. The respondent is responsible for all aspects of system and software performance for solution components within their cloud data center.
2. On Premise - For the purposes of this request an On-Premise solution is a solution that has all HW/SW components running completely within federal Government controlled data centers and network. After installation, the Federal Government will be responsible for operating the infrastructure and devices, application store and container management.

3. Hybrid - For the purposes of this request a Hybrid solution is a solution where the components are distributed across federal Government data centers and the respondent's cloud data center. It is anticipated that the respondent will provide all required hardware to the network edge of their cloud data center. The respondent will clearly describe all HW/SW components that will be within federal Government data center and those components within the respondent's cloud data center. The respondent would be responsible for all aspects of system and software performance for solution components within their cloud data center.

The Help Desks should be operationally located within the Continental United States (CONUS).

C.4.3 TASK 3 – PROVIDE MOBILE DEVICE MANAGEMENT (MDM)

MDM is a widely used term describing 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. Products that support MDM are evolving rapidly at this time.

MDM Requirements & Respondent Capabilities/Experience	Required or Optional	Section	Use Case Reference
1. General MDM Capabilities: Does the proposed solution address/describe how their solution meets all 10 of the mandatory general MDM requirements? (Y/N)	Required	C.4.3.1	
2. Device Enrollment: Does the proposed solution demonstrate the 19 capabilities identified regarding the ability to add a device to an MDM management domain? (Y/N)	Required	C.4.3.2	1,2,3
3. Device Profiles: Does the provider support the 21 items related to the creation of per-user and per-group device profiles? (Y/N)	Required	C.4.3.3	1,2
4. Device Feature Management: Does the proposed solution demonstrate the 7 required features and capabilities identified regarding device feature management? (Y/N)	Required	C.4.3.4	
5. Data Management: Does the proposed solution demonstrate the ability to read, write transmit and receive data on mobile devices as well as with backend systems/repositories to include meet FIPS 140 requirements? (Y/N)	Required	C.4.3.5	

MDM Requirements & Respondent Capabilities/Experience	Required or Optional	Section	Use Case Reference
6. Data Collection: Does the proposed solution demonstrate the ability to collect and report on the 6 data points identified? (Y/N)	Required	C.4.3.5.1	
7. Continuity of Operations and Disaster Recovery: Does the proposed solution describe how it performs Continuity of Operations (COOP) and Disaster Recovery (DR)? (Y/N)	Required	C.4.3.5.2	
8. File Management: File Management: Does the proposed solution demonstrate that the solution is able to hold a set of COTS and/or enterprise applications with respective data/files in a FIPS 140 secured space (e.g. whole device encryption, container or VDI) solution? Does the proposed solution also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and hosted file servers based on application and security requirements? (Y/N)	Required	C.4.3.5.3	
9. Personal Information Management: Does the proposed solution demonstrate the solution's ability to provide/enable a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection? (Y/N)	Required	C.4.3.5.4	
10. Security Content Automation Protocol (SCAP) Support: Does the proposed solution demonstrate the ability to support server-side components, including asset management, configuration management, patch management and remediation capabilities? (Y/N)	Required	C.4.3.6	
11. Device Inventory Management: Does the proposed solution demonstrate the ability to include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information? Does it record, track and manage the 16 pieces of information identified in inventory management? (Y/N)	Required	C.4.3.7	1,2,3,6,7,8

MDM Requirements & Respondent Capabilities/Experience	Required or Optional	Section	Use Case Reference
12. Device Inventory Reports: Does the proposed solution demonstrate the ability use the identified filters to run or export device inventory reports associated with the device, OS, and applications? (Y/N)	Required	C.4.3.8	6
13. System Performance Reports: Does the proposed solution demonstrate the ability to run system performance reports using the identified filters? (Y/N)	Required	C.4.3.9	
14. MDM Security/Compliance Reports: Does the proposed solution demonstrate the ability to run MDM security/compliance reports using the identified filters? (Y/N)	Required	C.4.3.10	6
15. Classified Data: Does the respondent describe the ability of the proposed solution to access classified data up to the SECRET level via a mobile device? (Y/N)	Optional	C.4.3.11	
16. PIV/CAC Support: Does the respondent adequately describe how the proposed solution is capable of supporting the use of PIV/CAC cards to support digital signatures, encryption, or access to enterprise resources? (Y/N)	Optional	C.4.3.12	10
17. Biometric Support: Does the respondent demonstrate the ability for the proposed solution to offer biometric support such as fingerprint or face recognition? (Y/N)	Optional	C.4.3.13	
18. Network Monitoring: Does the respondent demonstrate the basic diagnostic functions related to monitoring device network quality and performance?	Optional	C.4.3.14	

C.4.3.1 MDM GENERAL REQUIREMENTS

The respondent is asked to describe how the proposed solution meets the following general requirements:

1. Ability to enforce enterprise rules while allowing Agency/Bureau/sub-bureau/etc. enrollment, reporting, management, and compliance activities
2. Ability to take the following action upon a group of devices from a search: Reassign to Group (any type of logical grouping). User or device groupings are an example.

3. Ability to assign Profile to one or many Groups (any type of logical grouping). User or device groupings are an example.
4. Ability to view required applications from the Mobile Application Store (MAS)
5. Ability to view and run reports on user and device information for all Smartphones
6. Ability to run reports by groups of users to include location
7. Ability for the solution to support a Software Development Kit (SDK) or Application Programming Interface (API) Framework to integrate with existing or future Enterprise Applications
8. Ability for the MDM solution to be able to be monitored from industry standard tools (e.g. HP OpenView, SCOM, etc.)
9. Ability for the MDM solution to integrate certificates from the solution's internal PKI system to mobile devices as well as third party public PKI providers such as VeriSign. PKI shall support HSPD-12 and associated NIST standards.
10. Ability for the MDM to perform its functions from within a secure VPN(FIPS 140) used to transport all enterprise data (i.e.: no MDM control data transported unencrypted across the open internet).

C.4.3.2 DEVICE ENROLLMENT

Enrollment adds a device to the MDM management domain. The respondent must demonstrate that the proposed solution meets the following required capabilities:

1. Ability to set a Target Platform (Apple, Android, etc.) for profile provisioning
2. Ability for Target Device Model to be used for profile provisioning
3. Ability to specify minimum OS version for profile provisioning
4. Ability for Target Device Ownership (GFE, Personal etc.) to be used for profile provisioning
5. Ability to edit any field for a "live" or "active" profile
6. Ability for a user with appropriate authorization to self-enroll an agency or BYOD device
7. Ability to centrally manage multiple devices for a single user (user device view)
8. Ability to have different policies or grouping for multiple devices under one user (i.e.: tablet policy, phone policy)
9. Ability to apply multiple policies to devices simultaneously (user is member of group policy X, with device policy Y) – when multiple controls conflict, the most restrictive control takes precedence
10. Ability to use external directory service repository for enrollment
11. Ability for system to require users have read policy and signed agreement for enrollment
12. Ability to set support email and phone information for registration messages
13. Ability to set a URL to redirect user to upon successful enrollment
14. Ability to edit an enrollment activation notification message to the user (email and/or SMS)
15. Ability to set a default Device Ownership type upon enrollment for different groups
16. Ability to use internal user list for enrollment for different groups

17. Ability to set support email and phone information for registration messages for different groups
18. Ability to edit an enrollment activation notification message to the user or group of users (email and/or SMS)
19. Ability to send a user or group an activation enrollment message (email or SMS)
20. Ability to support over-the-air provisioning and hierarchies

C.4.3.3 DEVICE PROFILES

The solution must support the creation of per-user and per-group device profiles. Features and capabilities to be controlled appear in the next section.

The solution must demonstrate the following profile capabilities:

1. Ability to create a profile template
2. Ability to copy profiles
3. Ability to edit a "live" or "active" profile
4. Ability to set Profile Removal Permission (who can remove a profile from a device or user)
5. Ability to set Profile Start Date (when the profile starts applying to associated devices)
6. Ability to set Profile End Date (when the profile stops applying to associated devices)
7. Ability for an edited profile to automatically update devices that currently have the profile
8. Ability to push a profile to any individual device
9. Ability to automatically remove profiles from devices whose state changes from qualifying to not qualifying. This may happen as a result of changing a profile to be more exclusive.
10. Ability to support multiple profiles being applied to a single device (most restrictive rules apply)
11. Ability to delete a profile from the MDM system
12. Ability to set a description for a profile
13. Ability to manage the following via a profile:
    a) Allow installing applications
    b) Control use of camera or other sensors and recording devices
    c) Control use of installed applications, including default applications
14. Allow multiple Wi-Fi configurations for multiple profile's
15. Ability to manage device Wi-Fi settings via a policy via a MDM policy
16. For a profile: Control Wi-Fi Security Type: None, WEP, WPA/WPA2, Enterprise (any)
17. For a profile: Ability to support multiple VPN configurations for a profile.
18. For a profile: Support VPN Connection (or Policy) Type: IPSec (Cisco), Juniper SSL, FS SSL, and Custom SSL, etc.
19. For a profile: Ability to support a VPN connection Proxy for a VPN configuration
20. Ability to support multiple email/calendar/contact configurations per profile
21. Allow multiple Web Clip / Web Shortcut configurations per profile

22. Ability to support hierarchies

C.4.3.4 DEVICE FEATURE MANAGEMENT

The solution must be able to control the following features / capabilities at a minimum:

1. Multi-OS Support – Manage multiple operating system devices such as RIM's BlackBerry, Apple's iOS, Google's Android, Microsoft's Windows Phone, etc.
2. Device passcode enforcement (complexity, length, presence) in compliance with Section C.4.2.3.1-7 Password Management.
3. Installation of applications (See Mobile Application Management (MAM))
4. Camera (enable / disable)
5. Control all radios / communications:
   - Wi-Fi (enable / disable)
   - Bluetooth (enable / disable)
   - Near Field Communication (NFC) (enable / disable)
6. Ability to enable or disable specific hardware component and uses: Enable blue tooth headphone, disable Bluetooth keyboard
7. GPS (enable / disable)
8. Store enterprise data to removable media (disable)
9. (Optional) Roaming (enable / disable)
10. (Optional) – Microphone (enable / disable)
11. (Optional) – Geofencing for device features; enable or disable features based on device location
12. (Optional) - Geomasking - Geomasking for applications; enable or disable location data based upon policy and state

C.4.3.5 DATA MANAGEMENT

Data Management is the ability to read, write, transmit and receive data on mobile devices as well as with backend systems/repositories to include FIPS 140 requirements.

C.4.3.5.1 Data Collection

The solution must be able to collect and report on the following data:

1. Roaming status
2. Last policy update time
3. Last synchronization time
4. Jailbreak / root status
5. Available program memory
6. Available storage memory

C.4.3.5.2 Continuity of Operations and Disaster Recovery

The solution must describe how the solution performs Continuity of Operations (COOP) and Disaster Recovery (DR).

C.4.3.5.3 File Management

The Government seeks solutions that have the capability to secure data, files, and applications (for example pdf files or word docs) on a mobile device. Devices may be Government Furnished (GFE) or BYOD. The respondent must demonstrate that the solution is able to hold a set of COTS and/or enterprise applications with respective data/files in a FIPS 140 secured space (e.g. whole device encryption, container or VDI) solution, whether that is within a secured container or secured within the device OS. The respondent must also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and file servers based on application and security requirements.

C.4.3.5.4 Personal Information Management

The respondent must demonstrate the solution's ability to support a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities. To ensure that the information is available to other mobile and desktop devices the user may have, as well as for business continuity, backup/restore, and e-discovery purposes, solution providers must be able integrate functionality with a variety of Email, Calendaring and Contact applications, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection. The respondent should also demonstrate the solution's PIM capability to support multiple types of Federal Enterprise Email Systems from different vendors. Please identify which on-premise and cloud-based mail systems are supported, such as Microsoft Exchange, Lotus Notes, Gmail, MS 360, Lotus Domino, MS Exchange or Zimbra.

C.4.3.6 SECURITY CONTENT AUTOMATION PROTOCOL (SCAP) SUPPORT

SCAP provides the ability to automate security checks and configuration. Respondents must describe the SCAP support for the server-side components in your solution, including asset management, configuration management, patch management and remediation capabilities.

The request is only considering server SCAP support at this time. SCAP for devices is not currently a requirement.

C.4.3.7 DEVICE INVENTORY MANAGEMENT

The solution must include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information. At a minimum the solution should be able to record, track and manage the following information:

1. Device Manufacturer/Model
2. Government Furnished (GFE) or personal (BYOD) device
3. Carrier
4. Wireless Number
5. MAC Addresses
6. International Mobile Equipment Identity (IMEI)
7. SIM module data
8. Storage capacity
9. OS and Version
10. Device up time
11. Encryption Capability
12. User Name
13. Email
14. Phone number
15. Agency information
16. Supervisor contact information

Please identify which of the above elements can be automatically populated with the MDM solution.

The solution must also have the ability to extend or expand the schema.

C.4.3.8 DEVICE INVENTORY REPORTS

The solution must demonstrate the capability to run inventory reports. Device Inventory reports includes all data associated with the device, OS and applications. Device reports will be run and/or exported as needed, and will support the following filters:

1. Device Models
2. Operation System and build level
3. Last Access times (access time not compliance check)
4. Application inventory
5. Last Compliance Check
6. Device Compliance (ability to report on rooted/jailbroken devices, policy, etc.)
7. Carrier
8. Network Card IDs (MAC address)
9. Agency Assignment
10. BYOD or GFE (personal device or government furnished)
11. Security Policy Assignment (policy currently applied to device)

C.4.3.9 SYSTEM PERFORMANCE REPORTS

The solution must demonstrate the capability to run system performance reports. System performance reports include key performance data to provide insight into the usage of the devices, reliability of the solution, and performance of devices. System performance reports will be run as needed and will support the following filters:

1. Concurrent Connections
2. Peak Time Usage
3. Total active user and device counts
4. Bandwidth utilization trends
5. End-to-End testing results
6. Authentication processing times
7. Email/Calendar/Contact sync durations
8. Connection failure rate to/from device for the MDM system

C.4.3.10 MDM SECURITY / COMPLIANCE REPORTS

The solution must demonstrate the capability to run security/compliance reports. Security reports include all data relevant to the monitoring and support of the system's vulnerabilities and defenses, including attempts at fraud. Security status reports will be run as needed and will support the following data:

1. Non-compliant devices
2. Device wipe actions
3. Passcode reset actions
4. User/Devices with failed authentication
5. Aggregate data on failed authentications
6. Devices with blacklisted applications
7. Jailbroken devices
8. Device anti-virus versions
9. Mobile Management Agent

C.4.3.11 (OPTIONAL) CLASSIFIED DATA

Some Managed Mobility users may require the ability to access classified data up to the SECRET level via mobile devices. If your solution supports these capabilities, please describe how this is accomplished and indicate the specific impact to pricing for this solution, inclusive of exact dollar amounts.

C.4.3.12 (OPTIONAL) PIV / CAC SUPPORT

Respondents may optionally offer solutions that support the use of PIV/CAC cards or PIV-derived credentials per associated NIST standards to support digital signatures, encryption, or access to enterprise resources.

C.4.3.13 (OPTIONAL) BIOMETRIC SUPPORT

Agencies with strong authentication requirements may need biometric support per associated NIST standards such as fingerprint or face recognition with their mobile devices. The ability for the MDM to manage this capability may be combined with PIV / CAC support.

C.4.3.14 (OPTIONAL) NETWORK MONITORING

Network Monitoring is the monitoring of the mobile device network quality and performance (e.g., the number and location of dropped calls by enterprise devices).

The solution may include a device application that performs basic diagnostics, such as:

1. Verify network connection and performance
2. Test authentication settings
3. Verify certificates
4. Verify DNS functionality
5. Verify connection to services (mail, MDM, etc.)

C.4.4 TASK 4 – PROVIDE MOBILE APPLICATION MANAGEMENT (MAM)

MAM Requirements & Respondent Capabilities/Experience	All Required	Section	Use Case Reference
1. Application Deployment: Does the proposed solution demonstrate the ability to support the 5 controls and capabilities identified for application deployment? (Y/N)	Required	C.4.4.1	1,2,4,6,7
2. Mobile Application Store: Does the proposed solution include a Mobile Application Store that allows users to select private enterprise applications for installation on managed devices, integrated into the Managed Mobility MDM portal, which allows application provisioning by group policy and mandatory application deployment? (Y/N)	Required	C.4.4.2	2
3. Mutual Authentication: Does the proposed solution demonstrate the ability for applications to mutually authenticate to ensure the communications channel is not intercepted? (Y/N)	Required	C.4.4.3.1	
4. Application Installation Control: Does the proposed solution demonstrate the solution's process to support relevant authorizations and approvals (including change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance, including the ability to monitor application usage? (Y/N)	Required	C.4.4.3.2	1.2.6,7

MAM Requirements & Respondent Capabilities/Experience	All Required	Section	Use Case Reference
5. Blacklisting/Whitelisting: Does the proposed solution demonstrate the capability, managed through user and group policies, to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting)? (Y/N)	Required	C.4.4.3.3	2,5
6. Application Environment Requirements: Does the proposed solution demonstrate the capability to detect and enforce device environment conditions such as those listed? (Y/N)	Required	C.4.4.3.4	2
7. Application Signing: Does the proposed solution support requiring digital signatures for application installation? (Y/N)	Optional	C.4.4.3.5	
8. Third-Party Application mutual Authentication: Does the proposed solution offer the ability to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc…? (Y/N)	Optional	C.4.4.4	

C.4.4.1 APPLICATION DEPLOYMENT

The solution must support the following controls and capabilities for application deployment:

1. Commercial Application Store (iOS App Store, Google Play, etc.) (enable / disable)
2. Reporting of installed applications
3. Blocking application purchase
4. Application whitelisting / blacklisting
5. Staged/controlled application deployment (limit deployment by policy, group, location, etc. to facilitate gradual deployment of new or updated applications)
6. Must authenticate the user accessing the MAS either directly using User Authentication per section C.4.2.3.6, or via MDM utilizing approved PKI alternative authentication methodologies such as Kerberos Constrained Delegation if MAS is not integrated into MDM.

C.4.4.2 MOBILE APPLICATION STORE (MAS)

The solution must include a Mobile Application Store to allow users to select private enterprise applications for installation on managed devices. This capability must be integrated into the Managed Mobility MDM portal, and allow application provisioning by group policy, and mandatory application deployment.

The MAS should support the following capabilities:

1. Ability to add an application from a Commercial Application Store to the MAS
2. Ability to add an enterprise application to the MAS via a web GUI
3. Ability to add additional metadata to and report on metadata on any application added to the MAS (etc. name, description, version, OS, keywords, etc.)
4. Ability to specify the effective date for an internal application
5. Ability to specify the expiration date for an internal application
6. Ability to specify the minimum operating system and model for an internal application
7. Ability to download internal and public applications from MAS
8. Ability to categorize, group or tag applications (e.g., business applications, scientific applications, etc.)

C.4.4.3 APPLICATION SECURITY

C.4.4.3.1 Mutual Authentication

MDM applications on the device and services must mutually authenticate to ensure the communications channel is not intercepted. The mutual authentication should be certificate-based, with installation-specific certificates deployed to the server during deployment and to the device during provisioning.

C.4.4.3.2 Application Installation Control

The respondent must demonstrate the solution's process to support relevant authorizations and approvals (include change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance. This includes the ability to monitor application usage.

C.4.4.3.3 Blacklisting / Whitelisting

The solution must provide the capability to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting). This capability should be managed through user and group policies.

