



MANAGED SERVICES FOR ORACLE CLOUD FOR US GOVERNMENT



ORACLE

Partner

Thank you for downloading this Oracle asset. Since 1991, DLT Solutions has been a trusted Oracle partner for the Public Sector. We combine deep expertise across Oracle technologies including software, infrastructure, Oracle Support renewals and Oracle Cloud with dedicated professional services to deliver mission critical solutions that support your mission. We also provide multiple contract vehicle options to simplify procurement of Oracle products and services, including but not limited to SEWP for federal and DoD customers and OMNIA for state and local entities.

For more information, visit: dlt.com/oracle

Managed Services For Oracle Cloud for US Government – Service Descriptions

March 24, 2025

Contents

Professional Services Delivery Policies	4
Oracle Cloud Infrastructure for US Government	4
GLOSSARY	5
MCS – Oracle Advanced Data Security Service for US Government Cloud.....	9
MCS – Oracle Advanced Data Security Service for US Defense Cloud	9
MCS Oracle Managed Analytics Cloud Service for US Government Cloud.....	11
MCS Oracle Managed Analytics Cloud Service for US Defense Cloud	11
MCS - Oracle Managed Applications Unlimited for US Government Cloud	16
MCS - Oracle Managed Applications Unlimited for US Defense Cloud	16
MCS Oracle Managed Applications Unlimited Non-Production Service for US Government Cloud.....	22
MCS Oracle Managed Applications Unlimited Non-Production Service for US Government Cloud.....	22
MCS - Oracle Managed Applications Unlimited for US Government Cloud - Enhanced Recovery Service.....	25
MCS - Oracle Managed Applications Unlimited for US Defense Cloud - Enhanced Recovery Service.....	25
MCS - Oracle Managed Applications Unlimited for US Government Cloud – RAC Support Option for Minimum and Low Complexity Services.....	26
MCS - Oracle Managed Applications Unlimited for US Defense Cloud – RAC Support Option for Minimum and Low Complexity Services.....	26
MCS - Oracle Managed Database as a Service for US Government Cloud	27
MCS - Oracle Managed Database as a Service for US Defense Cloud	27
MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud.....	32
MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud	32
MCS - Oracle Managed Enterprise Application Cloud – Additional Managed OCPU or Storage for US Government Cloud	37
MCS - Oracle Managed Enterprise Application Cloud – Additional Managed OCPU or Storage for US Defense Cloud	37
MCS Oracle Managed Exadata Database Cloud Service for US Government Cloud	39
MCS Oracle Managed Exadata Database Cloud Service for US Defense Cloud	39
MCS - Oracle Managed IaaS Service for US Government Cloud	44
MCS - Oracle Managed IaaS Service for US Defense Cloud	44
MCS - Oracle Managed Identity and Access Management for US Government Cloud, Foundation	50
MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Foundation	50
MCS - Oracle Managed Identity and Access Management for US Government Cloud	52
MCS - Oracle Managed Identity and Access Management for US Defense Cloud	52
MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced	56
MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced	56
MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced – Enhanced Recovery Service.....	61
MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced – Enhanced Recovery Service.....	61
MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited Connector	63
MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited Connector.....	63
MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited Environment – Integration Service	67
MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited Environment – Integration Service.....	67
MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited, Custom	Error! Bookmark not defined.
MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited, Custom.....	Error! Bookmark not defined.
MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited Connector - Enhanced Recovery Service.....	69
MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited Connector - Enhanced Recovery Service	69
MCS - Oracle Managed Identity and Access Management - Integrated Applications Unlimited Connector - Enhanced Recovery Service for US Government Cloud	Error! Bookmark not defined.
MCS - Oracle Managed Identity and Access Management - Integrated Applications Unlimited Connector - Enhanced Recovery Service for US Defense Cloud	Error! Bookmark not defined.
MCS - Oracle Managed Integration Cloud Service for US Government Cloud	70
MCS - Oracle Managed Integration Cloud Service for US Defense Cloud.....	70
MCS - Oracle Managed Security Data Masking Service for US Government Cloud	75
MCS - Oracle Managed Security Data Masking Service for US Defense Cloud	75
MCS - Oracle Managed Security Data Masking Service for Managed Apps Unlimited for US Government Cloud.....	Error! Bookmark not defined.
MCS - Oracle Managed Security Data Masking Service for Managed Apps Unlimited for US Defense Cloud.....	Error! Bookmark not defined.
MCS - Oracle Operational Readiness for Oracle Cloud Guard Service for US Government Cloud	77
MCS - Oracle Operational Readiness for Oracle Cloud Guard Service for US Defense Cloud.....	77

MCS – Security Account Manager for US Government Cloud.....	79
MCS – Security Account Manager for US Defense Cloud.....	79
Oracle Cloud Infrastructure Accelerator Service for US Government Cloud Advantage	80
Oracle Cloud Infrastructure Accelerator Service for US Defense Cloud Advantage.....	80
APPENDIX 1: ORACLE MANAGED SERVICES FOR ORACLE CLOUD FOR US GOVERNMENT DELIVERY POLICIES..	84
Oracle Managed Services for Oracle Cloud for US Government Security Policy.....	85
Oracle Managed Services for Oracle Cloud for US Government Access Management Policy	87
Oracle Managed Services for Oracle Cloud for US Government Change Management Policy	90
Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy.....	91
Oracle Managed Services for Oracle Cloud for US Government Release Management Policy	91
Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy.....	92
Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy	94
Oracle Managed Services for Oracle Cloud for US Government Service Level and Availability Management Policy.....	95
Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy	98
Oracle Managed Services for Oracle Cloud for US Government Service Continuity Policy.....	98
Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy.....	99
Oracle Managed Services for Oracle Cloud for US Government Enhanced Recovery Policy.....	100
Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy	101

Professional Services Delivery Policies

The Oracle Professional Services Delivery Policies (“Policies”) available at <http://www.oracle.com/contracts> apply to all professional services in Your order.

Oracle’s Professional Services Delivery Policies are subject to change, but such changes will not materially reduce the level of performance, functionality, security, or availability for the Services for the duration of Your order.

Oracle Cloud Infrastructure for US Government

Oracle Cloud Infrastructure for the US Government includes Oracle Cloud for US Government, Oracle’s FEDRAMP compliant and DISA IL4-authorized cloud region, and US Defense Cloud, Oracle’s FEDRAMP compliant and DISA IL5-authorized cloud region, (collectively, the “Oracle Cloud for US Government”). The applicable cloud region of the Oracle Cloud for US Government where the services purchased by You under this Service Description are deployed is identified by the applicable part number in Your order and corresponds to Your separately purchased Oracle Cloud Infrastructure Cloud Services subscription for the same cloud region.

The services under these Service Descriptions are provided by Oracle resources that are U.S. Citizens or resources that are "U.S. Persons". U.S. Person means a person who is a U.S. Citizen, lawful permanent resident as defined by 8 U.S.C. 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3).

GLOSSARY

For purposes of the limitations described herein, the following definitions apply:

ACCOUNT & SERVICE REVIEW FREQUENCY, SERVICE PLAN UPDATE & SERVICE REQUEST REVIEW FREQUENCY, AVAILABILITY PLAN FREQUENCY, and OPERATIONAL REPORTING FREQUENCY are the maximum entitlement for Your use of continual service improvement and governance services as described in the *Appendix 1: Oracle Managed Cloud Service Delivery Policies*

BLOCK STORAGE ALLOCATION: Total GB of storage used as required to operate applications, shared services, and virtual machine database systems with Enterprise Edition Extreme Performance.

CEMLI: An acronym for any “configuration, extension, modification, localization, and integration”.

CO-RESIDENT THIRD PARTY PROGRAM: Any software from a Third Party Software vendor that resides in the same environment as, and simultaneously shares the same database and compute resources as, the Oracle Programs; Co-resident Third Party Programs do not include Required Software.

COMPARTMENT: A logical container within Oracle Cloud for US Government that organizes and isolates cloud elements, such as network, storage, and compute resources for a specific set of environments.

CRITICAL PATCH UPDATES (“CPUs”): Collections of security updates for Oracle products that are available to customers with valid technical support contracts and that are applied to the environment as part of the emergency release management process as described in the Release Management Policy.

DISASTER: An unplanned outage that causes a complete loss of access to and use of the Oracle Programs in the Production Environment at a primary data center location for a period greater than 24 hours, as declared by Oracle.

DISASTER RECOVERY ENVIRONMENT: An instance specifically setup to recover Production Environment data at a secondary data center location in the event of a Disaster.

END USER: A user authorized by You to use certain Oracle programs and components of the Managed Services Environment.

ENHANCED RECOVERY SERVICES: Services designed to recover production data from a primary data center location to a secondary data center location in the event of a Disaster in accordance with the Recovery Time Objective (“RTO”) and Recovery Point Objective (“RPO”).

FASTCONNECT: Network connectivity used for connecting Your network with Oracle Cloud Services.

INCIDENT: An event experienced by You in the use of the Managed Services for which a Service Request has been submitted, that is not consistent with the standard, documented operation of the Managed Services, and which causes, or may cause, a service interruption.

INITIATION PHASE: The period at the commencement of the Services during which Oracle and You will perform the defined activities to transfer relevant information.

LOAD BALANCER: Load balancing for automated traffic distribution.

MY ORACLE SUPPORT (“MOS”): Oracle’s web-based customer support and ticketing system under which Oracle provides technical support for Oracle Programs and by which You may submit Service Requests and/or Requests for Change. The use of My Oracle Support is obtained by purchasing technical support services from Oracle under a separate contract.

NON-PRODUCTION ENVIRONMENT: An instance that is specifically configured for Your use (or, as applicable, Your implementer’s use) of the Oracle Programs for non-production activities that relate to the Managed Services, such as development, training, data conversion, and CEMLI maintenance.

OCPU ALLOCATION: Total number of OCPUs deployed to support compute for applications, shared services, and virtual machine database systems with Enterprise Edition Extreme Performance as required for delivery of the Services.

OUTAGE: A complete loss of access to and use of the Production Environment, the Production Support Environment, or the Non-Production Environment. An Outage may be a Planned Outage or an Unplanned Outage.

PERIODIC MAINTENANCE PLAN (PMP): A written plan prepared and maintained by Oracle that generally describes the schedule for the application of Changes, updates, and patches to the Production Environment.

PLANNED OUTAGE: An Outage scheduled by Oracle during which Oracle performs system maintenance and other activities for the environment and the Managed Services.

PROBLEM: Either (i) the collection of multiple recurring Incidents that exhibit common symptoms and that originate from a single, common cause, or (ii) a single Incident that results from a single error, and that has an on-going significant impact on the Managed Services (such as an Unplanned Outage), in each case for which the cause is unknown.

PRODUCTION ASSESSMENT: A document that is prepared by Oracle prior to Production Go-Live and that contains Oracle’s assessment of the compliance of Your Environment with Oracle Managed Services standards.

PRODUCTION ENVIRONMENT: The instance within the Environment that is specifically set up and configured to support Your use of the Oracle Programs and used by You for production operations.

PRODUCTION GO-LIVE: The date on which You first commences use of the Production Environment for production operations (i.e., to process live data).

PRODUCTION READY STATUS: A designation given by Oracle to You indicating that You may commence use of a Production Environment for production operations.

PRODUCTION SUPPORT ENVIRONMENT: The TEST and DEMO Environments that are specifically set up and configured in a manner that closely resembles the Production Environment, and that are used, as applicable, to troubleshoot and facilitate Incident resolution, to test changes prior to promotion of such changes to the Production Environment and for demonstration purposes.

RAC: Oracle’s Real Application Cluster (“RAC”) software used within Your Cloud Service database environment.

RAC NODE: One Instance of an Oracle Real Application Cluster-enabled database running on one node in a cluster.

REFRESH: The process of copying database files, application files, and/or the application metadata and artifacts from a source environment to a target environment and updating related configurations within the environment.

RELEASE: A software change or set of software changes, to Oracle Programs, that is provided to You by Oracle's Support Services organization as part of Oracle's technical support services.

REQUEST FOR CHANGE ("RFC"): A request submitted by You via My Oracle Support for a Change to an environment in accordance with the Oracle Managed Services for Oracle Cloud for US Government Change Management Policy.

REQUEST SYSTEM: System through which Service Requests for the Services are raised and managed.

REQUIRED SOFTWARE: Third Party Software for which Oracle requires You to separately purchase a license and technical support in connection with Managed Services for certain Oracle Programs, and for which Oracle expressly performs Managed Services, as described in the applicable service description.

RESTORE: Reload of an image copy of database files and application files from a backup to the environment from which the copy was made.

ROOT CAUSE ANALYSIS ("RCA"): Process by which Oracle seeks to determine the root cause of a Problem and/or an Incident, identify details of any work-around, including reasons for the work-around, as applicable, and the history of the Problem or Incident.

SERVICE DELIVERY REVIEWS: Meetings conducted with You to review service reports, discuss findings, risks and remediation recommendations, review delivery of the Services, identify any changes in Your business or environment(s) that may impact effectiveness of the Services, and evaluate additional services that may be required to address new threats.

SERVICE INTERRUPTION: A material reduction of the functionality and responsiveness of a component of the Production Environment, a Production Support Environment, or a Non-Production Environment, such that Your ability to use the Managed Services to process one or more of Your key business transactions is significantly impacted.

SERVICE REQUEST ("SR"): A request for assistance with the environment or any component thereof submitted to My Oracle Support.

SEVERITY LEVEL: The level of criticality assigned to a Service Request based on the defined criteria described in the Oracle Managed Cloud Incident and Problem Management Policy in Appendix 1.

STABILIZATION PERIOD: A ramp period following Changes to a Production Environment, such as (a) initial system implementation or migration, (b) point releases and major upgrades of application software, (c) introduction of CEMLI, (d) introduction of Third Party Software, or (d) introduction of additional modules.

TENANCY: The main structure within Oracle Cloud for US Government that contains all of an organization's resources. Within a tenancy, administrators can create one or more Compartments, create additional users and groups, and assign policies that grant groups the ability to use resources with a Compartment.

THIRD PARTY SOFTWARE: Software from a Third Party Software vendor, which is not provided by Oracle as part of the Managed Services, and any software developed or provided by You. Examples of Third Party Software are Required Software and Approved Third Party Software.

TIER TYPES: Types of tiers within the Compute Cloud Services environment, of which one or more compute nodes may be deployed for a unique function in the architecture, including, but not limited to: database, private middle, public middle, Oracle Discoverer, Oracle Endeca Commerce, and UPK Content, Knowledge and Development.

UNPLANNED OUTAGE: A complete loss of access to and use of a Production Environment that was not scheduled by Oracle or You and is caused by an Incident or Problem.

USER ACCEPTANCE TESTING (“UAT”): A formal testing process that is part of the Change Management Process conducted by You of a specified Change to the environment for the purpose of determining whether such Change meets identified acceptance criteria.

VIRTUAL MACHINE DATABASE SYSTEM: A virtual machine that has Oracle Database software deployed and configured with a user-specified number of cores, software edition, and database version. The Virtual Machine Database System contains one container database (CDB) that can have multiple pluggable databases (PDBs). A single CDB with a single PDB is created by default when the Virtual Machine Database System is created.

VM COMPUTE: VM Compute is a virtual machine (VM) that is an independent computing environment that runs on top of physical bare metal hardware. The virtualization makes it possible to run multiple VMs that are isolated from each other.