C.4.4.3.4 Application Environment Requirements

The solution must be able to detect and enforce device environment conditions or enact required policy enforcement rules if device environment conditions cannot be enforced. Examples include:

1. Minimum or specific operating system versions
2. Required presence or absence of other applications
3. Absence of privilege escalation ("rooting" or "jailbreaking")

C.4.4.3.5 Application Signing

The solution should support requiring digital signatures for application installation, from both commercial and private application stores and direct application push / deployment. It is permissible to meet this requirement through OS capabilities.

C.4.4.4 (OPTIONAL) THIRD-PARTY APPLICATION MUTUAL AUTHENTICATION

The MDM solution may offer the ability provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc.

SECTION D - PACKAGING AND MARKING

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section D of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

D.1 PRESERVATION, PACKAGING, PACKING, AND MARKING

The contractor shall deliver all electronic versions by email and CD-ROM as well as placing in the designated repository. Identified below are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market:

- Text - Microsoft Word
- Spreadsheets - Microsoft Excel
- Briefings - Microsoft PowerPoint
- Drawings - Microsoft Visio
- Schedules - Microsoft Project

SECTION E - INSPECTION AND ACCEPTANCE

NOTE: The Section E of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

E.1 FAR CLAUSES INCORPORATED BY REFERENCE

The following clauses apply to this Task Order. Upon request the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

http://acqnet.gov/far/index.html

E.2 PLACE OF INSPECTION AND ACCEPTANCE

CLAUSE #	CLAUSE TITLE	DATE
52.246-3	Inspection of supplies – Cost reimbursement	May 2001
52.246-5	Inspection of services – Cost reimbursement	Apr 1984
52.246-11	Higher-level contract quality requirement	Feb 1999
52.246-15	Certificate of conformance	Apr 1984

Inspection and acceptance of all work performance, reports and other deliverables under this Task Order shall be performed by the COR.

E.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy and conformance to Task Order requirements by the COR. Inspection may include validation of information or software through the use of automated tools, testing or inspections of the deliverables, as specified in the Task Order. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality and adequacy of all deliverables.

The Government requires a period not to exceed 15 work days after receipt of final deliverable items for inspection and acceptance or rejection.

E.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the Task Order, the contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For software development, the final acceptance of the software program will occur when all discrepancies, errors or other deficiencies identified in writing by the Government have been resolved, either through documentation updates, program correction or other mutually agreeable methods.

Reports, documents and narrative type deliverables will be accepted when all discrepancies, errors or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments to deliverables must either be incorporated in the succeeding version of the deliverable or the contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, improper format, or otherwise does not conform to the requirements stated within this Task Order, the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the COR.

E.5 DRAFT DELIVERABLES

The Government will provide written acceptance, comments and/or change requests, if any, within 15 work days (unless specified otherwise in section F) from Government receipt of the draft deliverable. Upon receipt of the Government comments, the contractor shall have 15 work days to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The Contracting Officer (CO)/Contracting Officer's Representative (COR) shall provide written notification of acceptance or rejection of all final deliverables within 15 work days (unless specified otherwise in section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within 15 work days of the rejection notice. If the deficiencies cannot be corrected within 15 work days, the contractor will immediately notify the COR of the reason for the delay and provide a proposed corrective action plan within 15 work days.

SECTION F – DELIVERABLES OR PERFORMANCE

NOTE: Section F of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

F.1 FAR CLAUSES INCORPORATED BY REFERENCE

The following clauses apply to this task order. Upon request the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

http://acqnet.gov/far/index.html

F.2 PERIOD OF PERFORMANCE

The period of performance for this Task Order is one (1) year base period and four (4), one (1) year options for a total Period of Performance of five (5) years (if all optional periods are exercised)

F.3 PLACE OF PERFORMANCE PLACE OF PERFORMANCE IS THE XXX.

CLAUSE #	CLAUSE TITLE	DATE
52.242-15	Stop-work order	Aug 1989
52.242-15	Alternate I	Apr 1984

F.4 DELIVERABLES

The following schedule of milestones will be used by the COR to monitor timely progress under this Task Order. The following abbreviations are used in this schedule:

- NLT: No Later Than
- TOA: Task Order Award
- All references to Days: Government Workdays

NO.	DELIVERABLE	SOW REF	DELIVERY TIME
00	Project Start Date	-	TOA
	TASK 1		
01	Final Transition-In Plan	C.4.1.1	5 Days after TOA
02	Transition-Out Plan	C.4.1.2	60 Days Prior to TO expiration
	TASK 2		
03	Kick Off Meeting Agenda	C.4.2.1	3 days after TOA
04	Monthly Status Reports	C.4.2.2	10th Day of Month
05	Project Management Plan	C.4.2.3	5 days after TOA and Revised Yearly
06	Trip Reports	C.4.2.4	5 Days After end of Travel
07	QCP Update	C.4.2.5	5 Days after TOA

NO.	DELIVERABLE	SOW REF	DELIVERY TIME
08	508 Compliance Listing	C.4.2.6	30 Days after TOA
09	IPR Briefings	C.4.2.7	1 Day after IPR

F.5 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be delivered to the Contracting Officer (CO) and Contracting Officer's Representative (COR) at the address below: XXX

F.6 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT

The contractor shall notify the COR via a Problem Notification Report (PNR) Section J, Attachment H as soon as it becomes apparent to the contractor, that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including but not limited to termination.

SECTION G – CONTRACT ADMINISTRATION DATA

NOTE: The Section G of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

G.1 CONTRACTING OFFICER'S REPRESENTATIVE

The Contracting Officer will appoint a Contracting Officer's Representative (COR) in writing for each TO. The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to contractor personnel. The COR is not authorized to change any of the terms and conditions of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.2 INVOICE SUBMISSION

The contractor shall submit Requests for Payments in accordance with the format contained in GSAM 552.232-70, INVOICE REQUIREMENTS (SEPT 1999), to be considered proper for payment. In addition, the data elements indicated below shall be included on each invoice:

- Task Order number
- Paying Number
- Project No
- Project Title

The contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates and quantities of labor hours per labor category.

The contractor shall submit invoices as follows:

The contractor shall utilize electronic Tracking and Ordering System (TOS) to submit invoices. The contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

Select *Vendor Support*, log in using your assigned I.D. and password, then click on *Create Invoice*. The TOS Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to Finance Center. However, the COR may require the contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.3 INVOICE REQUIREMENTS

The contractor may invoice the fixed fee on a monthly basis. The monthly fixed fee invoiced shall be proportionate to the amount of labor expended for the month invoiced. The contractor shall submit simultaneous copies of the invoice to POC. If the Task Order has different contract types, each should be addressed separately in the invoice submission. The final invoice is desired to be submitted within 6 months of project completion.

G.4 COST PLUS FIXED FEE (CPFF) CLINS (FOR LABOR)

The contractor may invoice monthly on the basis of cost incurred for the CPFF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number

and title. All hours and costs shall be reported by CLIN element (as shown in Section B) and contractor employee and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date:

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category
- Monthly and total cumulative hours worked
- Billing rate (as proposed in the cost proposal)
- Corresponding Alliant ceiling rate
- Fixed fee
- Cost incurred not billed

All cost presentations provided by the contractor shall also include Overhead Charges, and General and Administrative Charges.

G.5 OTHER DIRECT COSTS (ODCS)

The contractor may invoice monthly on the basis of cost incurred for the ODC CLIN. The invoice shall include the period of performance covered by the invoice and the CLIN number and title and IA number. In addition, the contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required:

- ODCs purchased
- Consent to Purchase number or identifier
- Date accepted by the Government
- Associated CLIN
- Project to date totals by CLIN
- Cost incurred not billed
- Remaining balance of the CLIN

All cost presentations provided by the contractor shall also include Overhead Charges, General and Administrative Charges and Fee.

G.6 TRAVEL

The contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the JTR/FTR. Long distance travel is defined as travel over 75 miles. The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA Account number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel detail shall include separate columns and totals and include the following:

- Travel Authorization Request number or identifier
- Current invoice period
- Names of persons traveling
- Number of travel days

- Dates of travel
- Number of days per diem charged
- Per diem rate used
- Total per diem charged
- Transportation costs
- Total charges

All cost presentations provided by the contractor shall also include Overhead Charges and General and Administrative Charges.

G.7 CONTRACT ADMINISTRATION

Contracting Officer: Contracting Officer's Representative:

SECTION H – SPECIAL ORDER REQUIREMENTS

NOTE: The Section H of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

H.1 FAR CLAUSES INCORPORATED BY REFERENCE

The following clauses apply to this task order. Upon request the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

http://acqnet.gov/far/index.html

(Note: Clause numbers followed by an asterisk (*) require fill-ins by the CO)

H.1.1 52.227-15 - REPRESENTATION OF LIMITED RIGHTS DATA AND RESTRICTED COMPUTER SOFTWARE (DEC 2007)

CLAUSE #	CLAUSE TITLE	DATE
52.227-15*	Representation of Limited Rights Data and Restricted Computer Software	Dec 2007

(a) This solicitation sets forth the Government's known delivery requirements for data (as defined in the clause at 52.227-14, Rights in Data—General). Any resulting contract may also provide the Government the option to order additional data under the Additional Data Requirements clause at 52.227-16, if included in the contract. Any data delivered under the resulting contract will be subject to the Rights in Data—General clause at 52.227-14 included in this contract. Under the latter clause, a Contractor may withhold from delivery data that qualify as limited rights data or restricted computer software, and deliver form, fit, and function data instead. The latter clause also may be used with its Alternates II and/or III to obtain delivery of limited rights data or restricted computer software, marked with limited rights or restricted rights notices, as appropriate. In addition, use of Alternate V with this latter clause provides the Government the right to inspect such data at the Contractor's facility.

(b) By completing the remainder of this paragraph, the offeror represents that it has reviewed the requirements for the delivery of technical data or computer software and states [*offeror check appropriate block*]— [ ] (1) None of the data proposed for fulfilling the data delivery requirements qualifies as limited rights data or restricted computer software; or [ ] (2) Data proposed for fulfilling the data delivery requirements qualify as limited rights data or restricted computer software and are identified as follows:

(c) Any identification of limited rights data or restricted computer software in the offeror's response is not determinative of the status of the data should a contract be awarded to the offeror.

H.2 KEY PERSONNEL

The following are designated key personnel for this Task Order. The offeror shall propose appropriate labor categories for these positions.

The Government desires that key personnel be assigned for the duration of the Task Order.

H.2.1 PROGRAM MANAGER

The contractor shall identify a Program Manager to serve as the Government's point of contact and to provide technical supervision and guidance for all contractor personnel assigned to the Task Order.

The Government desires that the Program Manager has experience in managing personnel knowledgeable with network operations, software development, IA processes and procedures, system administration, and customer support. The Government desires the Program Manager have demonstrated experience in the management of Information Resource Management (IRM) projects with approximately 50 staff members, to include assignment of personnel, implementing cost controls, and developing project timelines.

H.2.2 GENERAL PERSONNEL REQUIREMENTS

See Section J, Attachment K for certification requirements.

H.2.2.1 APPLICATIONS SUPPORT SPECIALISTS

The Applications Support Specialists' desired qualifications include:

- Working knowledge and experience with the management and implementation of software applications
- Working knowledge and experience with scheduling, management and installation of COTS/GOTS software updates
- Working knowledge and experience with test and implementation plans for COTS / GOTS software updates
- Working knowledge and experience with batch and interface processes during application release testing
- Working knowledge and experience with troubleshooting COTS / GOTS application anomalies
- Working knowledge and experience with Software Application Administration, Routine Maintenance and Data Management
- Working knowledge and experience with Information Assurance policies and procedures with respect to software development
- Working knowledge and experience with Web-Based Applications and Systems including analysis, design, evaluation, programming, and support
- Working knowledge and experience with developing system application documentation
- Working knowledge and experience with providing software maintenance and troubleshooting services in support of Software Engineering Projects
- Excellent written and oral communications skills

H.2.2.2 APPLICATIONS OPERATORS

The Applications Operators' desired qualifications include:

- Working knowledge and experience with developing and maintaining data processing schedules
- Working knowledge and experience with executing and monitoring application interface and batch processes

- Working knowledge and experience with capturing, troubleshooting, and reporting anomalies of application, batch, interface, or system failures
- Working knowledge and experience with respect to analyzing, coding, and coordinating daily settings of process control codes for payroll and cost applications
- Working knowledge and experience with monitoring server status and utilizing software tools
- Working knowledge and experience with operating data processing printing equipment including scheduling and distribution of print jobs
- Excellent written and oral communications skills

H.2.2.3 SYSTEM ADMINISTRATORS

The Systems Administrators' desired qualifications include:

- Maintaining the functionality of Microsoft Windows and SUN Solaris / IBM AIX UNIX servers,
- Implementing updates in server hardware and software,
- Managing server configuration,
- Monitoring and managing use of disk space, memory, and connections,
- Managing accounts and permissions Windows and UNIX servers,
- Performing server backup and restore,
- Diagnosing system problems,
- Monitoring server performance and performing tuning enhancements,
- Troubleshooting and fixing hardware or software problems, and
- Managing server event logs.

H.2.2.4 CUSTOMER SUPPORT SPECIALISTS

The Customer Support Specialists' desired qualifications include working knowledge and experience with:

- Troubleshooting hardware and software,
- Equipment technical evaluation,
- User account management,
- IT user training,
- IT asset inventory,
- Providing IT services (e.g., moves, adds, changes (MACs), remedy tickets, NMCI trouble tickets, etc),
- Administration and management of global groups, distribution lists, public folders, account management, and remedy accounts,
- Managing IT hardware lifecycle management program,
- Replacing IT consumables,
- Maintaining IT equipment and consumable inventories,
- Distribution management of cell phones, blackberries, and accessories, and
- Excellent written and oral communication skills.

H.2.2.5 IA SUPPORT SPECIALISTS THE IA SUPPORT SPECIALISTS' DESIRED QUALIFICATIONS INCLUDE:

- Computer Information System Security Professional (CISSP)
- Experience with Security Management policy guidance and directives
- Knowledge and experience of current and emerging information assurance enterprise security practices
- Experience with DIACAPs, vulnerability assessments, IAVA reporting, and IA problem resolution
- Ability to convey complex information assurance data to a wide variety of government audiences
- Demonstrated oral and written communication skills

H.2.3 KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as key personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than 10 calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action as prescribed by FAR 52.249-6 Termination (Cost Reimbursement) or FAR 52.2498, Default (Fixed-Price Supply and Service).

H.3 RESERVED

H.4 RESERVED

H.5 GOVERNMENT FURNISHED PROPERTY (GFP)

H.5.1 GOVERNMENT-FURNISHED SPACE AND EQUIPMENT

The Government will provide on-site office facilities (computer, printer, desk, chair, telephone service) for up to fifty (50) contractor personnel at the appropriate sites (including one in Japan, two in San Diego) to complete requirements identified in this Task Order.

H.5.2 CONTRACTOR-FURNISHED VEHICLES

The contractor shall provide vehicles for tasks that require transportation of personnel or materials. The contractor personnel shall have insurance coverage that will allow them to operate the vehicles.

Throughout the life of this Task Order, the contractor may also be required to operate Government-owned vehicles to carry out duties described in the TO. The contractor shall maintain insurance in accordance with above paragraph.

H.6 SECURITY REQUIREMENTS

Security Clearance: Contractor personnel will be assigned to positions designated as IT-1 Critical Sensitive or IT-2 Non-Critical Sensitive as defined in SECNAV M-5510.30 Paragraph 5-3, subparagraph b(6), and Exhibit 5A.

Personnel requiring privileged access to the Government systems (e.g., System Administrators) are required to meet Information Assurance performance and IA certification requirements in accordance with DoD Manual 8570-1M, Chapter 3. Performance requirements will be set based on operating environment at the Information Assurance Technical level (IAT) I, II or III.

All Contractor personnel working on this Task Order must be U.S. citizens, and will be required to a minimum clearance equal to CONFIDENTIAL for Special Handling and Not For Release to Foreign Nationals (NOFORN) information will be required by all contractor personnel working on-site. Additionally, the OCONUS support functions may require higher-level clearance. These requirements will be identified by specific task and sub-task. This Task Order will also deal with sensitive data. Any password or user identification requirements will be coordinated through a designated Representative. A DD Form 254, Department of Defense Contract Security Classification Specification, will be provided at the time of award. The Contactor and COR will coordinate all security requirements and forward a completed DD Form 254 to the Contracting Officer for incorporation into the Task Order.

Information Assurance: Contractor personnel supporting this Task Order who require access to Government Information Systems are required to receive and complete; initial IA orientation awareness and Unclassified-Naval Nuclear Propulsion Information (U-NNPI) training before being granted access to the system(s) and annual IA awareness training to retain access, as required IAW DoD 8570.01-M and DODI 8500.2 E3.3.7. Access requests to IT systems will utilize OPNAV 5239/14 (July 2008) SAAR-N form.

H.7 INFORMATION ASSURANCE CERTIFICATION

Contractor personnel must agree as a "condition of employment" to obtain and maintain currency for appropriate certification(s) required for the position IAW DoD 8570.01M. All training and certification specifications are required to be met within six (6) months for any currently contracted employee, and must be met within six (6) months of any newly reporting personnel being assigned. The Contractor shall meet the applicable IA certification requirements, including:

- Agency-approved IA workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M
- Appropriate operating environment certification for IA technical positions as required by the Government 8570.01-M
- Upon request by the Government, the Contractor shall provide documentation supporting the IA certification status of personnel performing IA functions

Contractor personnel who do not have proper and current certifications shall be denied access to Government information systems for the purpose of performing IA functions. See Section J, Attachment K for certification guidance.

H.8 ORGANIZATIONAL CONFLICT OF INTEREST

If the contractor is currently providing support or anticipates providing support to the Government that creates or represents an actual or potential organizational conflict of interest (OCI), the contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the contractor (and any Subcontractors, consultants or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

H.9 NON DISCLOSURE REQUIREMENTS

If this TO requires the contractor to act on behalf of, or provide advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall ensure that all its personnel (to include Subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

- Execute and submit an "Employee/Contractor Non-Disclosure Agreement" Form (Section J, Attachment F) prior to the commencement of any work on the Task Order
- Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information
- All proposed replacement contractor personnel also must submit a Non-Disclosure agreement and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.10 CONTRACTOR'S PURCHASING SYSTEMS

The objective of a contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a Task Order the Contracting Officer shall verify the validity of the contractor's purchasing system. Thereafter, the contractor is required to certify to the Contracting Officer no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the contractor shall provide the results of the review to the Contracting Officer within 2 weeks from the date the results are known to the contractor.

H.11 PRIVACY ACT

Work on this project may require that personnel have access to Privacy Information. Personnel shall adhere to the Privacy act, Title 5 of the U.S. Code, Section 552a and applicable agency rules and regulations.

H.12 TASK ORDER CLOSEOUT

The contractor shall submit a final invoice within forty-five (45) calendar days after the end of the Performance Period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

H.13 PAST PERFORMANCE INFORMATION

In accordance with FAR 42.15 Contractor Performance Information, past performance evaluations shall be prepared for each task order that exceeds the simplified acquisition threshold placed against a Government-wide Acquisition Contract. For severable task orders, interim evaluations will be required prior to exercising any option periods. For non-severable task orders, evaluations must be collected, coordinated and reported upon completion of the task order.

The Government will provide and record Past Performance Information for acquisitions over $100,000 utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS).

Contractors are required to register in CPARS, so contractors may review and comment on past performance reports submitted.

Contractors must register at the following websites:

CPARS: http://www.cpars.csd.disa.mil/

PPIRS: http://www.ppirs.gov/

H.14 H.14 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

(1) Federal Travel Regulations (FTR) - prescribed by the General Services Administration, for travel in the contiguous United States.