MCS – Oracle Advanced Data Security Service for US Government Cloud

MCS – Oracle Advanced Data Security Service for US Defense Cloud

Part Number	Service Offering
B109118	MCS – Oracle Advanced Data Security Service for US Government Cloud
B109335	MCS – Oracle Advanced Data Security Service for US Defense Cloud

Description of Services

Oracle will setup and configure Oracle Data Safe for Your Oracle Database(s) in Your Oracle Cloud for US Government tenancy for which You have separately purchased a subscription in accordance with the Service Maximums in the Managed Services Exhibit (the “Data Security Services”). The Data Security Services may include the following:

1. Designate a resource who will act as Your primary point of contact to facilitate account management and service reviews.
2. Conduct a preliminary meeting to review the Data Security Services and provide You with a security questionnaire to be completed by You (the “Questionnaire”).
3. Perform an analysis of the security configuration settings collected during the preliminary meeting and provided by You in the Questionnaire.
4. Review and validate Your Oracle Cloud for US Government tenancy requirements.
5. Check prerequisites for enabling Oracle Data Safe in Your Oracle Cloud for US Government tenancy.
6. Enable and configure Oracle Data Safe for Your Oracle Cloud for US Government tenancy.
7. Validate that Oracle Data Safe is set up in accordance with Your requirements.
8. Identify and document Your Oracle Databases (“DB document”).
9. Register the Oracle Databases identified in the DB document (“Target Database(s)”) with Oracle Data Safe.
10. Conduct quarterly Service Delivery Reviews.

Security Compliance Monitoring

If included in Your order, as indicated in the Managed Services Exhibit, Oracle will provide the following security compliance monitoring activities (“Security Compliance Monitoring”):

1. Perform an Oracle Data Safe security assessment scan against the Target Database(s).
2. Review and analyze the results of the security assessment scan.
3. Provide a report detailing the results of the security assessment scan and provide recommendations to address any issues.
4. Conduct a meeting with You to review the results of the security assessment scan.
5. Work with You to remediate issues identified in the security assessment scan report using the change management process.
6. Establish a baseline once all issues identified in the security assessment scan report are either remediated or accepted by the You.

7. Track security drifts from the established baseline through subsequent executions of the security assessment scans.
8. Deliver a scan report based on the security assessment scan in a format determined by Oracle and subject to Oracle's vulnerability policies ("Security Compliance Report").
9. Retain the Security Compliance Reports for a period of 12 (twelve) months.

Database Audit Management

If included in Your order, as indicated in the Managed Services Exhibit, Oracle will provide the following database audit management activities ("Database Audit Management"):

1. Enable Oracle Data Safe audit features for the Target Database(s).
2. Configure and apply Oracle Database audit policies for the Target Database(s).
3. Document the applied Oracle Database audit policies for the Target Database(s).
4. Configure database activity monitoring to detect and audit suspicious and unauthorized database activities.
5. Provide You with Oracle Database activity monitoring audit reports.
6. Triage issues related to the Data Security Services, including connectivity issues related to the Target Database(s).
7. Retain the Database Audit Management reports for a period of 12 (twelve) months.

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Procure and maintain for the duration of the Data Security Services:
 - a. OCI subscriptions required for the use of Oracle Data Safe.
 - b. Oracle Database Cloud subscriptions or Oracle Database licenses for the Target Database(s).
2. If Your Oracle Cloud for US Government tenancy is managed by You, provide Oracle with the administrative access required for the Data Security Services.
3. Designate a security point of contact who will be authorized to access and review the security reports.
4. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, and this service description.
5. Use Oracle's ticketing system to submit Service Requests and/or Requests for Change related to the Data Security Services.
6. For Target Database(s) on Your premises, set up the connectivity required for the communication between Oracle Data Safe and Your Target Database(s), including configuration of the Oracle Data Safe connector.

MCS Oracle Managed Analytics Cloud Service for US Government Cloud

MCS Oracle Managed Analytics Cloud Service for US Defense Cloud

Part #:	Service Offering
B109114	MCS - Oracle Managed Analytics Cloud Service for US Government Cloud - Bundled Base
B109331	MCS - Oracle Managed Analytics Cloud Service for US Defense Cloud - Bundled Base
B109115	MCS - Oracle Managed Analytics Cloud Service for US Government Cloud - Standard Base
B109332	MCS - Oracle Managed Analytics Cloud Service for US Defense Cloud - Standard Base
B109116	MCS - Oracle Managed Analytics Cloud Service for US Government Cloud - Hosted Environment
B109333	MCS - Oracle Managed Analytics Cloud Service for US Defense Cloud - Hosted Environment
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle will provide the following services (the “OAC Services”) for the Oracle Analytics Cloud (OAC) Service for which You have separately purchased a subscription (“Your Subscription”). The OAC Services are available only for the number of environments identified in the Managed Services Exhibit for Your Subscription (the “Managed OAC Environments”):

1. Provision and configure the Managed OAC Environments identified in the Managed Services Exhibit.
2. Use the assigned Oracle Cloud Administrator roles and privileges to provide the OAC Services as described in the following Sections of [Exhibit 1: Oracle Managed Services for Oracle Cloud for US Government Delivery Policies](#):
 - a. [Oracle Managed Services Oracle Cloud for US Government Security Policy](#) for OAC Services programs and Co-resident Third Party Programs.
 - b. [Oracle Managed Services Oracle Cloud for US Government Access Management Policy](#), consisting of managing administrative access for Your Subscription using the Oracle Cloud Administrator role, including the following activities/tasks in accordance with the Maintenance Frequency Table below:
 - i. Adding, removing, and changing of the administrative users for each OAC Environment
 - c. [Oracle Managed Services Oracle Cloud for US Government Change Management Policy](#), excluding application of software patches and consisting of the following activities/tasks upon Your request in accordance with the Maintenance Frequency Table below:
 - i. Provisioning, configuration, and administration of the OAC Environments
 - ii. Change tasks to existing configurations of the OAC Service and database connections
 - d. [Oracle Managed Services Oracle Cloud for US Government Configuration Management Policy](#)
 - e. [Oracle Managed Services Oracle Cloud for US Government Release Management Policy](#), consisting of planning deployments of quarterly updates to the OAC Service and associated Oracle software that are intended to improve performance, security, availability, stability, manageability, or regulatory compliance. Bundled task and configuration changes may be deployed during maintenance windows requested by You and subject to the constraints identified in the table below (the “Maintenance Frequency”).

Maintenance Frequency Table

Activity/Task	Frequency per month
Change Tasks Administration	Up to 5 times
Change Task Configuration	Up to 5 times
User Access Administration	Up to 5 times
Change Capacity Management	Up to 2 times

- f. [Oracle Managed Services Oracle Cloud for US Government Incident and Problem Management Policy](#), consisting of response and resolution of individual incidents, associated Service Request (SR) tracking, problem identification, and Root Cause Analysis.
- g. [Oracle Managed Services Oracle Cloud for US Government Monitoring Policy](#), using monitoring features that are made available a part of the OAC Services.
- h. [Oracle Managed Services Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#) for Your Subscription.
- i. [Oracle Managed Services Oracle Cloud for US Government Continual Service Improvement Policy](#)
- j. [Oracle Managed Services Oracle Cloud for US Government Service level and Availability Management Policy](#), excluding Service Request Resolution Time Service Level and including the following:
 - **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
 - **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.
 - **Service Level Credit %.** The percentage of monthly recurring fees paid by You for the OAC Services to be credited based on the credit criteria.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
OAC Environment Availability	99.5%	<99.5%	10%
Performance Against Service Description	Performance of the OAC Services in accordance with this section	As described in this Service Description	As indicated below

Oracle OAC Environment Availability Service Level

The OAC Environment Availability Service Level consists of the measurement of the percentage of time that the individual OAC Environment is available for access and use by You to conduct production business operations ("Production OAC

Environment”), and are measured by Oracle on a monthly basis and calculated in accordance with the following formula:

$$\left\{ \frac{[\text{Total minutes in a calendar month} \times \text{number of Production OAC Environments} - \text{Sum of Unplanned Outage (caused by OAC Service failure) minutes measured for each Production OAC Environment in such month}]}{\text{Total minutes in the calendar month} \times \text{number of Production OAC Environments}} \right\} \times 100$$

Only Severity Level 1 Unplanned Outages caused by OAC Service failures of a Production OAC Environment shall be used to calculate Oracle’s monthly performance against the OAC Environment Availability Service Level.

Incidents for which the root cause is subject to exclusion per Oracle Managed Services Oracle Cloud for US Government Delivery Policies or that occur in a Production OAC Environment during a Stabilization Period shall not be included in the OAC Environment Availability calculation. A Production OAC Environment must have one associated Production Support Environment for service level credits to be applicable.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the total fees paid by You for the specific Service for the month in which the Service Level Credit accrued, MINUS any Service Level Credit earned under the OAC Environment Availability Service Level in connection with the OAC Services provided in such month.

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the OAC Services for the month in which the Service Level Credit accrued.

Service Maximums

The OAC Services are subject to the following constraints (“Service Maximums”).

Additional Service Maximums are documented in the Managed Services Exhibit, as applicable.

Service Maximums

Type	Quantity/Frequency
Service Plan Update & Service Request Review Frequency	Quarterly
Account & Service Review Frequency	Annual
Availability Plan Frequency	Annual

Supplemental Resources

If included in Your order, Oracle will provide additional resources, up to the number of days¹ per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for *Oracle Managed Analytics Cloud Service for US Government Cloud* or *Oracle Managed Analytics Cloud Service for US Defense Cloud*:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Issue reproduction
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. For MCS - Oracle Managed Oracle Analytics Cloud Service for US Government Cloud – Bundled Base (part #109331) or MCS – Oracle Managed Oracle Analytics Cloud Service for US Defense Cloud – Bundled Base (part #109114), purchase and maintain for the duration of the OAC Services one or more of the following services (the “Pre-requisite Service”):

The following:

Part #	Service Offering
B109092	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud – Base
B109309	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud – Base
B109109	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud – ExaCC Standard Base Per Rack
B109113	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud – ExaCS Standard Base Per Rack
B109326	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud – ExaCC Standard Base Per Rack
B109330	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud – ExaCS Standard Base Per Rack

Any service/part number described by the following service descriptions within this *Oracle Managed Services for Oracle Cloud for US Government Service Description* document

- MCS - Oracle Managed Applications Unlimited on US Government Cloud Services
 - MCS - Oracle Managed Applications Unlimited on US Defense Cloud Services
2. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, Oracle Managed Services Delivery Policies, and this service description.
 3. Follow the Oracle Managed Services Minimum Architecture Guidelines (available at <https://support.oracle.com> by searching on [Document ID 784630.1](#)).
 4. Procure and maintain for the duration of the OAC Services adequate capacity for the performance of the OAC Services and Your Subscription.
 5. Perform all required end-2-end testing to validate that the OAC Service platform is configured securely, and correctly.
 6. Separately purchase services to migrate content to the Managed OAC Environments, if required and subject to additional fees.

7. Develop applications and application logic.
8. Provide support and assistance to Oracle as required to perform the assigned Oracle Cloud Administrator roles and privileges.
9. Provide support and documented requirements to Oracle as necessary for Oracle to manage and configure the Managed OAC Environments
10. Be responsible for managing end user access and application privileges.

Service Assumptions

1. Users are setup and authenticated with Oracle Identity Access Management ("IAM").
2. The OAC Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Managed Applications Unlimited for US Government Cloud

MCS - Oracle Managed Applications Unlimited for US Defense Cloud

Part #	Service Offering
B109091	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two Minimum Complexity
B109308	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two Minimum Complexity
B109090	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two Low Complexity
B109307	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two Low Complexity
B109089	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two High Complexity
B109306	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two High Complexity
B109088	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier One Minimum Complexity
B109305	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier One Minimum Complexity
B109087	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier One Low Complexity
B109304	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier One Low Complexity
B109086	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier One High Complexity
B109303	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier One High Complexity
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle will provide the following Oracle Managed Applications for Oracle Cloud for US Government Services (the “Services”):

The following as described in the [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#):

- [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#)
- [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#)
- [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#)
- [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#)
- [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#), including the following:

Periodic Maintenance Plan (PMP) intervals for Oracle Managed Applications Unlimited on Oracle Technology Cloud:

Maximum Interval between Installations	Services
Weekly	Mandatory or emergency patching
Quarterly	- Legislative updates - Critical Patch Updates

Annual	• Technology Stack updates • Application patch sets that do not affect functionality • Continuous Innovation ("CI") updates ^{1,2} • Implementation of system assessment recommendations
--------	---

¹ Applicable for Application Unlimited program versions that qualify as Innovation Release (refer to the Oracle Lifetime Support Policy for current CI Release versions)

² The current applied CI update must be under Error Correction Support

Refreshes including post Refresh steps, at the frequency listed below (except for Your J.D. Edwards Enterprise One programs). The type of Refresh may vary depending on the applicable Oracle application. Oracle will define which type of Refresh, if any, is available for Your Services Environment:

- One per month per Production Environment prior to Production Go-Live
- One per quarter per Production Environment following Production Go-Live

6. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#)

7. [Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy](#)

8. [Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#)

9. [Oracle Managed Services for Oracle Cloud for US Government Continuity Policy](#), including the following pre-defined backup schedule for Production Environments:

Backup Type	Backup Frequency
Database and code tree	• Daily backups retained for one week • Semi-weekly backups retained for four weeks
Archive logs	• Daily backups retained for one day • Semi-weekly backups retained for four weeks

Oracle will perform and store one baseline backup of the database, application code tree, and archive logs, upon Your request prior to achieving Production Ready Status. The baseline backup will be stored for a period of three months.

10. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)

11. [Oracle Managed Services for Oracle Cloud for US Government Enhanced Recovery Policy](#) (for Applications Unlimited High Complexity packages)

12. [Oracle Managed Services for Oracle Cloud for US Government Decommission Policy](#)

13. [Oracle Managed Services for Oracle Cloud for US Government Service level and Availability Management Policy](#) as described in the *Appendix 1: Oracle Managed Services Delivery Policies*, including the following for the Oracle Managed Application Unlimited for US Government Cloud or Oracle Managed Application Unlimited for US Defense Cloud Services under this Service Description:

- **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
- **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.

- **Service Level Credit %.** The percentage of monthly recurring fees paid for the Services to be credited based on the credit criteria.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
Application High Availability	99.7% ¹	>=99.0% and < 99.7%	2%
		<99.0%	5%
Application Availability	99.5%	>=99.0% and < 99.5%	2%
		<99.0%	5%
Service Request Resolution Time Severity Level 1	4 hours (Unplanned Outage caused by infrastructure and/or component) 24 hours (Service Interruption (functional failure))	<90% of SRs resolved within target	3%
Service Request Resolution Time Severity Level 2	96 hours	<90% of SRs resolved within target	2%
Performance Against Service Description	Performance of Managed Services in accordance with this Service Description	As described in this Service Description	As indicated below

¹ Requires deployment on RAC with Oracle Database High Availability (or High Complexity packages)

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the Oracle Managed Services under the applicable Ordering Document for the month in which the Service Level Credit accrued.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the total fees paid by You for the Services under this Service Description for the month in which the Service Level Credit accrued, MINUS any Service Level Credit calculated under the corresponding Application Availability Service Level in connection with the Services provided in such month, MINUS any Service Level Credit earned under the Service Request Resolution Time Service Levels in connection with the Services provided in such month.

Environments

Oracle will monitor setup and Production Go-Live of the Services Environment via a Managed Services Production Assessment. You will adopt and comply with the Production Assessment process and participate in a review with Oracle following Production Go-Live.

Oracle will service one (1) Production Environment and one (1) Production Support Environment as part of the Services base offering and one additional Environment for J.D. Edwards Programs and PeopleSoft Programs as follows:

- J.D. Edwards Programs: One Pristine Environment
- PeopleSoft Programs: One DEMO Environment

Effort Tiers

The Services are available only for the following Oracle Programs: Oracle E-Business Suite, Siebel CRM, Primavera, Oracle Hyperion, PeopleSoft, J.D. Edwards Enterprise One, Demantra, Oracle Business Intelligence – Enterprise Edition, Agile Product Lifecycle Management, Oracle Transportation Management, Oracle Advanced Supply Chain Planning, Oracle Strategic Network Optimization, and Oracle Rapid Planning. The Services are categorized into two tiers, based on the relative installation and management effort of the associated Oracle Programs:

- **Tier One:** higher-effort Oracle applications including Oracle E-Business Suite (including Endeca), Siebel CRM, Primavera, Oracle Hyperion and J.D. Edwards EnterpriseOne
- **Tier Two:** lower-effort Oracle applications including PeopleSoft, Demantra, Oracle Business Intelligence Enterprise Edition, Agile Product Lifecycle Management, Oracle Transportation Management, Oracle Advanced Supply Chain Planning, Oracle Strategic Network Optimization, and Oracle Rapid Planning.