(2) Joint Travel Regulations (JTR), Volume 2, prescribed by the Government, for travel in Alaska, Hawaii, and outlying areas of the United States.

(3) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas", prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.15 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Contract, the contractor shall have this travel approved by, and coordinated with, the COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the

contractor shall prepare a Travel Authorization Request for Government review and approval. Long distance travel will be reimbursed for cost of travel comparable with the Joint Travel Regulations (JTR). If overseas travel is contemplated on the Task Order, the contractor shall also refer to the DSSR.

Requests for travel approval shall:

- Be prepared in a legible manner
- Include a description of the travel proposed including a statement as to purpose
- Be summarized by traveler
- Identify the Task Order number
- Identify the CLIN and Interagency Agreement account associated with the travel
- Be submitted in advance of the travel with sufficient time to permit review and approval

The contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.16 TRIP REPORTS

See paragraph C.4.2.6.

H.16.1 PASSPORT

Contractors going on OCONUS travel are required to obtain and maintain a United States passport.

H.17 ODCS

The Government may require the contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO, by the Government or the contractor. If the contractor initiates a purchase within the scope of this TO and the prime contractor has an approved purchasing system, the contractor shall submit to the COR a Request to Initiate Purchase (RIP). If the prime contractor does not have an approved purchasing system, the contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO. ODCS include overseas allowances.

H.18 TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS

If the Contractor acquires hardware/software maintenance support, all licenses and/or contractual rights to receive title shall be turned over to the Government upon completion of the Task Order.

The Government's liability to reimburse the contractor for costs incurred from the acquisition of hardware/software maintenance support SHALL BE LIMITED to costs incurred during the period of the order for which the Government received the hardware/software maintenance support acquired by the contractor on a cost reimbursable, fee basis.

H.19 ADMINISTRATIVE CONSIDERATIONS

H.19.1 REGULATIONS

The contractor and its employees shall become familiar with and obey all station regulations, including fire, traffic, cell phones, and security regulations. All contractor-employed personnel on the station shall keep within limits of the work (and avenues of ingress and egress) and shall not enter any restricted areas unless required to do so and are cleared for such entry. The contractor's equipment shall be conspicuously marked for identification.

H.19.2 PUBLIC RELEASE OF INFORMATION

The contractor shall not publicly disclose any information concerning any aspect of the materials or services related to this TO without the prior written approval of the COR.

H.19.3 RADIO TRANSMITTER RESTRICTIONS

The contractor shall not operate citizens band or amateur radio equipment (receive or transmit) within the geographic limits of the Station without permission of the Radio Frequency Officer. The contractor shall turn off all radio-transmitting equipment installed in privately owned motor vehicles upon entering the Station premises.

H.19.4 EXTRAORDINARY RESTRICTIONS REGARDING ACCESS OF VEHICLES AND PARKING

All contractor vehicle traffic shall enter Controlled Industrial Area at the Gate. The contractor shall ensure no equipment delivery traffic will occur between the hours of 0700 through 0800 and 1600 through 1700, Monday through Friday.

H.19.5 PRIVATE VEHICLE RESTRICTIONS

No contractor employees or representatives shall park private vehicles in the controlled areas of the Government. The contractor shall clearly mark any and all vehicles and equipment needed to perform work with proper insignia (company name) on the outside of the vehicle.

H.19.6 PHOTOGRAPHY AND RECORDING EQUIPMENT

The contractor shall not bring any photographic equipment, camera cell phones, camera black berries, video tape recorders, or recording devices at all the Government locations.

H.19.7 RESTRICTED USE OF COLORS

The contractor shall not use the colors Yellow, Blue, Magenta, and Red, as these are colors the agency uses to identify specially controlled materials. Garbage bags, plastic tape, bags, covers, or wrapping materials in these colors shall not be used by the contractor at the Station. The contractor shall recognize that Blue is used for Asbestos identification only and clearly identified as Asbestos; Red is used for Mercury-bearing material and clearly identified as Mercury.

H.20 OCONUS REQUIREMENTS

Contractor support shall include having contractor personnel in the Pacific Operations. Currently contractor support is being provided in Japan. The contractor shall be familiar with and be able to adhere to regulations (i.e. SOFA) governing contractor employment in Japan. The contractor shall be capable and able to provide staffing in countries other than Japan in the Pacific Operations.

SECTION I – CONTRACT CLAUSES

NOTE: The Section I of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

I.1 FEDERAL ACQUISITION REGULATION (48 CFR CHAPTER 1) SOLICITATION CLAUSES (HTTP://WWW.ARNET.GOV/FAR/)

CLAUSE NO CLAUSE TITLE DATE

52.217-8 OPTON TO EXTEND SERVICES (NOV 1999)

Fill-In Date: 30 days prior to expiration of Task Order.

52.217-9 OPTION TO EXTEND THE TERM OF THE

(SEP 2006)

CONTRACT: 30 days prior to expiration of Task Order.

I.2 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM) CLAUSES

CLAUSE NO CLAUSE TITLE DATE 552.232-1 Payments (APR1984)

I.3 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE SECTION J – LIST OF ATTACHMENTS

CLAUSE NO	CLAUSE TITLE	DATE
252.204-7004	Required Central Contractor Registration	(Nov 2001)
252.227-7013	Rights in Technical Data - Noncommercial Items	(Nov 1995)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Jun 1995)
252.227-7016	Rights in Bid or Proposal Information	(Jun 1995)
252.227-7019	Validation of Asserted Restrictions - Computer Software	(Jun 1995)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.239-7001	Information Assurance Contractor Training and Certification	(Jan 2008)
252.246-7001	Warranty of Data	(Mar 2003)

NOTE: The section numbers in this Task Order correspond to the section numbers in the Alliant Contract. Section J of the contractor's Alliant Contract is applicable to this Task Order and is hereby incorporated by reference. In addition, the following applies:

SECTION J – LIST OF ATTACHMENTS

Attachment A - Use Cases

Attachment B - Glossary and Abbreviations

Attachment A Use Cases

The following Use Cases are intended to assist the respondent with architecting a solution that will address the operational requirements of Government Agencies. They are written in a scenario format, with specific requirements highlighted.

Use Case #1 – New Hire

Required capabilities:

1. Multiple group policies per device
2. Automatic application deployment
3. Enterprise Application Management (MAM)
4. Enterprise Application Store (MAS)
5. Enterprise email integration
6. Device data monitoring, location monitoring

A new IRS field agent is hired and issued an agency device. The device is enrolled by the MDM system, and the device is added to the "Field Agents" policy group. This policy automatically pushes a set of required applications to the device, including an MDM agent, email client, agency secure intranet web browser, and enterprise application store, each installed in the secure managed container the MDM agent has set up on the device.

The MDM agent also prompts the user to define required device and container PINs. The new field agent's manager emails her a list of suggested applications to install from the enterprise application store, and recommends a free navigation application from the vendor application store. In a few weeks the new field agent has completed training, and their device is added to a new policy group that pushes the case history application to her device and enables use of the camera to capture document images.

Use Case #2 – Bring Your Own Device (BYOD)

Required Capabilities:

1. Black / Whitelisting
2. Automatic policy control implementation (in this case, location privacy)
3. Role-based access to applications
4. Application utilization, version
5. CAC / PIV authentication to management site
6. Separation of Personal and Business Data

An agency staffer is using a personally-owned device, an Android, to access enterprise data (BYOD). Their manager has approved them in the MDM portal, and assigned them a default device profile. The MDM portal sends an email to the staffer with a link to the portal. The staffer logs in to the portal with their agency PIV card, and is instructed to install the MDM

application from the public Google Play application store. After registering their device through the MDM application, the application blocks further connection to the enterprise because the staffer's device is not at the minimum Android OS version required. After the device is updated to the current OS available from their carrier, the MDM application enables connection to email, contacts and calendar. Since the device is identified as "BYOD" in the MDM management portal, continuous location tracking of the device through the MDM application is automatically disabled. It is still available on-demand if the device becomes lost or stolen.

A few days later the staffer learns of an enterprise application they think may help their work. The staffer attempts to install the application from the enterprise application store, but is denied. They contact their manager, and are told that the application is licensed, so distribution is limited to minimize costs. The manager authorizes the user for the application by adding them to that application's "permit" policy, and the user installs the application. 45 days later the staffer receives an automated email from the MDM that they haven't used the application in 30 days, and if they don't plan to use it to uninstall it as it's a per-user license application. Three months later, the manager receives a notification from the MDM system that their staffer hasn't used this application in over a month.

After discussing with the staffer, the manager discovers the application isn't as helpful as the staffer thought it would be, and they agree to remove it and release the license for the application. The manager removes the staffer from the application "permit" policy, and the application is automatically removed from their device.

Use Case #3 – Lost / Stolen Device (Unrecovered)

Required Capabilities:

1. Remote container wipe
2. Remote device wipe
3. Device location tracking
4. Device status reporting
5. User self-enrollment
6. BYOD provisioning

A GSA employee requests email, calendaring and contacts (Personal Information Management, or PIM) access on his personally-owned device. After management approval, the GSA help desk sends him an enrollment text message to his device. He enrolls his device into the MDM system and downloads the PIM application. The MDM solution requires he lock the device with a strong PIN. One morning he discovers his vehicle has been broken into and his device stolen. He calls the enterprise help-desk to report the loss, and since this is a personally-owned device he is asked for permission to turn on location tracking. The help desk locates the device across town in a location not familiar to the employee, and confirms the device has been locked since the night before. He asks the help-desk to remotely wipe the entire device. The employee reports the device stolen to law enforcement and his carrier, who issues him a new device after he pays a deductible. He contacts the help desk again to have the new device provisioned.

Use Case #4 – New Application Deployment

Required Capabilities:

1. Application selection and approval by either whitelist or blacklist approach

2. Application deployment via Over the Air (OTA)
3. Application deployment via role-based, organization, level, and/or other application policy parameters
4. Application selection and management as a function of enterprise or personal application status

Agency employees may select and download mobile applications based on their agency or organization's specific policy which may represent whitelist (approved application meeting a certain criteria) or blacklist (any application except those specified). Additional mobile application accessibility and mobile application management functionality may also reflect other agency policies including role/function (defined by OPM position # or agency), organization (agency, sub-agency, location, region, etc.), device ownership status (government, employee, other) and employee level (e.g., rank, pay scale, etc.).

The agency may also dictate application release management and application access to data as a function of the agency application policy.

Use Case #5 – Blocking of Inappropriate Website

1. Site blacklisting
2. Application blacklisting
3. Reporting possible erroneous filtering / blocking

A user receives an email from a colleague with several URLs taken from a web forum posting that address an area of interest to the user. The user selects each URL in turn on her device to view the content. The first link is uninteresting, but when she selects the second link her device informs her access is prohibited as it is listed as a gambling site. She observes that the link is a misspelling of a common web site, and successfully tries manually entering a corrected link.

The third link produces a message that the requested site is blocked for containing malware. Noting the URL is a .EDU website at a major university and suspecting this is an error, she selects the option to have the URL manually reviewed.

Use Case #6 – Security Problem Identified on Device

1. Ability to perform application installation in stages
2. Ability to control application installation via cellular or WiFi
3. Deployment policy for applications and device policies
4. Ability to report application presence on devices
5. Ability to define a policy for specific device types, operating system versions, or combinations of device configurations or settings

A new SMS attack on Android devices is announced, and the Agency has more than 10,000 devices that are on the list of vulnerable targets. The Agency identifies and tests an on-device SMS-filtering solution and decides on immediate deployment, notifying users via email about the new application. The MDM Administrator loads the approved application into the MDM private application store, associates it as a required application with the group policy governing the affected users, and sets the required OS version. She then has the MDM solution select 10% of the devices and deploy the application with a deployment policy that automatically installs the application if WiFi connectivity is present. After a few hours the MDM Administrator observes several hundred successful installs with no associated help-desk tickets, and instructs the MDM

solution to deploy the update via WiFi to all users. After 48 hours 80% of the devices have received the application. The SMS-filtering application is beginning to report actual SMS attacks attempted against devices (an application feature not required of the MDM), and the Agency governance decides that the application should be deployed to remaining users, regardless of the availability of WiFi. The MDM Administrator updates the deployment policy for the application, marking it as required, immediate installation, no connectivity restrictions. Within an hour 97% of the devices are running the new application. The MDM Administrator generates a list of user emails for devices that do not yet have the application installed. The Agency sends an email to the affected users requesting them to facilitate the update immediately, warns them of the threat, and lets them know that SMS will be disabled for their device in two days if the update is not installed. They are advised to contact the help desk for assistance. After two days, the MDM Administrator generates a list of remaining devices without the application and passes it to the service account management team. After receiving approval the account management team disables SMS service on those devices, and informs the MDM Administrator. She sends a notification email to the affected users about the change to their device plans, and directs them to the Help Desk for assistance.

Use Case #7 – Application Update

1. Automatic application updating
2. Custom user notifications and actions for policy events
3. Monitoring and reporting of application versions
4. Specify device state requirements for policy enforcement

A new version of application is available to two users, Fred and Ginger. They both receive messages on their device when they next run the application. They are told the application must be updated before a certain date and are asked they want to install the update now, be reminded later, or not be interrupted with the update message. Ginger chooses to be reminded later, and later that day installs the application update. The MDM application version monitoring system reflects Ginger's updated application in its statistics.

Fred has time-critical tasks to complete, and chooses to not be reminded any more about the update. The device informs him the update will happen automatically after the deadline. He forgets about the update after a few days, and the time limit for installing the update passes. The application deployment policy will enforce the update automatically, but only when connectivity is over WiFi, to not consume data from the device airtime plan. The MDM agent watches each start of the application, and when it is started while the device has WiFi connectivity, informs Fred that the application will now be updated. The application is updated, the MDM monitoring records the successful update, and Fred's device is now compliant.

Use Case #8 – Lost Device (Recovered)

Required Capabilities:

1. Device Location Tracking
2. User Self-Service

One day a user realizes she doesn't have her Government-Furnished device. In the user self-service portal to the MDM system she looks up her device based on the mobile number and name, and requests the device report its location and status. Since she has been authenticated

with her PIV card, the system identifies her as authorized. In a few minutes the device reports its location through the MDM portal. It is at a local library, and there have been no PIN failures (attempted accesses). She notes the address, and instructs the device to display a "lost phone" message with a callback number and sound a tone. The user heads to the library and is able to recover the device.

Use Case #9 – Mobile Law Enforcement or Inspection Worker with Tablet and Custom Application

Required Capabilities:

1. Device Location Tracking
2. Containerized application with ability to synchronize data with enterprise database remotely via secure, encrypted connectivity.
3. Commercial-off-the-shelf tablet computer with cellular service plan and agency-specific application

An agency has an organization of remote and mobile employees that use a tablet computer to record data for both law enforcement and on-site inspection activities. The data is immediately transported via the cellular network to the agency enterprise database where it is recorded and processed for analysis and transactions. Data may occasionally be sensitive but unclassified. Reliable, secure, and compliant communication is required. The agency may periodically push related application updates via Over-the-air as the employees may have limited access to agency buildings and on-site infrastructure.

Use Case #10 – Agency users want to access enterprise applications using their mobile device and/or tablet.

Required Capabilities:

1. PIV card authorizes MDM to create derived credential
2. New logical credential stored in mobile device
3. Maximize reuse of PIV data model

An agency as an organization of remote and mobile employees that use a mobile device and/or tablet computer to access the agency resources must be able to authenticate using their PIV cards. In most cases the mobile device and/or tablet computer may not support a card reader and it may not be practical for the agency user to have to carry around a card reader. The mobile platform must allow an agency to authenticate to agency applications at the appropriate level of assurance for that application.

Attachment B - Glossary and Abbreviations

Term	Description
Agency	"Department" or other administrative unit of the federal government, such as the General Services Administration (GSA), which is using this contract vehicle. This also includes quasi-government entities, such as the United States Postal Service.
Blacklist	Application or software not deemed acceptable and have been denied approval. This may vary between agencies.
Bureau	A sub-Agency Bureau level organization, which is using this contract vehicle, as defined by OMB (www.whitehouse.gov/sites/default/files/omb/circulars/a11/current_year/s79.pdf).
BYOD	Bring Your Own Device; Staff bring their personally-owned devices and the Enterprise installs capabilities such as email on them. May also refer to bringing devices from other agencies.
CAC	Common Access Card; a 2-factor electronic identity card used by the Department of Defense to identify individuals. The civilian equivalent is the Personal Identity Verification (PIV) card.
Capability	A technical service requirement that is a component of the base service.
COTS	Commercial Off-The-Shelf; solutions that can be purchased in a complete form from existing commercial vendors.
Data Plan	Includes web browsing, send and receive email, download attachments, downloading applications, and application data usage.
Device	Also called handheld wireless devices, these include handheld devices that are capable of wireless voice or data communications. The devices support cellular or paging technologies augmented by technologies such as WLAN and satellite.
Feature	An enhancement beyond base service that is to be selected at the option of the user. Features are normally separately priced, although some features have been defined to be not separately priced (NSP). Each feature must be ordered separately even if not separately priced.
FAS	Federal Acquisition Service.
FICAM	Federal Identity, Credential, and Access Management mainly addresses user certificate authentication although it does touch on passwords. FICAM is the guidance document, ICAM is the body that created it.
FIPS	Federal Information Processing Standards.
FSSI	Federal Strategic Sourcing Initiative; FSSI Wireless provides wireless service and device ordering capabilities to Government agencies.
GB	Gigabyte or 1000 MB of data.
GFE	Government Furnished Equipment.
GPS	Global Positioning System; A network of orbiting satellites that enable receivers on the ground to report their position, velocity and time. Mobile devices often use Assisted GPS (AGPS) which leverages cell towers to speed reporting time.
Government	All government entities that use or administer this contract vehicle, including state, local and education.
Government Web Store	Concept of web-based acquisition interface and management platform where government stakeholders (employees, citizens, partners) may initiate purchases, manage previous purchases, and manage contractor relationships. Concept is based on enterprise version of a commercial web storefront.

Term	Description
HSPD-12	Homeland Security Presidential Directive 12, which (among other things) directs agencies to deploy 2-factor authentication for information systems.
M2M	Machine to machine technologies that allow both wireless and wired systems to communicate with other devices of the same ability.
MAS/MAM	Mobile Application Services/Mobile Applications Management.
MB	Megabyte, a common term used to describe the amount of data being sent over a wireless network.
Mbps	Megabits per second, a common term used to describe wireless transmission speeds.
Mobile Device	Characteristics include 1) a small form factor, 2) at least one wireless network interface for Internet access or voice communications, 3) built-in (non-removable) data storage, 4) an operating system that is not a full-fledged desktop or laptop operating system, 5) built-in features for synchronizing local data with a remote location (desktop, laptop, organizational servers, etc.) if data capable, 6) generally operates using battery power in a non-fixed location.
Mobile Device Management (MDM)	MDM – Mobile Device Management. MDM is a widely used term describing 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. The definition of MDM varies and reflects its growth (pre-maturity) status.
Ordering Entity	Any Agency, sub-Agency, state or local government that is using this contract vehicle.
Ordering Agency Portal	The Government Agency that is using this contract vehicle. There may be one or more Ordering Entities under an Ordering Agency. A software (or web) solution that enables instant and effortless exchange of business information (Electronic Data Interchange – EDI) over the Internet. This is accomplished by the use of a common operating framework for accessing data and information from different systems. A typical TEMS portal will pull information from carrier electronic billing systems, which is uploaded into their platform (portal). This allows the administrator/user a single view that provides multiple carrier information in a seamless manner, offering efficiency.
Secure Communications	Communication services that includes security components such as encryption to ensure the privacy and integrity of the communications.
Smartphone	Electronic handheld wireless device that integrates the functionality of a mobile cellular phone, personal digital assistant (PDA) or other information appliance.
Subsystem	A subsystem is a set of elements, which is a system itself, and a component of a larger system (Wikipedia). For instance, a subsystem could include both the encryption software and the related software on the server.
TEMS	Telecommunications Expense Management Services, delivered by third parties, relating to processes for the sourcing, procurement and auditing functions connected with business communications expenses. It also considers nonrecurring services, such as one-time historical audits, and other advisory services relating to enterprises' communications expenditure [Gartner].
Text Messaging or SMS	Text Messaging or Short Message Service (SMS) is the exchange of brief written messages between cellular phones, smartphones, and data devices over cellular networks.
Third-Party Direct Billing	The receipt of invoices from parties other than the Contractor for services within or outside the scope of this agreement.