Service Maximums

The Services are subject to the following constraints (“Service Maximums”).

Service Maximums

Maximum		Tier Two, Minimum Complexity	Tier Two, Low Complexity	Tier Two, High Complexity	Tier One, Minimum Complexity	Tier One, Low Complexity	Tier One, High Complexity
Production Database Size ⁽¹⁾		1 TB	3 TB	7 TB	1 TB	3 TB	7 TB
RAC		No RAC	No RAC	RAC (4 RAC Nodes)	No RAC	No RAC	RAC (4 RAC Nodes)
Program Modules		<=15	<=20	>20	<=15	<=20	>20
Tier Types		<=7	<=7	>7	<=7	<=7	>7
Service Plan Update & Service Request Review Frequency		Quarterly	Quarterly	Monthly	Quarterly	Quarterly	Monthly
Account & Service Review Frequency		Annual	Annual	Semi-Annual	Annual	Annual	Semi-Annual
Availability Plan Frequency		Annual	Annual	Semi-Annual	Annual	Annual	Semi-Annual
Enhanced Recovery Services	RPO	N/A	N/A	1 hour (24 hours for Hyperion or OBIEE with Essbase)	N/A	N/A	1 hour (24 hours for Hyperion or OBIEE with Essbase)

Maximum		Tier Two, Minimum Complexity	Tier Two, Low Complexity	Tier Two, High Complexity	Tier One, Minimum Complexity	Tier One, Low Complexity	Tier One, High Complexity
	RTO	N/A	N/A	12 hours (24 hours for Hyperion or OBIEE with Essbase)	N/A	N/A	12 hours(24 hours for Hyperion or OBIEE with Essbase)
Disaster Recovery Testing Frequency		N/A	N/A	Annual	N/A	N/A	Annual
Cloud Service Units – Hours equivalents, included with Your initial purchase of the Services		15	25	50	15	25	50
Business Transaction Monitoring		Monitoring of 1 Login Transaction	Monitoring of 1 Login Transaction	Monitoring of 1 Login Transaction	Monitoring of 1 Login Transaction	Monitoring of 1 Login Transaction	Monitoring of 1 Login Transaction
Vulnerability Scans		12 per year	12 per year	12 per year	12 per year	12 per year	12 per year

⁽¹⁾ Production Database Size is the number of terabytes of Block Storage purchased by You for the Non-Metered Compute Cloud Services Production Environment. The Production Database Size limitations reflect the physical size of the Production Environment database; actual storage for all environments, backup, archive, and other storage requirements associated with data replication and file system management may be greater than the physical size of the Production Environment database

Supplemental Resources

If included in Your order, Oracle will provide additional resources, either on-site or remotely, up to the number of days¹ per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for *Oracle Managed Applications Unlimited for US Government Cloud or US Defense Cloud Service*:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Issue reproduction
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Delivery Policies and this service description.
2. Procure and maintain for the duration of the Services the amount of Oracle Compute Cloud Service and Oracle Storage Cloud Service required to provide adequate computing capacity for the performance of the Oracle Programs associated with the Services.
3. Procure the amount of Oracle Storage Cloud Service required for Oracle to perform backups of Your data, at the pre-defined intervals.
4. Acknowledge that (i) You have separately acquired and will continue to maintain for the duration of the Services the licenses and Oracle Software Update License & Support (also referred to as "Premier Support"), or any equivalent successor Oracle technical support offering, including availability of security patch updates (SPUs) and/or Critical Patch Updates (CPUs), for the Oracle Managed Applications and any other necessary Oracle programs, including those for which the Managed Services are provided, (ii) you will maintain licenses and technical support for any Third Party Software or Co-resident Third Party Programs used in your Environments, including availability of security updates, and (iii) your use of such programs and technical support are governed solely by the agreement(s) under which such licenses and technical support are obtained.
5. Be responsible for release management, configuration management, performance management, Incident and Problem management for all CEMLI in the Environment.
6. Manage access and application responsibility privileges of all End Users of the Oracle Programs and Co-resident Third Party Programs.

Service Assumptions:

1. Production database size is the number of terabytes of Block Storage purchased by You for the Non-Metered Compute Cloud Services Production Environment (the "Production Database Size"). The Production Database Size limitations reflect the physical size of the Production Environment database; actual storage for all environments, backup, archive, and other storage requirements associated with data replication and file system management may be greater than the physical size of the Production Environment database.

MCS Oracle Managed Applications Unlimited Non-Production Service for US Government Cloud

MCS Oracle Managed Applications Unlimited Non-Production Service for US Government Cloud

Part	Service Offering
B109085	MCS - Oracle Managed Applications Unlimited Non-Production Service for US Government Cloud
B109302	MCS - Oracle Managed Applications Unlimited Non-Production Service for US Defense Cloud

Description of Services

MCS - Oracle Managed Applications Unlimited Non-Production Service for US Government Cloud or US Defense Cloud (the “Services”) consists of the following activities for one of Your Non-Production Environments in which the Oracle Managed Applications Unlimited reside and for which you have purchased the Services.

1. Service planning reviews intended to coordinate Your planned activities.
2. The following policies as described in the [*Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies*](#):
 - a. [*Oracle Managed Services for Oracle Cloud for US Government Security Policy*](#)
 - b. [*Oracle Managed Services Oracle Cloud for US Government Access Management Policy*](#)
 - c. [*Oracle Managed Services Oracle Cloud for US Government Configuration Management Policy*](#)
 - d. [*Oracle Managed Services Oracle Cloud for US Government Incident and Problem Management Policy*](#)
 - e. [*Oracle Managed Services Oracle Cloud for US Government Monitoring Policy*](#)
 - f. [*Oracle Managed Services Oracle Cloud for US Government Capacity Management and Performance Advisory Policy*](#)
 - g. [*Oracle Managed Services Oracle Cloud for US Government Change Management Policy*](#) consisting of the following
 - i. Installation and/or configuration of Oracle Programs;
 - ii. Installation of software patches which repair or modify existing functionality or maintain currency alignment with legislative requirements;
 - iii. Installation and/or update of Co-resident Third Party Programs, CEMIs, and operating system printer queues;
 - iv. Execution of read-only scripts and/or data fix scripts or SQL updates (Note: updates to base tables must be made via scripts authorized by Oracle Support);
 - v. Database space and object management related to space utilization, database layout, Oracle physical file mapping, and free space fragmenting;
 - vi. Refreshes that copy database and full application code from a source Non-Production Environment to a target Non-Production Environment, including post Refresh steps;
 - vii. Startup, shutdown, and/or recycle of the application and/or database in Your Non-Production Environment;

- viii. Assistance with database and application configuration changes based on Oracle recommended practices and suggestions from Oracle Support;
- ix. Backup of Your Non-Production Environment consisting of a copy of the database and complete application code tree, including verification of the backup for consistency and usability in case of recovery in accordance with the following backup schedule:

Backup Type	Backup Frequency
Database and code tree	• Daily backups retained for one week • Weekly backups retained for four weeks
Archive logs	• Daily backups retained for one day

- x. Export to, or import of, a database, partition, and/or table using Oracle database or application utilities; and
 - xi. Data load using Oracle utilities and providing data load results, including logs and error messages.
- h. [Oracle Managed Services Oracle Cloud for US Government Continuity Policy](#) for Oracle Programs, Required Software, and Co-resident Third Party Programs (collectively, the “Managed Software”) in Your Non-Production Environment designed to recover the Services in the event of hardware failure or human error:
- i. Configuration of the Services for automated backup, including configuration of OCI components; and
 - ii. Assistance with recovery of database and application functionality from backups as required
- i. Service Level Objectives as described in the following table:
- **Service Level Target:** The level of performance that Oracle endeavors to achieve on a monthly basis.
 - **Service Request Response Time:** The Service Request Response Time Service Level measures the elapsed time from the submission of an SR in [My Oracle Support](#) to Oracle’s acknowledgement of the receipt of the SR in [My Oracle Support](#) (“Time to Respond”).