Term	Description
Trade Agreements Act (TAA)	The TAA of 1979 is an Act of Congress that governs trade agreements negotiated between the U.S. and other countries under the Trade Act of 1974. Its stated purpose is to: 1) Approve and implement the trade agreements negotiated under the Trade Act of 1974 [19 U.S.C. 2101 et seq.]; 2) Foster the growth and maintenance of an open world trading system; 3) Expand opportunities for the commerce of the United States in international trade; and 4) Improve the rules of international trade and to provide for the enforcement of such rules, and for other purposes. The TAA designated countries are listed in the following web site: http://gsa.federalschedules.com/Resource-Center/Resources/TAA-Designated-Countries.aspx
Trouble Ticket	Also called a trouble report, this is the documentation of a service or device failure that impacts the service. The ticket enables an organization to track the detection, reporting, and resolution of some type of problem.
WLAN Calling	Wireless Local Area Network: Enables a wireless handset to make and receive calls via an internet-connected WLAN (e.g., Wi-Fi network) instead of the cellular network.
White List	Whitelist: Application or software considered safe to run, and is preapproved.
Wireless Systems and Subsystems	Wireless infrastructure, servers, and software that enable an enterprise to enhance its cellular coverage, increase cellular capacity, and enable enterprise solutions (e.g., BlackBerry Enterprise Server) using services offered by the wireless industry.
24/7 phone support	Technical support and user assistance is provided by telephone and Internet 24 hours a day, 365 days (or 366 during leap years) per year.

Addendum

Task 1 – Life Cycle Management

Mobility Life Cycle Management	All Required	SOW Section Reference
1. Project Management: Does the proposed solution clearly demonstrate past experience in developing and implementing a Project Management Plan directly related to Managed Mobility, and how this example of project management tracked the quality and timeliness of the delivery of the required elements? (Y/N)	Required	
2. Professional Services: Does the respondent clearly describe how they provide initial deployment support services including installation, configuration, and the certification of initial solutions, as well as for additional professional services to support specific agency related integrations or customizations? (Y/N)	Required	
3. Enterprise System Integration: Does the respondent demonstrate experience in providing the steps necessary for deploying, integrating, and securing a mobility solution into an enterprise-wide environment? (Y/N)	Required	
4. Training: Training: Does the respondent demonstrate how they can be responsible for developing and updating the MDM-MAS Training Material content (Enterprise, User, Administration levels) as well as providing prepackaged online training, training classes and associated materials described in the Training Plan? (Y/N)	Required	
6. Operations Support: Does the respondent/solution provide access to help desk support that meets the identified criteria? (Y/N) Does the respondent indicate the location of their help desk support? (Y/N)	Required	
5. Demonstration Platform: Does the proposed solution possess a fully functional and secure demonstration platform with associated mobile devices to educate potential customers on the use, benefits and technical specification of the solution, and will it provide access to the portal for the purpose of sampling and demonstrations that will be connected to the respondent's site through a federal website? (Y/N)	Required	
7. Past Performance - Has the respondent provided past performance with references that include solution installations that are similar to the solution being offered within this RFP/SOW? If other partner solutions are being used to fulfill the requirement identified in the RFP/SOW, has the respondent described how the solution has been tested and sold to other government agencies? (Y/N)	Required	
8. Enterprise Configuration: Does the respondent demonstrate the non-core integration services as indicated? (Y/N)	Optional	

9. Integration with FSSI Wireless Portal: Does the respondent demonstrate how to integrate their proposed solution with the FSSI Wireless portal to automatically retrieve asset and plan data, and return relevant data to the FSSI portal?	Optional	
10. Pilot - The proposed solution will be delivered within the pre-production pilot timelines and installation dates identified in this RFP and agreed to in the SOW.	Optional	

Task 2 – Provide High Level Architecture

High Level Architecture Requirements & Respondent Capabilities/Experience	**Required or Optional**	**SOW Section Reference**
1. Scope/Scale: Is the respondent's solution scalable from an initial requirement of X users to the maximum requirement of Y users? (Y/N)	Required	
2. Multi-Tenancy: Does the proposed solution support the Department's / Agency's ("tenants") hierarchical organizational structure to apply hierarchical policy requirements within the solution, and support multiple configurations for each of the MDM requirements? (Y/N)	Required	
3. Solution Security: Does the proposed solution describe how they meet the 14 identified general controls/capabilities of solution security? (Y/N)	Required	
4. FISMA or FedRAMP : Does the respondent provide evidence that the proposed solution is capable of being certified at the FISMA moderate impact level? (Y/N)	Required	
5. FIPS Requirements: Does the respondent provide evidence that their solution uses FIPS 140 certified cryptographic modules and continued validation? (Y/N)	Required	
6. Containerization: If applicable, does the respondent describe how the proposed solution meets FIPS 140-2, controlled wipe capabilities, and platform-by-platform container protection as it related to BYOD scenarios? (Y/N)	Required	
7. IPv6 Support: Does the respondent provide evidence of either IPv6 compliance Program of Actions/Milestones (PoAM) signed by company official on plan to comply? (Y/N)	Required	
8. User Authentication: Does the respondent provide evidence of being capable of meeting HSPD-12 and associated NIST authentication standards related to the portal and device support, as well as support 2 multifactor authentication methods? (Y/N)	Required	
9. User Compliance: Does the proposed solution demonstrate the 4 items related to user compliance enablement? (Y/N)	Required	

10. Alerting: Does the proposed solution demonstrate the 8 alert capabilities required to notify agency operations staff via console display as well as appropriately via email and/or text message about devices under their management? (Y/N)	Required	
11. Security Reporting Capabilities: Does the proposed solution demonstrate the 8 reporting capabilities, as well as the stated support functions applicable to Audit Reports? (Y/N)	Required	
12. Privacy: Does the proposed solution disclose privacy-impacting features that cannot be disabled? (Y/N)	Required	
13. Service Delivery Model: Is the proposed solution delivered and by the provider as a full solution including all hardware, software, hosting, and installation services, using the [Select one on premise, Cloud, Hybrid]:? (Y/N)	Required	
Task 3 – Provide Mobile Device Management		
MDM Requirements & Respondent Capabilities/Experience	**Required or Optional**	**SOW Section Reference**
1. General MDM Capabilities: Does the proposed solution address/describe how their solution meets all 10 of the mandatory general MDM requirements? (Y/N)	Required	
2. Device Enrollment: Does the proposed solution demonstrate the 20 capabilities identified regarding the ability to add a device to an MDM management domain? (Y/N)	Required	
3. Device Profiles: Does the provider support the 22 items related to the creation of per-user and per-group device profiles? (Y/N)	Required	
4. Device Feature Management: Does the proposed solution demonstrate the 8 required features and capabilities identified regarding device feature management? (Y/N)	Required	
5. Data Management: Does the proposed solution demonstrate the ability to read, write transmit and receive data on mobile devices as well as with backend systems/repositories to include meet FIPS 140 requirements? (Y/N)	Required	
6. Data Collection: Does the proposed solution demonstrate the ability to collect and report on the 6 data points identified? (Y/N)	Required	
7. Continuity of Operations and Disaster Recovery: Does the proposed solution describe how it performs Continuity of Operations (COOP) and Disaster Recovery (DR)? (Y/N)	Required	

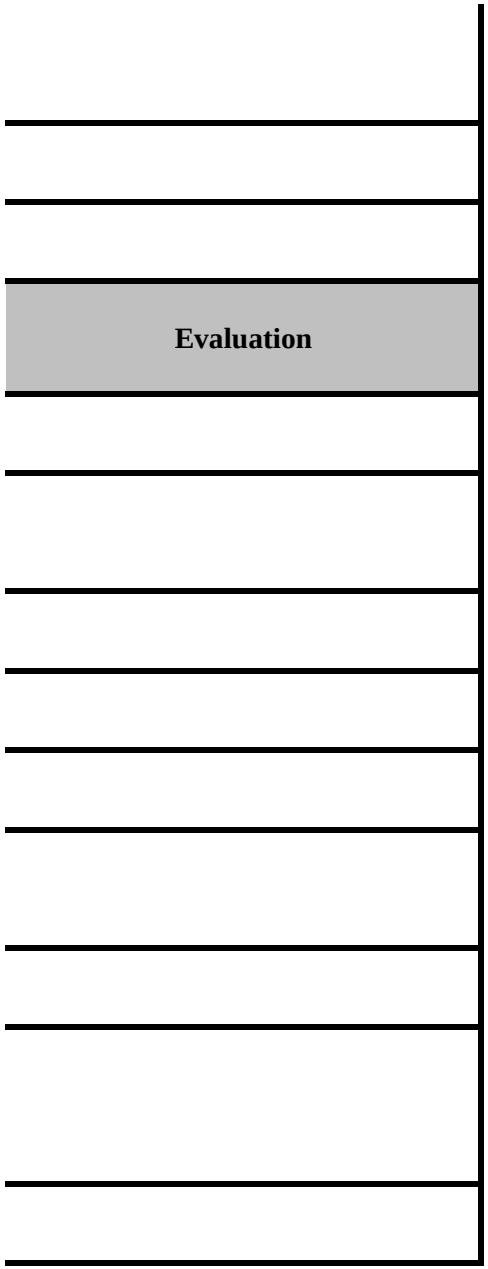
8. File Management: Does the proposed solution demonstrate that the solution is able to hold a set of COTS and/or enterprise applications with respective data/files in a FIPS 140 secured space (e.g. whole device encryption, container or VDI) solution? Does the proposed solution also demonstrate how the solution is able to share files between applications, between mobile devices, and/or between devices and hosted file servers based on application and security requirements? (Y/N)	Required	
9. Personal Information Management: Does the proposed solution demonstrate the solution's ability to provide/enable a secure Personal Information Manager (PIM) capability with email, calendar, and address book capabilities, as well as be capable of synchronizing files and data between the device and file servers by the use of a secure encrypted connection? (Y/N)	Required	
10. Security Content Automation Protocol (SCAP) Support: Does the proposed solution demonstrate the ability to support server-side components, including asset management, configuration management, patch management and remediation capabilities? (Y/N)	Required	
11. Device Inventory Management: Does the proposed solution demonstrate the ability to include a set of mechanisms to provision, control and track devices connected to corporate applications and data, and to relate this data to user information? Does it record, track and manage the 16 pieces of information identified in inventory management? (Y/N)	Required	
12. Device Inventory Reports: Does the proposed solution demonstrate the ability use the identified filters to run or export device inventory reports associated with the device, OS, and applications? (Y/N)	Required	
13. System Performance Reports: Does the proposed solution demonstrate the ability to run system performance reports using the identified filters? (Y/N)	Required	
14. MDM Security/Compliance Reports: Does the proposed solution demonstrate the ability to run MDM security/compliance reports using the identified filters? (Y/N)	Required	
15. Classified Data: Does the respondent describe the ability of the proposed solution to access classified data up to the SECRET level via a mobile device? (Y/N)	Optional	
16. PIV/CAC Support: Does the respondent adequately describe how the proposed solution is capable of supporting the use of PIV/CAC cards or PIV-derived credentials per associated NIST standards to support digital signatures, encryption, or access to enterprise resources? (Y/N)	Optional	

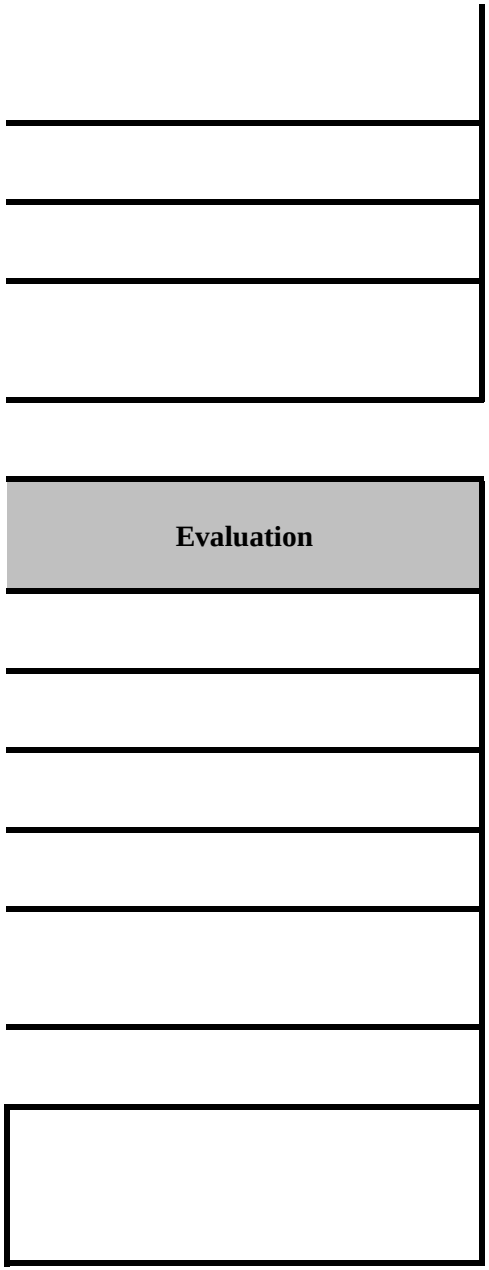
17. Biometric Support: Does the respondent demonstrate the ability for the proposed solution to offer biometric support per associated NIST standards such as fingerprint or face recognition? (Y/N)	Optional	
18. Network Monitoring: Does the respondent demonstrate the basic diagnostic functions related to monitoring device network quality and performance?	Optional	

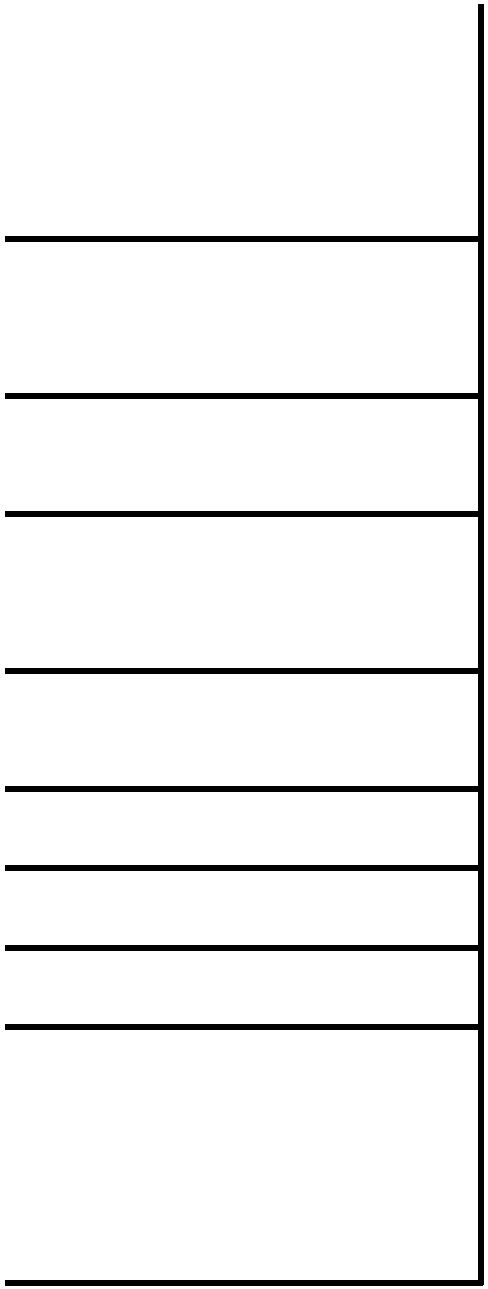
Task 4 – Provide Mobile Application Management

MAM Requirements & Respondent Capabilities/Experience	**All Required**	**RFTC Section 2 or other Reference**
1. Application Deployment: Does the proposed solution demonstrate the ability to support the 5 controls and capabilities identified for application deployment? (Y/N)	Required	
2. Mobile Application Store: Does the proposed solution include a Mobile Application Store that allows users to select private enterprise applications for installation on managed devices, integrated into the Managed Mobility MDM portal, which allows application provisioning by group policy and mandatory application deployment? (Y/N)	Required	
3. Mutual Authentication: Does the proposed solution demonstrate the ability for applications to mutually authenticate to ensure the communications channel is not intercepted? (Y/N)	Required	
4. Application Installation Control: Does the proposed solution demonstrate the solution's process to support relevant authorizations and approvals (including change tracking) to control downloading of authorized and unauthorized applications and help ensure user compliance, including the ability to monitor application usage? (Y/N)	Required	
5. Blacklisting/Whitelisting: Does the proposed solution demonstrate the capability, managed through user and group policies, to block and/or remove specified applications (blacklisting), and permit or force the installation of specified applications (whitelisting)? (Y/N)	Required	
6. Application Environment Requirements: Does the proposed solution demonstrate the capability to detect and enforce device environment conditions such as those listed or enact required policy enforcement rules if device environment conditions cannot be enforced? (Y/N)	Required	
7. Application Signing: Does the proposed solution support requiring digital signatures for application installation? (Y/N)	Optional	
8. Third-Party Application mutual Authentication: Does the proposed solution offer the ability to provide third-party applications with mutual authentication and secure communications through wrappers, binary patching, etc…? (Y/N)	Optional	

Evaluation


Evaluation


Evaluation



Evaluation

Practical Guide to Cloud Service Level Agreements
Version 1.0

April 10, 2012

Contents

Acknowledgements

The *Practical Guide to Cloud Service Level Agreements* is a collaborative effort that brings together diverse customer-focused experiences and perspectives into a single guide for IT and business leaders who are considering cloud adoption. The following participants have provided their expertise and time to this effort.

Workgroup Leaders

John Meegan (IBM) – Lead Technical Editor; Introduction and Keys to Success Section Leader
Gurpreet Singh (Ekartha) – Current SLA Landscape and Disaster Recovery Section Leader
Steven Woodward (Cloud Perspectives) – Roles & Responsibilities; Performance Objectives Leader
Salvatore Venticinque (Second University of Naples) – Service & Deployment Model Section Leader
Massimiliano Rak (Second University of Naples) – Service & Deployment Model Section Leader
David Harris (Boeing) – Business Policies Section Leader
Gerry Murray (Fort Technologies) – Business Policies Section Leader
Beniamino Di Martino (Second University of Naples) – Business Policies Section Leader
Yves Le Roux (CA Technologies) – Security and Privacy Section Leader
John McDonald (CloudOne Corporation) – Service Management Section Leader
Ryan Kean (The Kroger Co.) – Service Failure Management Section Leader
Marlon Edwards (Hoboken Consulting Group, LLC) – Disaster Recovery Section Leader
Dave Russell (IBM) – Management Process Section Leader
George Malekkos (Powersoft Computer Solutions Ltd) – Exit Process Section Leader

Extended Workgroup Members

The workgroup leaders wish to recognize the following individuals for their outstanding efforts to provide content, share their expertise and ensure completeness of the *Practical Guide to Service Level Agreements*: Amy Wohl (Wohl Associates), Asher Bond (Elastic Provisioner, Inc.), Claude Baudoin (cebe IT & KM), Christopher Ferris (IBM), Melvin Greer (Lockheed Martin), Richard Miga (Synergistic Solutions), Thomas Somers (IBM).