Service Level	Service Level Target
Service Request Response Time	<= 2 hours

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Be responsible for Your, Your Users’ and Your third parties’ use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, [Appendix](#)

1: Oracle Managed Services Oracle Cloud for US Government Service Delivery Policies, and this Service Description.

2. Procure and maintain for the duration of the Services the amount of Oracle Compute Cloud Service and Oracle Storage Cloud Service required to provide adequate computing capacity for the performance of the Oracle Programs associated with the Services.
3. Be responsible for release management, configuration management, performance management, Incident and Problem management for all CEMLI in Your Non-Production Environment.
4. Perform analysis and be responsible for resolution of Incidents caused by Co-resident Third Party Programs.
5. Manage access and application responsibility privileges of all End Users of the Oracle Programs.

Service Assumptions

1. Oracle is not responsible for adverse impacts experienced by the Services due to insufficient computing capacity, including to the performance, availability, stability, and manageability of the Oracle Programs associated with the Services.

MCS - Oracle Managed Applications Unlimited for US Government Cloud - Enhanced Recovery Service

MCS - Oracle Managed Applications Unlimited for US Defense Cloud - Enhanced Recovery Service

Part #	Service Offering
B109084	MCS - Oracle Managed Applications Unlimited for US Government Cloud - Enhanced Recovery Service
B109301	MCS - Oracle Managed Applications Unlimited for US Defense Cloud - Enhanced Recovery Service

Description of Services

MCS - Oracle Managed Applications Unlimited for Oracle Cloud for US Government- Enhanced Recovery Service (“Services”) consists of:

1. [Oracle Managed Services for Oracle Cloud for US Government Enhanced Recovery Policy](#) as described in the [Appendix 1: Oracle Managed Services Oracle Cloud for US Government Service Delivery Policies](#).

Service Maximums

The Services are subject to the following constraints (“Service Maximums”).

Service Maximums		
Enhanced Recovery Services	RPO	1 hour (24 hours for Oracle Hyperion or OBIEE with Essbase)
	RTO	12 hours (24 hours for Oracle Hyperion or OBIEE with Essbase)
	Testing Frequency	Annual

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Be responsible for Your, Your Users’ and Your third parties’ use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, [Appendix 1: Oracle Managed Services Oracle Cloud for US Government Service Delivery Policies](#), and this Service Description.
2. Procure and maintain for the duration of the Services the amount of Oracle Compute Cloud Service and Oracle Storage Cloud Service required to provide adequate computing capacity to achieve disaster recovery service objectives.
3. Be responsible for release management, configuration management, performance management, Incident and Problem management for all CEMLI in the Environment.
4. Manage access and application responsibility privileges of all End Users of the Oracle Programs and Co-resident Third Party Programs.

MCS - Oracle Managed Applications Unlimited for US Government Cloud – RAC Support Option for Minimum and Low Complexity Services

MCS - Oracle Managed Applications Unlimited for US Defense Cloud – RAC Support Option for Minimum and Low Complexity Services

Part #	Service Offering
B109083	MCS -Oracle Managed Applications Unlimited for US Government Cloud – RAC Support Option for Minimum and Low Complexity Services
B109300	MCS -Oracle Managed Applications Unlimited for US Defense Cloud – RAC Support Option for Minimum and Low Complexity Services

Description of Services

Oracle Managed Applications Unlimited – RAC Support Option for Minimum and Low Complexity Services (the “Services”) consist of:

1. Use of Oracle's Real Application Cluster (RAC) software within Your Cloud Service environment for up to four (4) RAC Nodes in accordance with and to supplement the established maximums of one (1) of the following services separately purchased by You (hereinafter “Pre-requisite Service”):

Pre-Requisite Service

Part #	Service Offering
B109088	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier One Minimum Complexity
B109305	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier One Minimum Complexity
B109090	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier Two Low Complexity
B109307	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier Two Low Complexity
B109091	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier Two Minimum Complexity
B109308	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier Two Minimum Complexity
B109090	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier One Low Complexity
B109304	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier One Low Complexity

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Purchase and maintain for the duration of the Services:
 - a. one of the Pre-requisite Services listed above.
 - b. the associated amount of OCI required to provide RAC Support Service

MCS - Oracle Managed Database as a Service for US Government Cloud

MCS - Oracle Managed Database as a Service for US Defense Cloud

Part #:	Service Offering
B109103	MCS - Oracle Managed Database as a Service for US Government Cloud - Standard Base
B109320	MCS - Oracle Managed Database as a Service for US Defense Cloud - Standard Base
B109102	MCS - Oracle Managed Database as a Service for US Government Cloud - Bundled Base
B109319	MCS - Oracle Managed Database as a Service for US Defense Cloud - Bundled Base
B109104	MCS - Oracle Managed Database as a Service for US Government Cloud - Managed Database
B109321	MCS - Oracle Managed Database as a Service for US Defense - Managed Database
B109105	MCS - Oracle Managed Database as a Service for US Government Cloud - Managed Pluggable Database
B109322	MCS - Oracle Managed Database as a Service for US Defense Cloud - Managed Pluggable Database
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle will provide the following Managed Database as a Service services (the “Managed DBaaS Services”) for Oracle’s database software executing with Oracle Database as a Service (“DBaaS”) on Oracle Cloud for US Government for which You have separately purchased a subscription (“Your Subscription”). The Managed DBaaS Services are available only for Your Subscription and are deployed for the number and type of databases identified in the Managed Services Exhibit (the “Managed DB Environments”).

1. Provision and configure the Managed DB Environments.
2. Apply routine patches and updates of the compute node for bare metal (“BM”) configurations and compute node user domain DomU for virtual machine (“VM”) configurations in accordance with the Service Maximums Table below or at Oracle’s sole discretion for events associated with critical or urgent business requirements.
3. Use the assigned Oracle Cloud Administrator roles and privileges to provide the Managed DBaaS Services for the Managed DB Environments as described in the [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#).
 - a. [Oracle Managed Services Oracle Cloud for US Government Security Policy](#) for Oracle Database as a Service programs.
 - b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#), including managing administrative access for Your Subscription using the Oracle Cloud Administrator role that includes the following activities/tasks in accordance with the Service Maximums Table below:
 - i. Setting up new users and application privileges for each Managed DB Environment;
 - ii. Administration (adding, removing, and changing) of users and application privileges for each Managed DB Environments.
 - c. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#), including the following activities/tasks upon Your request in accordance with the Service Maximums Table below or at Oracle’s sole discretion for events associated with critical or urgent business requirements:
 - i. Installation, configuration, and administration of the Oracle Database as a Service software components and the Managed DB Environments;

- ii. Changes to existing configurations of the Managed DB Services and database connections;
- iii. Scaling or bursting (BM only) of the compute capacity for Your Managed DB Environments.
- iv. Installation of software patches which repair or modify existing functionality or maintain alignment with current business requirements.
- d. [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#), including planning of quarterly updates to the Oracle Database as a Service and associated Oracle software that are intended to improve performance, security, availability, stability, manageability and/or regulatory compliance. Bundled changes and configuration changes may be deployed during maintenance windows requested by You and subject to the constraints identified in the Service Maximums table.
- e. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#), including response to and resolution of individual incidents, associated Service Request ("SR") tracking, problem identification, and Root Cause Analysis.
- f. [Oracle Managed Services for Oracle Cloud for US Government Service Continuity Policy](#), using monitoring features that are made available as part of the Managed DBaaS Services to monitor the Managed DB Environments, including automated health checks.
- g. [Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#)
- h. [Oracle Managed Services for Oracle Cloud for US Government Service Continuity Policy](#), including (i) weekly full and daily incremental backups and (ii) retention of archive logs for 30 days, limited to Production Environments and Production Support Environments, and requiring object storage for backups provided by You, which is usually 7 times the amount of database storage in use.
- i. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)
- j. [Oracle Managed Services for Oracle Cloud for US Government Service Level and Availability Management Policy](#), excluding Service Request Resolution Time Service Level and including the following:
 - **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
 - **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.
 - **Service Level Credit %.** The percentage of monthly recurring fees paid by You for the Managed DBaaS Services to be credited based on the credit criteria.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
Service Availability	99.5%	<99.5%	10%

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
Performance Against Service Description	Performance of the Managed DBaaS Services in accordance with this Service Description	As described in this Service Description	As indicated below

Service Availability Service Level

The Service Availability Service Level consists of the measurement of the percentage of time that the individual Managed DB Environments is available for access and use by You to conduct production business operations (“Production Environments”), and are measured by Oracle on a monthly basis and calculated in accordance with the following formula:

$$\left\{ \frac{[\text{Total minutes in a calendar month} \times \text{number of Production Environments}] - \text{Sum of Unplanned Outage (caused by component or infrastructure failure) minutes measured for each Production Environment in such month}}{\text{Total minutes in the calendar month} \times \text{number of Production Environments}} \right\} \times 100$$

Only Severity Level 1 Unplanned Outages caused by Managed DB Service failures of a Production Managed DB Environments shall be used to calculate Oracle’s monthly performance against the Managed DB Environments Availability Service Level.

Incidents for which the root cause is subject to exclusion per the Delivery Policies or that occur in a Production Environment during a Stabilization Period shall not be included in the Service Availability calculation. A Production Environments must have at least one associated Production Support Environment for service level credits to be applicable.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the total fees paid by You for the specific Service for the month in which the Service Level Credit accrued, MINUS any Service Level Credit earned under the Service Availability Service Level in connection with the Managed DBaaS Services provided in such month.

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the Services for the month in which the Service Level Credit accrued.

Service Maximums

The Managed DBaaS Services are subject to the following constraints (“Service Maximums”).

Service Maximums

Type	Quantity/Frequency		
	1-9 Databases	10-20 Databases	20+ Databases

Type	Quantity/Frequency		
Patching requests per month	One	Two	Up to four
Scaling and bursting (BM only) requests per month	One	Two	Up to four
Change and configuration administration tasks per month	Up to four (4)	Up to ten (10)	Up to sixteen (16)
User access and privilege configuration and administration tasks per month	Up to four (4)	Up to ten (10)	Up to sixteen (16)
RAC	VM only (included with Extreme Performance OCPU subscription or a sufficient number of Customer provided RAC licenses)		
Database Encryption	- Initial Transparent Data Encryption (TDE) configuration - One (1) key rotation per year for TDE databases (Keys are maintained in Oracle Wallet)		
Service Plan Update & Service Request Review Frequency	Quarterly		
Account & Service Review Frequency	Annually		
Availability Plan Frequency	Annually		

Supplemental Resources

If included in Your order, Oracle will provide additional resources, either on-site or remotely, up to the number of days¹ per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for *Oracle Managed Database as a Service for US Government Cloud or US Defense Cloud*:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Issue reproduction
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, [the following obligations apply in addition to the obligations in the Policies](#):

4. For MCS - Oracle Managed Database as a Service for US Government Cloud – Bundled Base (part #B109102) or MCS - Oracle Managed Database as a Service for US Defense Cloud – Bundled Base (part # B109319) purchase and maintain for the duration of the Managed DBaaS Services one or more of the following services (the “Pre-requisite Service”):

a. The following:

Part #	Service Offering
B109114	MCS - Oracle Managed Analytics Cloud Service for US Government Cloud – Standard Base
B109332	MCS - Oracle Managed Analytics Cloud Service for US Defense Cloud – Standard Base
B95474	MCS - Oracle Managed Application Cloud for US Government Cloud, Custom
B109092	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud - Base
B109309	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud
B109109	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud – ExaCC Standard Base Per Rack
B109113	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud – ExaCS Standard Base Per Rack
B109326	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud – ExaCC Standard Base Per Rack
B109330	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud – ExaCS Standard Base Per Rack

b. Any service/part number described by the following service descriptions within this *Oracle Managed Services for Oracle Cloud for US Government Service Description* document.

- MCS - Oracle Managed Applications Unlimited for US Government Cloud Services
 - MCS - Oracle Managed Applications Unlimited for US Defense Cloud Services
5. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, the Delivery Policies, and this Service Description.
 6. Procure and maintain for the duration of the Managed DBaaS Services adequate capacity for the performance of the Managed DBaaS Services and Your Subscription.
 7. Perform all required end-2-end testing to validate that the Managed DBaaS Service platform is configured securely and correctly.
 8. Separately purchase services to migrate content to the Managed DB Environments, if required and subject to additional fees.
 9. Develop applications and application logic.
 10. Provide support and assistance to Oracle as required to perform the assigned Oracle Cloud Administrator roles and privileges.
 11. Provide support and documented requirements to Oracle as necessary for Oracle to manage and configure the Managed DB Environments.
 12. Separately purchase upgrades for the database software subject to additional fees.

Service Assumptions

1. The Managed DBaaS Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud

MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud

Part #	Service Offering
B109092	MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud - Base
B109309	MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud - Base
B109095	MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud – Base, Configurable
B109312	MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud – Base, Configurable

Description of Services

Oracle will provide the following services for one (1) or more Oracle enterprise application(s) (the “Oracle Managed Applications”) on Oracle Cloud for US Government in accordance with the Service Maximums table of this Service Description (the “MEAC Services”):

1. Provide the MEAC Services for each Oracle Managed Application that resides in Your Production Environment, Production Support Environment, Non-Production Environments, DR Environment, Pristine Environment, and/or DEMO Environment, in accordance with the Service Maximums table.
2. Provide the MEAC Services for additional Non-Production Environments, DR Environments, Pristine Environments, and/or DEMO Environments, in accordance with the Service Maximums table.
3. Provision and manage the services required to run the environments for the Oracle Managed Applications hosted on Oracle Cloud for US Government for which You have separately purchased a subscription (“Your Subscription”) and in accordance with the Service Maximums below.
4. Manage the Oracle Technology Stack in accordance with the Oracle Managed Cloud Minimum Architecture Guidelines (available at <https://support.oracle.com> by searching on [Document ID 784630.1](#)) and as required to support Your Third Party Programs integrated with Your Oracle Managed Application environment, and/or other additional shared services required for the Oracle Managed Application.
5. Provide up to the number of vulnerability assessment scans, identified in the Service Maximums table, of the virtual machines and database systems for the Production Environment and Production Support Environment of one (1) Oracle Managed Application identified by You as follows:
 - a. Implement external and internal security vulnerability scans of the virtual machines and database systems for the Production Environment and Production Support Environment (the “Vulnerability Scan”).
 - b. Deliver a scan report based on the Vulnerability Scans identified in the previous bullet 5.a., in a format determined by Oracle and subject to Oracle’s Security Vulnerability Disclosure Policies which are available at <https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html>.
6. Provide the services as described in the following sections of [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#)

- b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#)
- c. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#)
- d. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#)
- e. [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#), including the following:

Periodic Maintenance Plan (PMP) at the following intervals:

Maximum Interval between Installations	Services
Weekly	• Mandatory or emergency patching
Quarterly	• Legislative updates • Critical Patch Updates
Semi-Annual	• Technology Stack updates • Application patch sets that do not affect functionality • Continuous Innovation ("CI") updates ^{1,2} • Implementation of system assessment recommendations

¹ Applicable for Application Unlimited program versions that qualify as Innovation Release (refer to the Oracle Lifetime Support Policy for current CI Release versions)

² The current applied CI update must be under Error Correction Support

7. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#)
8. [Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy](#)
9. [Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#)
10. [Oracle Managed Services for Oracle Cloud for US Government Continuity Policy](#), including daily backups and retention of archive logs for 30 days, limited to Production and Production Support Environments.
11. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)
12. [Oracle Managed Services for Oracle Cloud for US Government Enhanced Recovery Policy](#)
13. [Oracle Managed Services for Oracle Cloud for US Government Decommission Policy](#)
14. [Oracle Managed Services for Oracle Cloud for US Government Service level and Availability Management Policy](#), including the following:
 - **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
 - **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.