Additional Reviewers

The following reviewers provided feedback on the *Practical Guide to Cloud Service Level Agreements*: Jenny Huang (AT&T), Karen Caraway (The MITRE Corporation), Kenneth Dilbeck (TMForum), Roopali Thapar (IBM), Tobias Kunze (Red Hat).

Introduction

This document is an extension of the *Practical Guide to Cloud Computing* white paper that was delivered by the Cloud Standards Customer Council (CSCC) in October, 2011.

The aim of this guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers as they analyze and consider service level agreements (SLA) from different cloud service providers. The paper will give guidance to decision makers on what to expect and what to be aware of as they evaluate SLAs from their cloud computing providers. A checklist of key criteria for evaluating and comparing SLAs from different providers will be included. Additionally, this paper will highlight the role that standards play to improve interoperability and comparability across different cloud providers, and identify areas where future standardization could be effective.

SLAs are important to clearly set expectations for service between the cloud consumer (buyer) and the cloud provider (seller). Each cloud entity engaged by the enterprise should have a cloud SLA defined, including: cloud provider, cloud carrier, cloud broker and even cloud auditor. Consideration must also be given to the different models of service delivery: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS)) as each model brings different requirements. This paper focuses primarily on the SLA details between the cloud consumer and cloud provider, and focuses on the requirements that are common across the various service models (emphasis is given to the IaaS service model since SLAs are more advanced in this area).

The *Practical Guide to Cloud Service Level Agreements* contains a set of guidelines and strategies to help decision makers in all major activities related to cloud SLAs.

The section entitled "Current SLA Landscape" explains the dynamics that currently exists between consumers and providers in the SLA space and the impact that company size has on the power to negotiate terms. This section also highlights the nuances of SLA development for different service models.

The section entitled "Guide for Evaluating Cloud Service Levels Agreements" is the heart of the guide. It provides a prescriptive series of steps that cloud consumers should take to evaluate cloud SLAs with the goal of comparing cloud service providers or negotiating terms with a provider. It provides guidance for the business and service level objectives of the SLA, highlighting what to be aware of and how to compare service levels across different cloud providers. This section takes into account the realities of today's cloud computing ecosystem and postulates how it is likely evolve in the future, including the important role that standards will play to improve interoperability and consistency across providers.

Current SLA Landscape

The Service Level Agreement (SLA) serves as a means of formally documenting the service(s), performance expectations, responsibilities and limits between cloud service providers and their users. A typical SLA describes levels of service using various attributes such as: availability, serviceability,

performance, operations, billing, and penalties associated with violations of such attributes. Well-designed SLAs can significantly contribute to reducing causes of potential conflict and can facilitate issue resolution before a dispute materializes.

To guarantee an agreed service level, service providers must be capable of measuring and monitoring relevant metrics. But often there is a gap between correlating the metrics collected and monitored by service providers to higher-level functional guarantees which are of interest to consumers. This problem is quite challenging and development of SLAs by service providers has to take this into account. This is typical for all types of cloud services and is acute for SaaS providers which offer applications at higher levels of functionality. This is among the many reasons why SLAs for SaaS applications usually lack stringent service level guarantees. A vast majority of SaaS and PaaS providers simply offer no SLAs, although they strive to develop internal operations that contribute to increased reliability.

The situation for IaaS is better than SaaS and PaaS, but most public cloud infrastructure services are available only through non-negotiable standard contracts. They strictly limit the provider's liability and the remedies do not provide significant benefit to consumers in case of service disruptions. Furthermore, most IaaS providers put the burden of SLA violation notification and credit request on their customers. Since a vast majority of the users of IaaS public clouds are small and medium businesses (SMB), the pressure on cloud providers to offer stringent SLAs is minimal.

In today's nascent cloud services industry, SLAs provided by cloud vendors are increasingly being viewed by consumers as unsatisfactory forms of protection that weigh heavily in the provider's favor. Disputes often arise over the structure of the agreements, monitoring of performance, and service unavailability. The reasons for this are numerous and cover both the challenges faced by cloud providers, and the lack of market power by consumers to potentially seek more stringent agreements.

Recent cases of cloud service outages highlight the dilemma for cloud consumers. In some cases, the SLAs offered by providers were loose enough to ensure that service providers were not violating the terms of the SLA despite a serious outage in mission critical areas of the service. In such cases, cloud consumers had no options to seek adequate penalties despite significant adverse effects. Cloud providers are taking account of such problems and are beginning to offer different service options that shield customers from such risks.

In general, the larger the customer deployment, which translates to higher subscription and upfront fees, the more power customers exert in negotiating stringent SLAs. Even in the case of SaaS providers, large customers are successful in negotiating a stronger agreement, where none may be offered to SMB customers. This does point to the trend that as cloud deployments proliferate to larger enterprise customers, the demand for stronger SLAs will intensify. As competition increases at all levels, better SLAs will inevitably become a competitive factor. At that time, large enterprises and SMBs, alike, will be able to choose based on more flexible and more favorable SLA terms and, in general, these terms will improve.

Guide for Evaluating Cloud Service Level Agreements

Before evaluating any cloud SLA, consumers must first develop a strong business case and strategy for their cloud computing environment. This includes identifying specific services that will be deployed in the cloud along with a clear understanding of the criticalness of these services to the business. A check on the exit clauses of current hosted services contracts is also important. Only after this strategic analysis has been completed can the consumer effectively evaluate and compare SLAs from different providers.

With the cloud business case and strategy as a prerequisite, this section provides a prescriptive series of steps that should be taken by cloud consumers to evaluate cloud SLAs with the goal of comparing cloud service providers or negotiating terms with a provider. The following steps are discussed in detail:

1. Understand roles and responsibilities
2. Evaluate business level policies
3. Understand service and deployment model differences
4. Identify critical performance objectives
5. Evaluate security and privacy requirements
6. Identify service management requirements
7. Prepare for service failure management
8. Understand the disaster recovery plan
9. Define an effective management process
10. Understand the exit process

Requirements and best practices are highlighted for each step. In addition, each step takes into account the realities of today's cloud computing landscape and postulates how this space is likely to evolve in the future, including the important role that standards will play to improve interoperability and comparability across providers.

Step 1: Understand Roles & Responsibilities

In order for consumers to understand specific roles and responsibilities explicitly or implicitly stated in a cloud SLA, it is important that they are aware of the various actors that can potentially participate in a cloud computing environment. The National Institute of Standards and Technology (NIST) Reference Architecture[1] identifies 5 unique cloud actors:

- *Cloud Consumer*. The person or organization that maintains a business relationship with, and uses service from, cloud providers.
- *Cloud Provider*. The person, organization or entity responsible for making a service available to cloud consumers.
- *Cloud Carrier*. The intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.
- *Cloud Broker*. An organization that manages the use, performance and delivery of cloud services, and negotiates relationships between cloud providers and cloud consumers.
- *Cloud Auditor*. A party that can conduct independent assessments of cloud services, information system operations, performance and security of the cloud implementation.

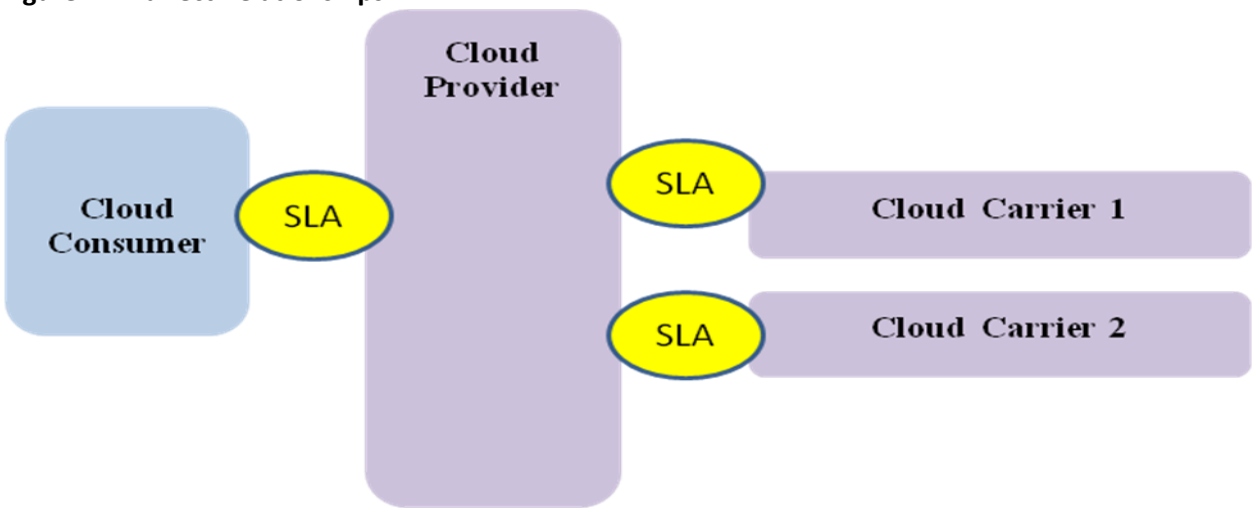
[1] Refer to http://www.nist.gov/itl/cloud/refarch.cfm for more information on the NIST Reference Architecture.

The use of the term “broker” varies significantly and should be clarified with the various stakeholders, especially in context of a cloud SLA. An entity may provide broker services and functionality, but as a legal organizational entity not be recognized as a cloud broker. For example, an entity may perform research and negotiate on behalf of a consumer, but the actual SLA and contract terms are between the cloud consumer and cloud provider. The distinction of acting “broker like” vs. being an actual “broker” will evolve as the cloud computing industry matures and terminologies become more consistent. Due to these complexities this paper does not address all the SLA considerations for cloud brokering.

Consumers need to recognize the activities and responsibilities of each cloud actor that is engaged in delivering their cloud environment, and precisely define requirements and desired service levels for each actor. This paper focuses primarily on the cloud consumer/cloud provider SLA, although other SLAs may be addressed in a particular context.

In some cases, the consumer/provider relationship will indirectly include additional actors. Figure 1 below illustrates an environment where a cloud provider has established a SLA with two cloud carriers to establish service levels for communication and transport. In addition to cloud provider expectations, the consumer/provider SLA in this example may also include specific carrier and transport expectations. In this case, the cloud provider is also acting as a “broker” for the other two cloud carriers.

Figure 1. Indirect Relationships



Each cloud SLA will be unique based upon the consumers’ requirements and the cloud ecosystem under consideration. SLAs can contain various expectations between the actors and are not limited to quantitative measures, but can include other qualitative aspects such as alignment with standards and data protection. It is strongly recommended that cloud consumers gain a solid understanding of the

spectrum of SLAs that currently exist for cloud providers (and other actors as appropriate) in order to compare providers and assess tradeoffs between cost and service levels.[2]

The following sections, which cover the cloud SLA evaluation steps in detail, will each elaborate on the expected responsibilities between consumer and provider for both business level and service level objectives. In order to make sound business decisions, it is important that consumers understand what to expect from their cloud provider. This, in turn, will help them define their own responsibilities and help them assess the true cost of moving to the cloud.

Step 2: Evaluate Business Level Policies

Consumers must consider key policy issues when reviewing a cloud SLA since there are interdependencies between the policies expressed in the SLA and the business strategy and policies developed in other aspects of the business. The data policies of the cloud provider, as expressed in the SLA, are perhaps the most critical business level policies that should be carefully evaluated.

The duty of care a cloud provider has to its clients and their data is partly governed by the data protection legislation applicable in the user's local jurisdiction and also in those jurisdictions in which its data may reside or made available. Consumers should carefully consider these legal requirements and how the SLA their provider(s) offers deals with issues such as movement of data to offer multisite redundancy across several jurisdictions.

Table 1 highlights the critical data policies that need to be considered and included in the cloud SLA.

Table 1. SLA data policies

Data Policy	Description / Guidance
Data Preservation	• Timely and efficient capturing and preservation of data is critical to maintaining the organizational memory of a business or the general user. • It enables the data controller to address operational, strategic and litigious situations from an informed perspective. • Cloud users should ensure the service supports their data preservation strategy that includes sources, scheduling, backup, restore, integrity checks, etc.
Data Redundancy	• Users should ensure they have an appropriate data preservation strategy that addresses redundancy within the system. • This should be complemented by the SLA their cloud provider offers and can be tested to demonstrate service availability. • The consumer should be concerned as to the protections offered or omitted by the

[2] Refer to the Queen Mary School of Law Legal Studies Research Paper titled *Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services* at http://ssrn.com/abstract=1662374 for a comprehensive analysis of leading cloud service providers.

	service provider.
Data Location	• SLAs which cover single and multi-jurisdiction scenarios are challenging. • Users should carefully consider as part of their data management strategy how the SLA will complement where their data will reside, where it is processed, and how this meets regulatory requirements. • For example, can the provider truly deliver a sound technical solution when data spans several jurisdictions? Can the user trust that the data will be located where the provider commits it will be?
Verification of new data location	• Clients should ensure that when a provider elects to provide its service from another location it will be required to notify its clients of the new location and provide a means for the client to independently verify where the data will be relocated. • Preferably the provider should be required to obtain the permission of the client to relocate the data before moving to a new location.
Data Seizure	• Legal powers enable law enforcement and other government agencies to seize data under certain circumstances. • Consumers should also ensure there are arrangements in place to make a user's data available in the event that their SLA provider goes out of business and the data center provider locks access to its systems pending payment of the outstanding account.
Data Privacy	• It is a requirement to conduct business in compliance with applicable laws on data privacy protection and data security. • The declared data privacy policy from the provider should be included in the SLA. • Examples of privacy terms that should be addressed in the SLA include the data sets gathered, data retention policies, how the data is communicated, how personal data is stored and used, etc. • Refer to the Privacy section on page 24 for more information.

In addition to data policies, there are a number of other business level policies expressed in the cloud SLA that require careful evaluation. All of these policies will impact and influence the consumer's cloud strategy and business case. In many cases, these policies, as defined in the cloud SLA, are non-negotiable and are similar across different cloud providers. However, there will be instances where some of these policies can be negotiated and/or some of these policies differ sufficiently across different cloud providers to warrant careful consideration from consumers.

Table 2 below highlights the critical business level policies that need to be considered and addressed in the cloud SLA.

Table 2. SLA business level policies

Policy	Description / Guidance

Guarantees	• SLA guarantees should be defined, objective and measurable with an appropriate scaled penalty matrix which complements the impact of non-performance by the provider.[3] The SLA should clarify:
	  ○ What constitutes excused or excluded performance
	  ○ Escalation procedures
	  ○ How service-level bonuses and penalties are administered
	  ○ Remedy circumstances and mechanisms
	• Such guarantees should include an availability measurement expressed as a percentage, e.g. 99.999%, which denotes the amount of time the service is guaranteed to be working.

Acceptable Use Policy	• Given the dislocated relationship that can exist between the provider and the consumer (the provider may not know the final end user of its service), the acceptable use policy will clearly describe how the consumer may use its service and the agreement generally will describe what actions the provider may take in the event of a breach. • In today's cloud environment, this policy is typically non-negotiable and the terms generally favor the cloud provider.
List of Services Not Covered	• The SLA will state under what conditions and with which described services the consumer is supported. The SLA may also state what is excluded and what constitutes illegal use. • Consumers should look for explicitly stated exceptions and understand why the provider has excluded them.
Excess Usage	• Providers operate business models to drive revenue. Consumers may find that usage above their contracted thresholds may incur 'premium' rates which can be punitive and disrupt their budgets. • Consumers should correctly size their usage requirements, reduce the opportunity for usage creep and consider and understand the 'what-ifs' of breach of their usage thresholds. • The cloud is a great tool to vary the size of the resource pool your business buys but, as in any business model, buy only what you need and avoid excess usage charges.

[3] Guarantees including measurable metrics will be covered in greater detail in the sections that follow.

Activation	• Providers will delineate a time at which the service becomes active and the SLA commences operation. This time stamp can then be used to measure time and if an outage occurs may be used to establish the start of a penalty incurring 'event'. • Examples of activation include the time at which the consumer checks the 'accept terms and conditions' box or when the consumer acknowledges the secure URL providing login credentials to their new cloud service. • From a SLA compliance perspective, it is important for consumers to understand the trigger points under the SLA so they can independently measure 'event' timing. • It is also important to understand when the agreement is in operation as both the provider and the consumer have responsibilities such as Fair Use and Legal Use.
Payment and penalty models	• The SLA should clarify when/how payment is to be made. Provider payment models vary. Monthly recurring or "pay as you use" models are typical. • Associated with these payment models are credit terms which may require advanced payment or payment every 30 days. "Just in time" service providers are sensitive to poor credit control and are likely to be more diligent in suspending service. • Equally, the consumer needs to be diligent in obtaining service credit payments for outages.
Governance / Versioning	• Providers' services evolve. New features may be added, others will go out of warranty, and some may persist indefinitely. Where the assumptions or conditions under which the SLA was initially accepted are changed, the consumer should review the impact on their specific situation. • A good provider will maintain a proactive policy of advising consumers of changes to their SLA and practice version control. • Consumers should ensure that there is a mechanism in place to be informed of changes and, if not, amend their contract to put the onus on the provider to contact them at a designated contact point with updates within a reasonable timeframe.
Renewals	• Renewals are an opportunity to bargain for better rates and relocate to another provider if necessary. • Providers may operate auto renewals which state, for example, this contract will auto renew on its anniversary if the consumer does not give 90 days notice of their intention to cancel. • Consumers should read the terms and conditions for the renewal arrangements, and consider the conditions under which a provider may vary the service terms at renewal. Provider systems are organic as are consumer requirements. More attractive service functionality may be available or more consumer flexibility required.

Transferability

- Consumers should consider the potential for needing to transfer an agreement in the event their business is sold.
- In addition, the provider's business may be sold to a competitor and it may suit the consumer to relocate and discontinue the commercial agreement with the new owner.
- Consumers may operate several accounts with a provider and want to offset account credits between accounts. Is this supported in the provider's contract terms?

Support

- The consumer should ensure they follow the reporting guidelines of the provider to ensure the support terms specified in the SLA are activated.
- An example of a support and escalation matrix is provided below. All three target times in the table are associated with the commencement 'time stamp' of the service or the notification of a service affecting event.

Priority	Description	Target Response Time	Target Update Time	Target Fix Time
P1	Production software unusable/Production cloud servers inaccessible	1 hour, Provider's executive notified of issue	1hr	Immediate work commences and continues until issue resolved or workaround deployed
P2	Partial software functionality unusable/Partial service unavailable	4 hours	1day	2 days, subject to available maintenance slot
P3	Cosmetic issue	1 working day	1 working day	Next software release/service update
P4	Information request	2 working days	2 working days	n/a

Planned Maintenance

- All systems require maintenance. Complex systems may be designed to include sufficient resources such that maintenances can be carried out without affecting the service.
- The SLA may, however, describe 'uptime' as an availability percentage (e.g. 99.90%). This is the equivalent of 8.5 hours downtime per annum. SLAs may state that this does not include 'planned maintenance'. Thus, the provider may have a service outage for 8.5 hours + maintenance time under the SLA and the consumer is not entitled to compensation.

Subcontracted Services

- Providers sometimes include in their SLAs indication that the SLA of an upstream (subcontracted) provider will be passed to the consumer and the only available penalties are those of the upstream provider even though these may be of a lesser quality than the consumer understands when reviewing the SLA of their immediate

	provider. • Equally, the consumer should ensure that the immediate provider SLA is unambiguous in stating that their SLA applies to the complete service and not limited to the immediate provider's component of the overall service.
Licensed Software	• Cloud services may include third party licensed software which is sold on a monthly licensed basis under a service provider license agreement. Such software is updated regularly by its manufacturer. • Providers may opt to pass the responsibility for 'patching' the licensed software over to the consumer once they have started to use the service. This can be preferable to the provider as later releases may negatively affect the consumer's service. • The provider may alternatively 'push' the update in which case the consumer, as specified in the SLA, may require notification of the update. Upon notification, the consumer can issue an 'opt out' option.
Industry Specific Standards	• Regulated industries, like government, financial services, and healthcare, will have specific and usually quite onerous and costly standards which must be addressed in the cloud SLA and implementation. • Consumers who operate in these regulated industries should ensure that the full resources of their legal team are brought to bear on the negotiation of the SLA.
Additional terms for different geographic region or countries	• Consumers should consider the provider's origins and primary market. Detailed refinements to the home market SLA may be required to properly cover consumers who are located in remote markets. • Data protection legislation is one aspect of this. However, consumers should not limit their examination of the agreement to this solely.

Step 3: Understand Service and Deployment Model Differences

Services offered by cloud providers typically fall into one of the three major groups of service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). For each category, there are significant differences in the levels of cloud resource abstraction, service level objectives, and key performance indicators that will potentially be included in a cloud SLA. In addition, the level of clarity varies significantly for each service model. In general, PaaS and SaaS objectives are less precise than IaaS objectives since the variety of solutions and applications offered by providers is much broader for these service models.

Table 3 highlights the different SLA considerations for each of the cloud service models.

Table 3. SLA considerations for Service Models

Service Model	SLA Considerations

IaaS	• Cloud IaaS SLAs are similar to SLAs for network services, hosting, and data center outsourcing. The main issues concern the mapping of high level application requirements on infrastructure services levels.
	• Metrics are well understood across the IaaS abstractions (compute, network, and storage). Consumers should expect to find the following metrics in their cloud SLA.
	  ○ Compute metrics: *availability, outage length, server reboot time*
	  ○ Network metrics: *availability, packet loss, bandwidth, latency, mean/max jitter*
	  ○ Storage metrics: *availability, input/output per second, max restore time, processing time, latency with internal compute resource*
	• Compute metrics usually exclude service levels for compute performance. Consumers are simply guaranteed to have the compute resources for which they paid with technical enforcement at the hypervisor level.
	• Network metrics in a cloud SLA generally cover the cloud provider's data center connectivity to the Internet as a whole, not to any specific provider or consumer.
	• Denial-of-service (DoS) attacks may be explicitly excluded from the SLA even if the provider offers protection via firewalls and intrusion detection systems.
	• There are several standardization efforts within the IaaS space which help describe and manage the services offered at this level.[4] Whenever possible, consumers should ensure the cloud SLA includes provisions requiring their cloud providers to support open standard interfaces, formats and protocols to increase interoperability and portability.

PaaS	• Two main approaches exist for building PaaS solutions: *integrated solutions* and *deploy-based solutions*. When reviewing the PaaS SLA, consumers should consider tradeoffs in flexibility, control, and ease of use to determine which approach best meets their business needs. ○ Integrated solutions, like Google App Engine (GAE)[5], are web accessible development environments which enable developers to build an application using the infrastructure and middleware services supported by the cloud provider. Management of the application and its execution is primarily controlled by the cloud

[4] IaaS standards include: DMTF CIMI (Cloud Infrastructure Management Interface), DMTF OVF (Open Virtualization Format), SNIA CDMI (Cloud Data Management Interface), The Open Group's SOCCI (Service-Oriented Cloud-Computing Infrastructure), OGF OCCI (Open Cloud Computing Interface), the ISO Study Group on Cloud Computing (SGCC), and de-facto industry alignment on IaaS service level objectives, warranties, guarantees, performance metrics, etc.

[5] Refer to http://code.google.com/appengine/ for information on Google App Engine.

	provider. Typically, service developers only have access to a provider-defined set of APIs (Task API in GAE) which offer limited control on the coordination of code execution. ○ Deploy-based solutions enable deployment of middleware on top of resources acquired from an IaaS cloud provider, offering deployment services to the consumers which automate the process of installation and configuration of the middleware.[6] These PaaS solutions offer a rich set of management capability including the ability to automatically change the number of machines assigned to an application, and self-scaling according to the application's usage. • Consumers must distinguish between PaaS development environments and PaaS production environments when reviewing their cloud PaaS SLA. PaaS production environments will typically require more stringent service level objectives than PaaS development environments. • The state of PaaS metrics is currently immature with metrics varying significantly across providers. Standards initiatives are just starting to emerge in this space. In the meantime, consumers are advised to identify the PaaS services that are critical to their business and ensure that their cloud SLAs contain clear and measurable metrics for these services. • Standards that help identify PaaS services offered by cloud providers and standard interfaces for communicating with PaaS providers to provision or manage PaaS environments are also lacking. The lack of standards results in poor portability and interoperability across providers. Standards, like OASIS TOSCA[7], are emerging which will help address this issue. Consumers should ensure their cloud SLA includes support for open standards, as they become available, to reduce vendor lock in.
SaaS	• Given the wide variation of services provided at the SaaS level, it is difficult to provide a comprehensive and representative list of SaaS service level objectives for consumers to look out for in their cloud SLAs. • Consumers should expect general SaaS service level objectives like *monthly cumulative application downtime*, *application response time*, *persistence of consumer information*, and *automatic scalability* to be included in their SLA. • Consumers should ensure that data maintained on the provider's cloud resources be stored using standard formats to ensure data portability in the event that a move to a different provider is required.

[6] Deploy-based solutions are supported by commercial providers like IBM, Oracle and Microsoft as well government sponsored projects like OPTIMIS, CONTRAIL, Cloud4SOA and mOSAIC in Europe.

[7] Refer to http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=tosca for details on TOSCA.

In addition to service models, service deployment terms should be included in a cloud SLA. These terms should clarify to both parties signing the SLA the information required to verify the correctness of deployment actions. Specifically, these terms should identify:

- Deployment model
- Deployment technologies adopted

The deployment model included in the SLA should clearly specify one of the following options: *Private*, *Community*, *Public*, or *Hybrid*. Consumers must be well educated on the characteristics and differences in each of these deployment models since potential value and risk varies significantly.[8]

Table 4 highlights the different SLA considerations across the deployment models.[9]

Table 4. SLA considerations for Deployment Models

Deployment Model	SLA Considerations
Private (On-site)	• SLA considerations for Private (On-site) are similar to those of a traditional enterprise IT SLA. However, given that data center resources may be shared by a larger number of internal users, consumers must ensure that critical service objectives like availability and response time are met via ongoing measurement and tracking.
Private (Outsourced)	• SLA considerations for Private (Outsourced) are similar to Private (On-site) except cloud services are now being provided by an external cloud provider. The fact that IT resources from the provider are dedicated to a single consumer mitigates potential security and availability risks. • Consumers should ensure the cloud SLA specifies security techniques for protecting the provider's perimeter and the communications link with the provider. • Consumers should consider the criticalness of the service being deployed to justify the added expense of this model over the Public model.
Public	• SLA considerations for the Public model are greater than the Private (Outsourced) model since the provider's IT resources are now shared across multiple consumers. • As a result, consumers should carefully review the cloud SLA to understand how the provider addresses the added security, availability, reliability and performance risks introduced by multi-tenancy. • The ability to measure and track specific service level objectives becomes more

[8] Refer to the Practical Guide to Cloud Computing for considerations on selecting a deployment model.

[9] The Community deployment model is not called out explicitly in the table since it is very similar to the Public deployment model.

	important in the Public deployment model. Consumers should also ensure the cloud SLA provides adequate methods and processes for ongoing measurement.
Hybrid	• SLA considerations for the Hybrid model are similar to the Public model with the increased likelihood for unique integration requirements between cloud and enterprise services. As a result, consumers should ensure the cloud SLA adequately covers their service and data integration requirements.

In addition to specifying the deployment model, the SLA should clarify how a service is made available to service users on a given cloud provider, for example:

- A web application is deployed on an application server as a WAR file[10] (the application server enables WAR uploading).
- A grid application is deployed on a grid container as a GAR (Grid Archive) file.
- A virtual machine is deployed on an IaaS provider as a virtual machine disk image that may be represented in one of many different formats. Adoption and support for standards like the Distributed Management Task Force (DMTF) Open Virtualization Format[11] (OVF) is recommended.

When SLAs are signed, a clear description of the technologies involved in the deployment of services may be specified (for example, WAR, GAR, OVF, etc.). Note that there is a close relationship between deployment technologies and the kind of services being offered.

Step 4: Identify Critical Performance Objectives

Performance goals within the context of cloud computing are directly related to efficiency and accuracy of service delivery. Performance considerations often include: availability, response time, transaction rate, processing speed, but can include many other performance and system quality perspectives.[12] Consumers must decide which measures are most critical to their specific cloud environments and ensure these measures are included in their SLA.

Performance statements that are important to the cloud consumer should be measureable and auditable, and documented in the SLA providing a comfort level to both parties. Performance considerations are dependent on the supported service model (IaaS, PaaS and SaaS) and the type of services provided within that model, for example, network, storage and computing services for IaaS.

[10] Refer to http://java.sun.com/j2ee/tutorial/1_3-fcs/doc/WCC3.html for more information on the WAR (Web application ARchive) file.

[11] Refer to http://www.dmtf.org/standards/ovf for more details.

[12] System quality measures that could be included in service performance include accuracy, portability, interoperability, standards compliance, reliability, scalability, agility, fault tolerance, serviceability, usability, durability, etc.

Of course, in order for performance objectives to be meaningful, measurement is a critical consideration where clarity and consistency are very important, if not crucial, to gain trust in the cloud. Measuring without context is useless and performance metrics are no different. It must be clear how the metric will be used and what decisions will be made from the metrics, continually evaluating and aligning with specific goals and objectives.

This section will focus on two performance metrics: *availability* and *response time*. The intention is to provide a basic framework to help identify and define cloud metrics that will be meaningful and consistent. This section is not meant to be exhaustive - it does not contain all the potential metrics and possible definitions. Many of the measurement and metric definitions may already be supported by your cloud provider; therefore the specific interpretation of the term in context of a specific solution is critical. Some calibration may be required between existing captured measures and those specifically requested as part of the SLA.

Industry standard measures with applicable definitions should be used to improve consistency, enabling meaningful comparative and trend analysis. For instance, IEEE also has good measurement definitions and categorizations for activities such as maintenance.[13] Other organizations and private benchmarks exist. The key is to always calibrate values to get an "apple to apples" comparison to an appropriate level of accuracy.

To be effective, a performance metric must be clearly defined in the SLA and understood by both parties. Here are the generally accepted definitions for the two metrics of interest:

- *Availability*. Percentage of uptime for a service in a given observation period.
- *Response time*. Elapsed time from when a service is invoked to when it is completed including delays (typically measured in milliseconds).

Table 5 describes three different example scenarios (network availability, storage availability, and service response time) and the specific performance information required for each.

Table 5. Availability and Response Time metrics examples

	Network Availability (example)	Storage Availability (example)	Service Response Time (example)
Metric Name in SLA	Network Percentage Available Critical Business Hours	Storage Percentage Available	Service XXX Response Time in a Given Hour; Service YYY Response Time in a Given Hour.

[13] Other standard measures include the International Software Measurement Association – International Function Point Users Group that retains several software measurement guidelines (such as ISO/IEC 20926) that are used for benchmarking and works closely with the International Software Benchmarking Standards Group.

Constraints	Critical time is business hours 12AM GMT to 12PM GMT Monday thru Friday	No constraints	Response times will only be evaluatd for services XXX and YYY which are PaaS reuseable services that will be invloked by our applications.
Collection Method	Machine	Machine	Machine
Collection Description	Using the DMTF, OGF[14], or other standard to consistently collect the measures.	Using the DMTF, OGF, or other standard to consistently collect the measures.	Using the DMTF, OGF, or other standard to consistently collect the measures.
Frequency of Collection	The network is "pinged" every one minute.	Specific storage services (read and update) are randomly "pinged" every one minute.	For each XXX and YYY service invoked, the response time will be collected.
Other Information	Considered 60 seconds of uptime for each successful "ping".	Considered 60 seconds of uptime for each successful "ping".	Each service will be reported separately. Hourly averages will be calculated.
Clarification	No reference to quality or availability of specific service. This is exclusively a measure of network availability.	No reference to quality or availability of specific service. This is exclusively a measure of storage availability.	No idividual services reporting is needed (for example, listing of all services that exceeded SLA agreed response time).
Usage 1 in SLA	Network availability will be 99.5% between 12AM GMT to 12PM GMT Monday thru Friday.	Storage availability will be 99.9%.	Response time for XXX service must be less than 500 MS, YYY service less than 200 MS.
Usage 2 in SLA	For any day when network availability is less than 99.5%, a 20% discount will be applied for the entire day network charges.	For any day when stroage availability is less than 99.9%, a 50% discount will be applied for the entire day storage charges.	If in any given hour the response times as stated are not met, all services of that type during that hour will be processed at no charge.

Cloud resources, both hardware and facilities, should also be considered when assessing critical performance objectives for cloud SLAs. Hardware includes: compute (CPU and memory), networks (routers, firewalls, switches, network links, and interfaces), storage components (hard disks), and any other physical computing infrastructure elements. Facilities include: heating, ventilation and air conditioning (HVAC), power, communications, and other aspects of the physical plant.

Resources need to be clearly stated in the SLA to clarify scope, constraints and expectations for the cloud computing services of interest. To be successful, higher level business objectives and goals need to be understood such that critical resource metrics can be identified that address facility and hardware

[14] Refer to http://www.gridforum.org/ for more information on the Open Grid Forum.

expectations. Some metrics may not be technical, but can include measures such as watts of power usage, cubic feet of network cabinets, or even revenue dollars from real estate sold. For example, one frequent objective for the IaaS service model is to reduce power usage, or perhaps reduce the footprint size of the data center.

In summary, when considering performance metrics in a cloud SLA, it is recommended that consumers:

- Understand the business level performance objectives for the cloud opportunity (for example, reduce cost and time to market per unit of software functionality).
- Identify the set of metrics that are critical to achieving and managing the business level performance objectives.
- Ensure these metrics are defined at the right level of granularity that can be monitored on a continuous basis cost effectively.
- Identify standards to provide consistency for cloud metrics in areas such as metric definitions and methods of collection.
- Analyze and leverage the metrics on an ongoing basis as a tool for influencing business decisions.

Step 5: Evaluate Security[15] and Privacy Requirements

Security controls in cloud computing are, for the most part, no different than security controls in any IT environment. However, because of the cloud service models employed, the operational models, and the technologies used to enable cloud services, cloud computing may present different risks to an organization than traditional IT solutions. At a basic level, assets supported by the cloud fall into two general categories:

- Data
- Applications/Functions/Processes

Information is either being moved into the cloud or applications are being executed in the cloud (from partial functions all the way up to full applications).

A critical initial step for ensuring sufficient cloud security is establishing a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity of enterprise data. This scheme should include details about data ownership, definition of appropriate security levels and protection controls, and a brief description of data retention and destruction requirements. The classification scheme should be used as the basis for applying controls such as access controls, archiving or encryption.

[15] The security part of this section is based on the Cloud Security Alliance "Security Guidance for Critical Areas of Focus in Cloud Computing, V3.0" and quotes portions of this document. The document is available at http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf.

In order to determine which level of security is required for a specific asset, a rough assessment of an asset's sensitivity and importance is required. For each asset, the following questions should be asked:

1. How would the business be harmed if the asset became publically available and distributed?
2. How would the business be harmed if an employee of our cloud provider accessed the asset?
3. How would the business be harmed if the process or function were manipulated by an outsider?
4. How would the business be harmed if the process or function failed to provide expected results?
5. How would the business be harmed if the information/data were unexpectedly changed?
6. How would the business be harmed if the asset was unavailable for a period of time?

Table 6 below highlights the key steps consumers should take to ensure their cloud SLA sufficiently addresses their unique security requirements.

Table 6. Key security considerations for cloud SLAs

SLA Security Considerations	Strategic Activities

Assess asset sensitivity and application operational security requirements	• An assessment of the confidentiality, integrity, and availability requirements for the asset must be completed.
	• Consumers must address application operational security and availability requirements in response to identified risks and in line with the organization's data classification, information architecture, information security architecture, and risk tolerance.
	• A common challenge organizations face with the cloud is managing data. Many organizations report individuals or business units moving sensitive data to cloud services without the approval or even notification of IT or security.
	• Take steps to detect unapproved data moving to cloud services:
	  ○ Monitor for large internal data migrations with database activity monitoring (DAM) and file activity monitoring (FAM)
	  ○ Monitor for data moving to the cloud with URL filters and data loss prevention
	• Protect data in transit. All sensitive data moving to or within the cloud at the network layer, or at nodes before network transmission should be encrypted, sensitive volumes should be encrypted to limit exposure to snapshots or unapproved administrator access, and sensitive data in object storage should be encrypted, usually with file/folder or client/agent encryption.

Understand Legal/Regulatory Requirements	• Due to potential regulatory, contractual and other jurisdictional issues it is extremely important to understand both the logical and physical locations of data.
Establish and track security	• Metrics and standards for measuring performance and effectiveness of information security management should be established prior to moving into

metrics	the cloud. • At a minimum, organizations should understand and document their current metrics and how they will change when operations are moved into the cloud and where a provider may use different (potentially incompatible) metrics. ○ Refer to the following resources for specific information on security metrics: ISO 27004:2009[16], NIST Special Publication (SP) 800-55 Rev.1, Performance Measurement Guide for Information Security[17], and CIS Consensus Security Metrics v1.1.0[18]

Assess and compare cloud providers' security capabilities	• Determine if the provider's guarantees adequately address your security requirements.[19]
	
	• The provider's security governance processes and capabilities should be assessed for sufficiency, maturity, and consistency with the user's information security management processes.
	
	• The provider's information security controls should be demonstrably risk-based and clearly support these management processes.
	
	• Where a provider cannot demonstrate comprehensive and effective risk management processes in association with its services, customers should carefully evaluate use of the provider as well as the user's own abilities to compensate for the potential risk management gaps.
	
	• Assess the cloud provider's level of security and its maturity:
	  ○ If compliance to a normative standard (e.g. ISO 27001) is given:
	  ▪ Verify the compliance certificate and its validity
	  ▪ Look for verifiable evidence of resource allocation, such as budget and manpower to sustain the compliance program
	  ○ Verify internal audit reports and evidence of remedial actions for the findings

Audit cloud provider's security SLA compliance	• A right to audit clause in a cloud SLA gives customers the ability to audit the cloud provider, which supports traceability and transparency in the frequently evolving environments of cloud computing and regulation. • Use a normative specification in the right to audit clause to ensure mutual

[16] See http://www.iso.org/iso/catalogue_detail.htm?csnumber=42106.

[17] See http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf.

[18] See http://benchmarks.cisecurity.org/en-us/?route=downloads.show.single.metrics.110.

[19] The Cloud Security Alliance Consensus Assessments Initiative Questionnaire (CAIQ) provides a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider. Refer to http://cloudsecurityalliance.org/research/cai/ for details.

understanding of expectations.

- In time, this right should be supplanted by third-party certifications (e.g., driven by ISO/IEC 27001/27017[20]).

Some of the security risks associated with cloud computing are unique, partly due to an extended data centric chain of custody, and it is in this context that the business continuity, disaster recovery, and traditional security environments of a cloud service provider need to be assessed thoroughly and in reference to industry standards. Consumers should ensure that the provider is compliant with global security standards like ISO 27001 ISMS[21] or other industry-standards such as TOGAF[22], SABSA[23], ITIL[24], COSO[25], or COBIT[26].

Providers should notify consumers about the occurrence of any breach of its system, regardless of the parties or data directly impacted. The provider should include specific pertinent information in the notification, stop the data breach as quickly as possible, restore secure access to the service as soon as possible, apply best-practice forensics in investigating the circumstances and causes of the breach, and make long-term infrastructure changes to correct the root causes of the breach to ensure that it does not recur. Due to the high financial and reputational costs resulting from a breach, consumers may want the provider to indemnify them if the breach was their fault.

Privacy

In many countries throughout the world, numerous laws, regulations, and other mandates require public and private organizations to protect the privacy of personal data and the security of information and computer systems. Table 7 provides an overview of the worldwide privacy regulations that currently exist.

[20] Visit http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43757 for working draft of ISO 27001, reference 3 ISO/IEC 27017 Security in cloud computing.

[21] Visit http://www.iso.org/iso/catalogue_detail?csnumber=42103 for details.

[22] TOGAF® is an Open Group Standard see http://www.opengroup.org/togaf/.

[23] Visit http://www.sabsa.org/ for information on the Sherwood Applied Business Security Architecture.

[24] Visit http://www.itil-officialsite.com/ for information on the Information Technology Infrastructure Library.

[25] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) published an Enterprise Risk Management — Integrated Framework (2004): see http://www.coso.org/ for details.

[26] COBIT is an IT governance framework and supporting toolset - see http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx for details.

Table 7. Worldwide privacy regulations

Region	Regulation
Asia Pacific region, Japan, Australia, New Zealand, and others	• These regions have adopted data protection laws that require the data controller to adopt reasonable technical, physical, and administrative measures in order to protect personal data from loss, misuse, or alteration, based on the Privacy and Security Guidelines of the Organization for Economic Cooperation and Development (OECD)[27], and the Asia Pacific Economic Cooperation's (APEC) Privacy Framework.[28]
Japan	• In Japan, the Personal Information Protection Act[29] requires the private sectors to protect personal information and data securely. In the healthcare industry, profession-specific laws, such as the Medical Practitioners' Law[30], the Law on Public Health Nurses, Midwives and Nurses[31], and the Dentist Law[32], require registered health professionals to protect the confidentiality of patient information.
Europe, Africa, Middle East	• The European Economic Area (EEA) 30 Member States have enacted data protection laws that follow the principles set forth in the 1995 European Union (EU) Data Protection Directive and the 2002 ePrivacy Directive (as amended in 2009). These laws include a security component, and the obligation to provide adequate security must be passed down to subcontractors. • Other countries that have close ties with the EEA, such as Morocco and Tunisia in Africa, Israel and Dubai in the Middle East have also adopted similar laws that follow the same principles.
Americas	• North, Central, and South American countries are also adopting data protection laws at a rapid pace. Each of these laws includes a security requirement that

[27] The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were adopted on 23 September 1980, see http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html.

[28] In 2004, the APEC Privacy Framework was endorsed by APEC Ministers for more details see http://www.worldlii.org/int/other/PrivLRes/2005/4.html.

[29] Act on the Protection of Personal Information (Act No. 57 of 2003) – see http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf for details.

[30] Medical Practitioners' Law (Law No. 201 of July 30, 1948) - http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

[31] Law on Public Health Nurses, Midwives and Nurses (Law No. 203 of July 30, 1948) - http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf

[32] Dentists Law (Law No. 202 of July 30, 1948) - see http://jalii.law.nagoya-u.ac.jp/official_gazette/pdf/19480730f_eb.00000.010.010_0010.0010.0_a.127600.01217100.pdf for details.

	places on the data custodian the burden of ensuring the protection and security of personal data wherever the data are located, and especially when transferring to a third party. • In addition to the data protection laws of Canada[33] and Argentina[34] which have been in existence for several years, Colombia, Mexico, Uruguay, and Peru have recently passed data protection laws that are inspired mainly from the European model and may include references to the APEC Privacy Framework as well.
United States	• There is no single privacy law in the Unites States. A range of government agency and industry sector laws impose privacy obligations in specific circumstances. There are numerous gaps and overlaps in coverage. • Current industry sector privacy laws include: o The Federal Trade Commission Act [35] which prohibits unfair or deceptive practices - this requirement has been applied to company privacy policies in several prominent cases. o The Electronic Communications Privacy Act of 1986[36] which protects consumers against interception of their electronic communication (with numerous exceptions). o The Health Insurance Portability and Accountability Act (HIPAA)[37] which contains privacy rules applying to certain categories of health and medical research data. o The Fair Credit Reporting Act[38] includes privacy rules for credit reporting and consumer reports. o The Gramm-Leach-Bliley Act (GLBA)[39] govern the collection,

[33] Personal Information Protection and Electronic Documents Act (PIPEDA) - see http://laws-lois.justice.gc.ca/eng/acts/P-8.6/ for details.

[34] Law for the Protection of Personal Data (LPDP), Law No. 25.326 - see http://www.protecciondedatos.com.ar/law25326.htm for details.

[35] See http://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I for details.

[36] See http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc18.wais&start=3919965&SIZE=21304&TYPE=TEXT for details.

[37] The final HIPPA regulation and modifications can be found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf.

[38] See http://www.ftc.gov/os/statutes/fcradoc.pdf for details.

	disclosure, and protection of consumers' nonpublic personal information for financial institutions ○ These laws hold organizations responsible for the acts of their subcontractors. For example, the security and privacy rules under GLBA or HIPAA require that organizations compel their subcontractors, in written contracts, to use reasonable security measures and comply with data privacy provisions. • Government agencies, such as the Federal Trade Commission (FTC) or the State Attorneys General have consistently held organizations liable for the activities of their subcontractors.
Worldwide	• The Payment Card Industry (PCI) Data Security Standards (DSS)[40], which apply to credit card data anywhere in the world, including data processed by subcontractors has similar requirements.

When data is transferred to a cloud, the responsibility for protecting and securing the data typically remains with the collector or custodian of that data, even if in some circumstances, this responsibility may be shared with others. When it relies on a third party to host or process its data, the custodian of the data remains liable for any loss, damage, or misuse of the data. It is prudent, and may be legally required, that the data custodian and the cloud provider enter into a written (legal) agreement that clearly defines the roles, expectations of the parties, and allocates between them the many responsibilities that are attached to the data at stake.

If privacy issues are not adequately addressed in the SLA, the cloud consumer should consider alternate means of achieving their goals including seeking a different provider, or not sending sensitive data to the cloud. For example, if the consumer wishes to send HIPAA-covered information to the cloud, the consumer will need to find a cloud service provider that will sign a HIPAA business associate agreement or else not send that data to the cloud.

Preservation of information, included in some privacy regulations, can require that large volumes of data be retained for extended periods. What are the ramifications of this under the cloud SLA? What happens if the preservation requirements outlast the terms of the SLA? If the consumer preserves the data in place; who pays for the extended storage and at what cost? Does the consumer have the storage capacity under its SLA? Can the consumer effectively download the data in a forensically sound manner

[39] See http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html for details.

[40] PCI DSS provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents. See https://www.pcisecuritystandards.org/security_standards/ for details.

so it can preserve it off-line or near-line? These are some of the privacy related questions that need to be addressed in the cloud SLA.

Identity protection is another area that may need to be addressed in the cloud SLA. Almost all cloud-based storage systems require some authentication of participants (cloud consumer and/or cloud provider) to establish trust relations, either for only one endpoint of communication or for both. Although cryptographic certificates can offer sufficient security for many of these purposes, they do not typically cater to privacy because they are bound to the identity of a real person (cloud consumer). Any usage of such a certificate exposes the identity of the holder to the party requesting authentication. There are many scenarios (e.g., storage of electronic health records) where the use of such certificates unnecessarily reveals the identity of their holder.

Over the past 10-15 years, a number of technologies (e.g. Anonymous Credentials[41])have been developed to build systems in a way that they can be trusted, like normal cryptographic certificates, while at the same time protecting the privacy of their holder (i.e., hiding the real holder's identity). Such attribute-based credentials are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital (secret) signature key. However, attribute-based credentials (ABCs) allow their holder to transform them into a new credential that contains only a subset of the attributes contained in the original credential. These transformed credentials can be verified just like ordinary cryptographic credentials (using the public verification key of the issuer) and offer the same strong security.

Step 6: Identify Service Management Requirements

The fundamental goals of any cloud computing environment are to reduce cost, improve flexibility and increase reliability of the delivery of a service. Critical to meeting these goals is a uniform, straightforward, transparent and extensible system for managing and monitoring cloud services. In this section we will outline some key considerations in service management when entering into a service level agreement with a cloud computing provider.

Every computing system requires internal controls, management, automation and self-healing in order to operate in today's interconnected world, and the cloud is no different. Although the standards for SLA language for service management are evolving, it is of upmost importance to include provisions for the considerations outlined below in your agreements.

Auditing

First and foremost in ensuring manageability of cloud services is a methodology for auditing and reviewing those services. This helps discern between providers who are fully capable of deep manageability and those who provide only a simple veneer on someone else's offerings. As stated by many an experienced manager, organizations and people do what you inspect, not what you expect.

[41]See for example "New Digital Security Models" by the Danish National IT- and Telecom Agency (NITA) http://ebookbrowse.com/new-digital-security-models-pdf-d70827649

The objective of any SLA terms in the area of auditing is multi-fold:

1. Provide you with an unbiased assessment of your ability to rely on the service provided
2. Assess the depth and effectiveness of the provider's internal systems and measures
3. Provide tools to compare quality levels with other competing providers
4. Uncover issues in your own organization's ability to interface with the provider and provide uninterrupted services

This last objective is especially important. Many documented challenges have come not from a cloud provider's ability to service a customer, but the ability of the customer's systems to interface properly with the cloud. Therefore any audit scope should include both the provider and any internal systems exposed to the cloud to ensure a complete "envelope" of integrity.

When considering the scope of any auditing protocol, you must step beyond contract terms and conditions and ensure that you are addressing general issues of management and governance. For example, it's insufficient to include a provision to regularly audit security and encryption keys, only to neglect addressing any internal resource allocations, scheduling, review and approval processes needed to perform the audit and address any issues stemming from the audit. Consider carefully the importance of leveraging existing methods of audit and compliance that already exist in your organization, and look to extend those to the cloud vs. creating new ones.

Monitoring & Reporting

Transparency of the service level is extremely important to a successful service management protocol. While every cloud vendor offers different systems for visualizing data and its implications (web based, e-mail based, live, reactive, portal-based), consumers should demand from any cloud SLA a minimum set of capabilities:

1. *Cloud Performance Management*. This domain focuses on the response times for systems within the cloud architecture and between the cloud and the target user systems.
2. *Load Performance*. This domain focuses on measurements and timings for when the cloud is under stress, either intentional or unintentional. As systems can perform differently when under different loads, and the interactions and dependencies of a complex cloud are often unknown in advance, it's important to visualize data both in a steady state as well as under load.
3. *Hybrid and Inter-cloud Performance*. As many clouds consist of different subsystems, often sourced from different cloud providers, it's critical to visualize data about the interactions between those hybrid cloud components.
4. *Application Performance*. This domain focuses on the applications executed from the cloud, particularly internal processing benchmarks as well as end-user experience measurement.
5. *Problem Notification*. This domain focuses on monitoring and reporting on failures and issues with the cloud system. Addressed are issues with prioritization, notification and severity level assessment.

Although the benchmarks in each of these areas are evolving, ensuring your SLA includes the ability to see, assess and react to measurements in these areas will help keep your cloud infrastructure running smoothly.

Metering

A core characteristic of many cloud services is an on-demand model, where services used are billed as they are consumed, on a time or capacity basis. Therefore it is important to have confidence and transparency in the metering system employed by cloud providers, as embodied in the service level agreements you build. At a minimum, you must ensure that metering systems employed for your cloud providers include:

1. Assurance of accurate billing, and a methodology for handing objections or challenges to any automated metered billing
2. The ability to segregate different services into different methods of billing: for example, performance testing, analytics, security scanning, backup, and virtual desktops might all be measured differently and metered separately.
3. Ability to handle taxation issues from geography to geography, and from user to user. As each country and municipality has implemented different approaches to taxation of online commerce, your provider must be able to discern between these sources of use and meter them independently.

Rapid provisioning

While auditing, monitoring, measuring and metering relate primarily to the cost savings features of the cloud, rapid provisioning is a key underlying quality of the improved flexibility that comes from the cloud. However, it's not without its own unique qualities that must translate into your service level agreements with providers:

1. *Core provisioning speed*. As part of a cloud SLA, there should be baseline expectations of the speed of deployment of new systems, new data, new users, new desktops or any function that's core to the service provided by the cloud vendor.
2. *Customization*. It's unusual that any templated method of rapid provisioning can be used "out of the box" without configuration and customization. Without careful management of the expectations and contractual levels for this function, any savings gained by automated rapid provisioning can evaporate in the face of delays in customizations post-deployment.
3. *Testing*. Important to any strong SLA are provisions for testing automated deployment and scaling prior to need. This is particularly acute in areas where provisioning is employed in disaster recovery or backup situations.
4. *Demand Flexibility*. It does no good to have a technical solution to rapid provisioning if the system is incapable of dynamic de-provisioning to match downturns in demand.

This is not an exhaustive list of considerations, only the basic requirements of any contractual definition of rapid provisioning. Each organization will need to add their own particular additional topics, particularly for different industries or IT applications running in the cloud.

Resource change

Change is an inevitable part of any IT system, and the cloud is no different. Fortunately, there is little that is special about the cloud in regards to considerations for change management. Procedures for requesting, reviewing, testing, and acceptance of changes differ little from those already in use with other IT subcontractor contracts and outsource agreements. The only unique issue is the sensitivity that many have to changes that have potentially radical implications, such as the cloud. In this case, extra care should be taken to manage the process carefully.

Upgrade to existing services

A subset of change management is upgrades or improvements in existing contracted services, such as when an upgrade or patch is needed, or when a new version of an underlying management system or SaaS application is rolled out. In these cases, it's important to outline in your cloud SLA a set of basic steps for these inevitable needs.

1. **Responsibility to develop requested changes.** There should be a clearly defined responsibility set for which party is in the lead for different types of upgrades. For example, if the upgrade is dependent on many subsystems or people internal to an organization, not in the cloud, it might be advisable to center the responsibilities on the contracting organization vs. the cloud provider. On the other hand, if the majority of the upgrade happens with cloud-provider personnel within the cloud space, it's likely the provider would assume primary responsibility.
2. **Process for identifying a timeline to develop, test and implement the change.** There must be a clearly defined "chain of command" and project plan for all changes made to the cloud environment, properly resourced and timed to ensure reasonable contingencies and problem resolution. Here too, little is different regarding a cloud solution vs. a traditional IT solution, with the exception of the increased anxiety and scrutiny that the cloud draws today.
3. **Process for resolving problems resulting from change.** Since problems can often be compounded and result from multiple factors both within and outside the cloud, an SLA-based outline of upgrade procedures must include a clearly defined set of responsibilities and methods for resolving issues introduced by any upgrade.
4. **Back-out process if the changes cause major failures.** Even the best-laid plans often run aground on the rocks of reality. Cloud services providers should automatically embed rollback checkpoints throughout an upgrade plan in order to "pull the plug" and restore any upgrade to its initial state should an unexpected and unsolvable problem crop up during the upgrade procedure. Throughout the process, regular communication meetings should occur to keep both parties in sync.

Step 7: Prepare for Service Failure Management

Service failure management outlines what happens when the expected delivery of a service does not occur. Service capabilities and performance expectations should be explicitly documented in the cloud SLA. If not, the likelihood of misunderstandings between consumer and provider increases significantly. For example, a web service performing poorly in terms of response time may not be considered a service failure to the provider unless it is clearly called out in the SLA.

The level of service failure management will vary greatly dependent upon provider, and the ability to negotiate a greater level will vary upon size of the consumer. As a result, it is important for consumers to incorporate their own service failure management capabilities to ensure they are made aware of any issues in a timely fashion.

Remedies

The primary remedy for service failure is service credits. These are based upon a percentage of the fees paid by the consumer during the billing cycle. The actual percentage will vary depending on the provider. However, it is common that these service credits will not exceed 100% of the paid fees. This often results in service credits not being in proportion to business cost or risk.

It is also important to note that common service level agreements put the responsibility of reporting a service interruption on the consumer. The consumer will need to contact the provider and be prepared to show that their service has been impacted by a service interruption.

Limitations

Within each cloud provider's agreement there are likely liability limitations for certain types of service interruptions. While these may vary dependent upon the provider, a sampling of several major providers shared the following exclusions:

- Scheduled or emergency outages
- Acts of force majeure
- Suspension of service due to legal reasons
- Internet access issues outside the control of the provider

In addition to common, shared limitations, there are providers who may also cite unscheduled downtime as being excluded from the SLA metrics. Consumers are strongly encouraged to fully understand all facets of their cloud SLA.

Given these limitations, it is important that consumers plan for unavailability. This may include keeping a separate, on-premise backup copy of the cloud data. While this may be more feasible for a large company, a small company may need to either ensure the provider is backing up data or contract a second provider to complete these backups. The frequency of the backups would be dependent upon the criticality of the data and the data's rate of change.

Roles / Responsibilities

The roles of cloud computing service failure management are similar to the Information Technology Infrastructure Library (ITIL) incident management roles. The consumer incident manager would have responsibility to drive the incident and crisis management process. Assuming the failure is impactful to service delivery, the consumer incident manager should be plugged into the provider's incident management process as well. This collaboration should be negotiated into the agreed upon SLA. This may also be more easily negotiated for large organizations. Smaller organizations may need to proactively reach out to the provider when an incident occurs and engage in a more manual fashion.

The end goal is to ensure that the consumer is knowledgeable of activity being taken to resolve provider incidents which impact service delivery.

On the consumer side, additional roles include the help desk, and development and engineering support teams. The help desk should be in communication with the incident manager so as to understand impact and estimated time to resolution. This is important as the help desk is likely receiving questions regarding the service availability from their customers. The development and engineering support teams would be engaged to triage and resolve applicable failure scenarios.

Notification process of a failure (perceived or real)

Notification of a process failure could be triggered by two paths. The first is the result of a synthetic transaction integrated into the consumer's monitoring processes. A synthetic transaction is a "fake" transaction that flows through the entire system to test availability and response of all components. This path could alert on individual components throughout the transaction stream. An alert due to the execution failure of the SaaS component could be indicative of a corresponding issue at the provider. It is beneficial to build retry logic into the application to address items such as communication issues that would present themselves as a service call failure.

The capability of a synthetic transaction to identify issues is dependent upon the type of application transaction used (asynchronous or synchronous). It is recommended that calls to invoke a SaaS provided application component are routed through a service bus as this provides standard routing architecture with capabilities such as logging, queuing, retries, etc.

The second notification path would be triggered by the provider's monitoring system. This alert would, ideally, be integrated into the consumer's alerting system. This is not prevalent in today's cloud service delivery, but it is an important point to try to negotiate into a cloud SLA. An alert would be sent to the consumer in the event that the issue causes a service interruption and, potentially, impacts agreed upon SLA terms. Upon receiving notification, the consumer should follow their established incident escalation process.

Problem identification should be a joint activity between the consumer and the service provider. This may be common place in the relationship between a large consumer and provider. For smaller consumers, the provider may provide problem information via an informational website rather than a personal interaction. It is critical that the consumer fully understand the provider's monitoring and alerting processes. The monitoring and alerting processes should be called out in the agreed upon SLA. In the event that this is non-negotiable, the onus shifts to the consumer to provide monitoring and alerting. This is especially important in the instance of SaaS offerings that provide components to a larger solution.

As monitoring of problem identification should be a joint responsibility, the monitoring and alerting systems at the provider and consumer should have an integration point. This may include a statement in the SLA to send an e-mail or web service call when an incident occurs. This ensures that alerts created at the provider that impact the service delivery of the solution are captured within the consumer's incident management process.

Step 8: Understand the Disaster Recovery Plan

Disaster recovery is a subset of business continuity and focuses on processes and technology for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure in case of a disaster. By the term disaster we mean either natural disaster or man-made events that have an impact of availability of IT infrastructure or software systems.

It is common to see a false sense of security among cloud consumers regarding disaster recovery planning. Just because businesses are outsourcing the infrastructure (IaaS), applications (SaaS), or platforms (PaaS) to the cloud does not absolve them of the need for serious disaster planning. Every company is unique in the importance it assigns to specific infrastructure/ applications, thus, a cloud disaster recovery plan is specific to each organization, and business objectives should play an important role in determining the specificity of disaster recovery planning.

The process of devising a disaster recovery plan starts with identifying and prioritizing applications, services and data, and determining for each one the amount of downtime that's acceptable before there is a significant business impact. Service priority, required recovery time objectives (RTOs), and recovery point objectives (RPO's) will determine the overall disaster recovery approach. For example, in some applications maintaining uptime may be more important than having the data precisely replicated as of the last time of failure. Further, while 99%+ uptime SLAs are common in cloud computing (approximately 4 days of down time a year), it may not be adequate for specific application and business needs.

In general, current cloud SLAs provide inadequate guarantees in case of a service outage due to a disaster. Most cloud SLAs provide cursory treatment of disaster recovery issues, procedures and processes. That being said, it is rare for SMBs – the primary customer of clouds today, to internally develop the extensive disaster recovery infrastructure of large and established cloud providers.

Despite the limitations in cloud SLAs, cloud adopters should address key disaster recovery questions/issues with their service providers early in the process of cloud adoption. The key areas to address with cloud providers are:

- How is service outage defined?
- What level of redundancy is in place to minimize outages including co-location of services in different geographical regions?
- Will there be a need for a scheduled down time?
- Who has the burden of proof to report outages? This can be difficult to prove in case of conflicts with the cloud providers.
- What is the process that will be followed to resolve unplanned incidents?
- How will unplanned incidents be prevented or reduced?
- When does the time clock start on lack of service availability in order to measure service credits?
- How will incidents be documented or logged?
- What actions will be taken in the event of a prolonged disruption or a disruption with a serious business impact?

- What is the process of performing disaster recovery testing, and how often are the tests conducted? Are the reports of the tests provided to clients and are the tests automated?
- What is the problem escalation process?
- Who are the key service provider and customer contacts (name, phone number, email address)?
- What is the contingency plan during a natural disaster?
- How is the customer compensated for an outage? It must be noted that cloud providers have limits on the maximum compensation provided in case of an outage, and the compensation is an insignificant remedy in case of serious outage.
- Does the cloud vendor provide cloud insurance to mitigate user losses in case of failure? Although this is a new concept, some major cloud vendors are already working with insurance providers.

Answers to the questions above will be highly specific to particular organizations, and their specific disaster recovery needs. For large enterprises the questions mentioned above can be used as a framework to seek a stronger disaster recovery component in a negotiated SLA. It is important to emphasize that this is only possible for large enterprises with large contracts. Established cloud vendors are quite resistant to altering existing SLAs.

There are large numbers of events that can have negative impact on the availability of cloud services provisioned by customers. Although, detailing all of them is out of the scope of this section, some of the important areas that cloud consumers should consider are in areas of security/intrusion detection, denial of service, viability of a cloud provider, data ownership and recovery. As an example to highlight the above, consider a company using SaaS for critical applications, such as order management, billing, or ERP. The cloud user will face major technological hurdles in shifting to another provider in case of a disaster like a financial failure of the cloud vendor. Cloud users should make it a priority to address key contingencies in case of such an event. Issues such as access to data and the application in a timely manner are critical to clarify.

While, in most cases, companies will be able to retrieve the application data from an established SaaS provider, the business logic and software systems will be left behind. One solution is to deploy the SaaS software onsite and run it internally – clearly a difficult and risky solution to implement. So, despite good planning, in some cases no easy solutions are available for negative events. Development of data and meta-data standards in specific application domains could provide a considerable benefit for customers and allow them to migrate to different SaaS solutions in the event of a disaster. The development of such standards though is in direct conflict with the interests of many providers, and will take time to materialize.

It is also important to understand that risk mitigation related to disaster recovery for cloud solutions will also depend upon the specific cloud type (IaaS, SaaS etc). Compared to the SaaS example above, in the case of a negative event for an application running on an IaaS, the client can implement a different set of solutions. One example solution would be to architect the application to continue performing in the face of individual resource failure (e.g., server failure, storage failure, network failure, etc), or in the case of a significant infrastructure failure use

hot/warm sites in a different geographical zone or on a completely different cloud. The key point to understand is that risks and solutions associated with negative events will be different for SaaS, IaaS and PaaS.

When it comes to disaster recovery the public cloud presents a due-diligence paradox.[42] While there are myriad options for implementing disaster recovery, and the cloud may simplify enterprise IT by abstracting away all the complexity, it also increases the difficulty of performing comprehensive due diligence. Lack of such diligence accompanied by weak SLAs represents a potential risk in the area of business continuity and disaster recovery. Thus, companies should view developing a disaster recovery plan as an important part of moving to the cloud. Companies can consider using business continuity/disaster recovery standards as part of their planning efforts. Existing standards such as BS 25999:2007, NFPA 1600:2010, NIST SP 800-34, ASIS SPC.1-2009, ISO 27031, and ISO 24762 can provide an effective starting point for planning disaster recovery.

The cloud is growing at a rapid pace and cloud providers are facing a learning curve. In response to recent outages, providers are broadening the service options available to consumers. Recent announcements on increased interoperability among different providers for certain cloud services will be beneficial to customers. It also is an acknowledgement that industry players must work together in order to make the cloud more reliable for consumers.

Step 9: Develop an Effective Management Process

In the evolving world of cloud computing, there is a need for an effective management process for any problems that may arise. Today's reality is that cloud SLAs contain very limited information on consumer-provider management processes except possibly for large enterprises that are capable of negotiating unique terms. Implementing an effective management process is an important step to ensuring internal and external user satisfaction with cloud based service(s).

Table 8 below highlights the key elements of a successful management process.

Table 8. Management process

Element	Description
Establish monthly status meetings	• Establishes proactive management to quickly resolve SLA compliance issues. • Reduces the possibility of surprises and dissatisfaction with the service(s). • Led by cloud provider and attended by stakeholders from both the cloud consumer and the cloud provider.

[42] Refer to http://www3.cfo.com/article/2012/1/the-cloud_cost-of-disaster-recovery-in-cloud?currpage=2.

	• Meeting minutes should be documented.

Ensure proper attendance	It is important to have the right people in the status meetings. Both the cloud consumer and the cloud provider need to be represented and each party must have a stake in the overall success of the service(s). Examples of the attendees in the status meetings are as follows:
	• Cloud Consumer
	  ○ Customer Support management representative.
	  ○ Technical Support management representative.
	• Cloud Provider
	  ○ Technical Support management representative.

Topics of discussion	While the primary purpose of the status meeting is to focus on ensuring all problems are resolved within the agreed to criteria, there are some additional items that can be discussed with the purpose of ensuring both parties are aligned with the continuing management of the service(s): • Potential changes in the support processes or key personnel changes. • Plans for enhancements to the existing services. • Plans for adding new services to the existing environment. • Other topics which may impact the level of service being provided or expected.
Track key indicators	Four key indicators should be tracked to ensure that the SLA criteria are being met and that the downstream users of the service (either internal or external to the enterprise) are experiencing the level of service that has been agreed to: • High impact problems and time to resolution. • Number of open problems and their respective impact. • Total view of problems not resolved within agreed to time frames. • Trends of number of problems being reported with the resulting resolutions.
Produce reports	In order to ensure SLA compliance, a set of reports, generated by the cloud provider, needs to be available to all parties. • Reports that focus on the current reporting period addressing: ○ All problems reported (sorted by impact).

- Problems closed (sorted by impact).
- Duration of open problems (sorted by impact).

- A second set of reports which summarize the year to date (YTD) activity, by month and by impact, to identify trends.

It is the responsibility of the cloud provider to lead the status meetings and to provide a clear picture of the status of services, using the provided reports. To ensure that there is no confusion with agreed to actions and target dates, a set of minutes should be recorded. It is also very important that the person(s) responsible for the items be documented. Having a complete set of minutes from each status meeting accomplishes two objectives. Firstly, it eliminates any confusion in what and who is responsible for an action on a specific problem. Secondly, if there is ever a dispute over either a specific problem or the overall performance of the service, the minutes will serve as the record to resolve the dispute.

For problems which require management awareness, it is the responsibility of the attending stakeholders at the meeting to advise their respective management chains on the status of a particular issue.

Escalation Process

Inevitably, there will be problems which fall outside the normal management process and will need additional focus to ensure a timely resolution. An example of the exceptional process is a major outage, i.e. loss of service, which can not wait for the monthly status meeting and requires an immediate notification of the management chain.

While we use the term escalation, the escalation process is really upward communication for awareness for a particular situation and not an upward delegation of responsibility for the resolution of the problem.

Table 9 below highlights the overall objectives of escalation, general guidelines for when to initiate an escalation, and the types of escalations that can be invoked.

Table 9. Escalation considerations

Consideration	Description
Objectives	• Raise management awareness to avoid surprises (gives the perception that senior management is in control of the situation). • Gain agreement for action plans to resolve a problem. • Develop either a plan and gain agreement for additional resources, when required.
Guidelines	• Problem has a critical impact to the overall business to either an internal service or a

	customer facing service. • Service is still available but is significantly degraded; potential impact to a customer facing service. • Problem is of a significant impact and has missed the agreed to targets for resolution. • Independent of impact, problems are not being closed within the expected guidelines. • Number of problems is increasing with no agreed to resolution to reverse the trend.

Types	• **Immediate**
	  ○ A critical business impact is identified.
	  ○ Significant impact to a customer facing service.
	• **As required**. Typically after the monthly status meeting when:
	  ○ The duration of problem resolution is not being met.
	  ○ Number of open problems exceeds expectations.
	  ○ Trend for reported problems is increasing without a satisfactory resolution plan being offered.

Once an escalation has been initiated, the goal is to ensure that both chains of management understand the problem, its impact, and the currently agreed to action plan for resolution including containment of the problem, especially if the problem impacts an external customer service.

If a resolution of an escalated problem can not be reached through the escalation process then the terms of the SLA can be brought to bear to force resolution. Bringing the SLA terms into the discussion should be a last resort and only invoked should there be continual non-compliance of the SLA. One of the outcomes of continuous breaches to the SLA can be termination of the agreement with the provider for the contracted service(s). It should be noted that the minutes generated from the management process will be an important set of documentation to support the termination process.

Escalation should not be considered a last resort in the problem management process. Escalation should be used as an early warning activity to raise management awareness of a potential problem before it becomes critical. Escalation is a tool to manage the services and ultimately provide the best services to the users of the service(s), whether the users are internal or external to the organization.

Step 10: Understand the Exit Process

An exit clause should be part of every cloud SLA and describes the details of the exit process including the responsibilities of the cloud provider and consumer in case the relationship terminates prematurely or otherwise.

There are numerous potential scenarios that could cause the termination of service between consumer and producer which would result in the execution of the exit process. For example, a provider may be unable to deliver the required levels of performance and availability specified in the SLA, or it may be the case that the provider is going out of business. Regardless of the reason, a clearly defined exit process that ensures secure and speedy transfer of consumer data and applications is essential.

A consumer exit plan should always be prepared at the outset of the SLA and is an integral contractual annex. This plan should ensure minimal business disruption for the customer and ensure a smooth transition. The exit process should include detailed procedures for ensuring business continuity and it should specify measurable metrics to ensure the cloud producer is effectively implementing these procedures.

By far, the most important aspect of any exit plan is the transmission and preservation of consumer data which is critical to achieving business continuity. In addition, consumers must ensure that their data is completely removed from the provider's environment once the exit process is complete. Consumers should look out for and beware of the following details when they evaluate the exit clause included in a cloud SLA.

- The level of provider assistance in the exit process and associated fees should be clear in the SLA. In most cases, there should be no additional cost associated with the exit process.
- Providers should be responsible for extracting consumer data from their IT environments, or at least aid the consumer in extracting their data by providing clear and concise documentation.
- The format of the data transmitted from the provider to the consumer should be specified in the cloud SLA and should leverage standard data formats whenever possible to ease and enhance portability.
- The SLA should specify that all data and information belonging to the consumer be maintained for a specific time period after transition and then be completely removed immediately after.
    - The typical time period is 1-3 months which gives the consumer sufficient time to find a new provider and to continue receiving service from the current provider in the interim.
    - The time period should be explicitly documented in the cloud SLA and only with the consumer's written notice should data be removed and destroyed before that time.
- Consumers should ensure that the SLA provides appropriate business continuity protection during the exit process.
- At the completion of the exit process, consumers should receive written confirmation from the provider that all of the consumer's data has been completely removed from the provider's IT environment. The written confirmation should also state that the provider agrees not to use the consumer's data for any reason in the future, including using the data for statistical purposes.

The bottom line is that consumers should undertake due diligence when evaluating and ultimately selecting a cloud provider. A trustworthy cloud provider should be prepared to work with consumers on a fair and effective exit strategy.

Summary of Keys to Success

Table 10 summarizes the critical keys to success for any organization evaluating and comparing SLAs from different cloud providers.

Table 10. Summary of keys to success

Key to Success	Summary
Develop a strong business case and strategy for cloud computing environment	• Assess criticalness of services being deployed in the cloud. • Determine functional and non-functional requirements for each service (performance, availability, security, privacy, etc.). • Understand legal and regulatory requirements concerning the data maintained in the cloud. • Identify key performance metrics for each service.
Assess provider's SLA against functional and non-functional requirements	• Based on the criticalness of the service being deployed in the cloud, determine if the cloud provider's SLA is sufficient to address the functional, non-functional, legal, and regulatory requirements of the service. • If not, determine if the cloud provider is willing to negotiate on the key aspects of the SLA that are not in line with your business strategy. • If the cloud provider is not willing to negotiate on these critical points, seek alternative providers who more closely address your requirements. • If a cloud provider who addresses your requirements cannot be found, strongly consider keeping the service within your enterprise IT environment.
Determine how to monitor SLA performance	• Assuming a cloud provider is found that meets your service requirements; understand the management process defined in the SLA. • Ensure your SLA includes the ability to see, assess and react to key performance measurements that will help keep your cloud infrastructure running smoothly. • Understand the notification process when service issues arise including method and timliness of notifications along with prioritization and severity level assessment of issues. • Be aware of remedies and liability limitations offered by the cloud provider when service issues arise.
Ensure an adequate disaster recovery plan can be defined and executed	• The cloud consumer bears the risk of disaster scenarios that severely limit the ability of their cloud provider to deliver service. • Cloud consumers must understand the provider's ability to support their data preservation strategy which includes criticalness of data, data sources,

	scheduling, backup, restore, integrity checks, etc. • Roles and responsibilities must be clearly documented in the SLA. In many cases, the cloud consumer may be responsible for implementing most of the data preservation strategy. • Based on the criticalness of the data, cloud consumers should clearly define recovery time objectives. • Consumers should test and verify the disaster recovery plan prior to production deployment. • Cloud consumers should consider purchasing additional risk insurance if the costs associated with recovery are not covered under their organization's umbrella policy for IT services or operational risk riders.

Ensure support for an efficient exit process	• The goal of the exit plan is to ensure minimal business disruption for the consumer should the relationship with the cloud provide terminate prematurely.
	• The exit plan should be taken into account during the assessment phase of potential cloud providers.
	• The provider's SLA should be carefully reviewed to ensure the consumer defined exit plan is capable of being implemented.
	  ○ The consumer should be able to terminate the agreement at any time, without penalty, provided sufficient notice is given to the provider.
	  ○ Data maintained on the provider's cloud resources should be stored using standard formats to ensure data portability.
	  ○ Transmission of data from the provider's cloud resources should leverage standard packaging and data transfer techniques.
	• Roles and responsibilities must be clearly documented in the SLA. In many cases, the cloud consumer may be responsible for initiating most of the exit process steps.

In addition, emerging standards in the following areas will help improve the ability for consumers to evaluate and compare the service levels offered by different providers:

- Standards that create consistent ways to describe services and associated terms including price.
- Standardized metrics that allow consumers to effectively track SLA performance.

- Standardized security and regulatory compliance requirements to identify control points for risk management.
- Standards that enable coordinated end-to-end SLA management for both cloud consumers and cloud providers.

Cloud computing offers a value proposition that is different from traditional enterprise IT environments. With proper focus on the key success factors, consumers are able to effectively review and compare SLAs from different cloud providers to ensure the promise of the cloud is realized.

Works Cited

Cloud Standards Customer Council (2011). *Practical Guide to Cloud Computing.* http://www.cloud-council.org/10052011.htm
This guide is to provide a practical reference to help enterprise information technology (IT) and business decision makers adopt cloud computing to solve business challenges.

2010 International Conference on High Performance Computing and Simulation
Low level Metrics to High level SLAs - LoM2HiS framework: Bridging the gap between monitored metrics and SLA parameters in cloud environments. Emeakaroha, Vincent C.; Brandic, Ivona; Maurer, Michael; Dustdar, Schahram

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing (Draft): Recommendations of the National Institute.* Gaithersburg: National Institute of Standards and Technology. http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf
This white paper defines cloud computing, the five essential characteristics**,** three service models, and four deployment models.

Queen Mary School of Law Legal Studies Research Paper No. 63/2010.
Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services http://ssrn.com/abstract=1662374
This document provides a comprehensive comparison of terms and conditions from the leading cloud service providers.

Cloud Security Alliance. *Security Guidance for Critical Areas of Focus in Cloud Computing Version 3.0 (2011).* http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf
This document provides an actionable, practical road map to managers wanting to adopt the cloud paradigm safely and securely.

Additional References

CSMIC SMI – Service Measurement Index, Carnegie Mellon University, 2011

International Function Point Users Group, Guidelines to Software Measurement, International Function Point Users Group, 1994.

International Function Point Users Group, Software Non-Functional Assessment Process Release 1.0, International Function Point Users Group, September 2011

itSMF Metrics for IT Service Management, Van Haren Publishing, 2006

ITU-T Cloud Computing Technical Reports – March 2012
http://www.itu.int/ITU-T/newslog/Cloud+Computing+And+Standardization+Technical+Reports+Published.aspx

National Institute of Standards for Technology Cloud Computing Standards Roadmap, NIST CCSRWG – 070, Eleventh Working Draft, May 2, 2011

TM Forum – GB 917 SLA Handbook – Release 3, TM Forum, January 2011

Woodward, Steven M, Using Project Metrics to More Efficiently Manage Projects – IT Measurement Practical Advice from the Experts; International Function Point Users Group (IFPUG), pages 271-292. Boston: Addison Wesley, 2002

Woodward, Steven M, Cloud Computing Solution Measurement. The IFPUG Guide to IT and Software Measurement, Taylor & Francis, for publication 2012