- **Service Level Credit %.** The percentage of monthly fees for the MEAC Services to be credited based on the credit criteria.

Oracle will provide the applicable Application Availability Service Level Target in accordance with the Managed Services Exhibit, if applicable.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
Application Availability	99.5%	>=99.0% and < 99.5%	2%
		<99.0%	5%
Application High Availability ¹	99.7% ¹	>=99.0% and < 99.7%	2%
		<99.0%	5%
Service Request Resolution Time Severity Level 1	▪ 4 hours (Unplanned Outage caused by infrastructure and/or component) ▪ 24 hours (Service Interruption (functional failure))	<90% of SRs resolved within target	3%
Service Request Resolution Time Severity Level 2	96 hours	<90% of SRs resolved within target	2%
Performance Against Service Description	Performance of the Services in accordance with this Service Description	As described in this Service Description	As indicated below

¹ Requires deployment of additional OCI components in accordance with the *Managed Enterprise Application Cloud Minimum Architecture Requirements*

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the MEAC Services for the month in which the Service Level Credit accrued.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the fees paid for the MEAC Services for the month in which the Service Level Credit accrued, MINUS any Service Level Credit calculated under the corresponding Application Availability Service Level in connection with the MEAC Services provided in such month, MINUS any Service Level Credit earned under the Service Request Resolution Time Service Levels in connection with the MEAC Services provided in such month.

Service Maximums:

The MEAC Services are subject to the following constraints (the “Service Maximums”).

Changes to Service Maximums for part # B109095 – MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud – Base, Configurable or part # B109312 –

MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud, Base, Configurable will be documented in the Managed Services Exhibit, as applicable.

Service Maximums

Type		Quantity/Frequency
Oracle Managed Applications		Oracle E-Business Suite, Siebel CRM, Oracle Hyperion, PeopleSoft, J.D. Edwards EnterpriseOne, Oracle Business Intelligence – Enterprise Edition (OBIEE), Oracle Transportation Management, Oracle Value Chain Planning
OCPU (Compute and Database Systems)		Up to 30 OCPUs
Storage (Block and File System)		Up to 3,200 GB of storage
Database		VM Database Systems or Exadata Cloud Service
Compute		VM Compute
Number of RAC Nodes		Up to 2
Refresh data from the Production Environment		Once per month
Service Plan Update & Service Request Review Frequency		Quarterly
Account & Service Review Frequency		Quarterly
Availability Plan Frequency		Annually
Enhanced Recovery Services	RPO	1 hour (24 hours for Oracle Hyperion or OBIEE with Essbase)
	RTO	12 hours (24 hours for Oracle Hyperion or OBIEE with Essbase)
	Testing Frequency	Annual
Vulnerability Scans		12 per year

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Identify the Oracle Managed Applications, in accordance with the Service Maximums table.
2. Procure and maintain for the duration of the MEAC Services the Oracle Cloud for US Government components as determined by Oracle and documented in the *Managed Enterprise Application Cloud Minimum Architecture Requirements* (available at

<https://support.oracle.com> by searching on [Document ID 784630.1](#)) to provide adequate computing capacity for the performance of the Oracle Programs associated with the MEAC Services, including any required shared services.

3. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, Delivery Policies, and this Service Description.
4. Be responsible for release management, configuration management, performance management, Incident and Problem management for all CEMLI in the Services Environments.
5. Manage access and application responsibility privileges of all End Users of the Oracle Managed Applications and Third-Party Programs integrated with Your Oracle Managed Applications environment(s).
6. Acknowledge that (i) You have separately acquired and will continue to maintain for the duration of the MEAC Services the licenses and Oracle Software Update License & Support (also referred to as "Premier Support"), or any equivalent successor Oracle technical support offering, including availability of security patch updates (SPUs) and/or Critical Patch Updates (CPUs), for the Oracle Managed Applications and any other necessary Oracle programs, including those for which the Managed Services are provided, (ii) you will maintain licenses and technical support for any Third Party Software or Co-resident Third Party Programs used in your Environments, including availability of security updates, and (iii) your use of such programs and technical support are governed solely by the agreement(s) under which such licenses and technical support are obtained.
7. Procure and maintain for the duration of the MEAC Services, the quantity of licenses for the Oracle Database and/or subscription to Virtual Machine Database Systems or Exadata Cloud Service required to deliver the MEAC Services.
8. Perform post Refresh activities for the Oracle Managed Applications and Third-Party Software following a Refresh.
9. Provision and manage Your Third-Party Software other than Co-resident Third Party Programs integrated with Your Oracle Managed Applications environment(s), including the performance of such Third-Party Software.

Service Assumptions

1. Oracle will provide recommendations regarding sizing of Your Environments in accordance with the *Managed Enterprise Application Cloud Minimum Architecture Requirements* (available at <https://support.oracle.com> by searching on [Document ID 784630.1](#)) as required for Oracle to deliver the MEAC Services.
2. The MEAC Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Managed Enterprise Application Cloud – Additional Managed OCPU or Storage for US Government Cloud

MCS - Oracle Managed Enterprise Application Cloud – Additional Managed OCPU or Storage for US Defense Cloud

Part #	Service Offering
B109093	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud – Additional Managed OCPU
B109310	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud – Additional Managed OCPU
B109096	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud – Additional Managed OCPU, Configurable
B109313	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud – Additional Managed OCPU, Configurable
B109094	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud – Additional Managed Storage
B109311	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud – Additional Managed Storage
B109097	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud – Additional Managed Storage, Configurable
B109314	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud – Additional Managed Storage, Configurable

Description of Services

Oracle will provide the following Oracle Managed Enterprise Application Cloud – Additional Managed OCPU or Storage services (the “Services”):

1. Add Oracle managed compute and/or storage, as applicable, separately purchased by You, to the Services Environment in accordance with and to supplement the established maximums of one of the following services separately purchased by You (hereinafter “Pre-requisite Service”):

Pre-Requisite Service

Part #	Service Offering
B109092	MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud – Base
B109309	MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud – Base

The added compute and/or storage subject to the Service Maximums table below, may be used for activities to maintain required application architecture of the Services Environment, including, but not limited to the following:

- i. scale or burst the Pre-Requisite Service;
- ii. provision additional non-production environments; and
- iii. provision additional required middleware, such as SOA for Oracle E-Business Suite, Third Party Software integrated with Your application environment, and/or other additional shared services.

2. Provide architecture sizing guidelines to assist you with planning future architecture needs.
3. Service Level and availability management as described in the Service Description for the Pre-Requisite Service.
 - a. For purposes of calculating Service Levels, the monthly fees for the Services shall be added to the monthly fees defined in the Service Description for the Pre-Requisite Service.

Service Maximums

The Services are subject to the following constraints (the “Service Maximums”).

Service Maximums

Type	Quantity/Frequency	Quantity/Frequency
Usage Unit	1 OCPU	200 GB (Block or File System)

Cooperation and Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Purchase and maintain for the duration of the Services the Pre-Requisite Service.
2. Purchase the additional quantities of Oracle Cloud for US Government components in accordance with *Managed Enterprise Application Cloud Minimum Architecture Requirements* (available at <https://support.oracle.com> by searching on [Document ID 784630.1](#)).
3. Acknowledge that (i) you have separately acquired and will continue to maintain for the duration of the Services the licenses and Oracle Software Update License & Support (also referred to as “Premier Support”), or any equivalent successor Oracle technical support offering, including availability of security patch updates (SPUs) and/or Critical Patch Updates (CPUs), for necessary Oracle programs, including those for which the Managed Services are provided, (ii) you will maintain licenses and technical support for any Third Party Software or Co-resident Third Party Programs used in your Environments, including availability of security updates, and (iii) your use of such programs and technical support are governed solely by the agreement(s) under which such licenses and technical support are obtained.
4. Procure and maintain for the duration of the Services, the quantity of licenses for the Oracle Database and/or subscription to Virtual Machine Database Systems or Exadata Cloud Service required to deliver the Services.

Service Assumptions

1. Oracle will provide recommendations regarding sizing of Your Environments in accordance with the *Managed Enterprise Application Cloud Minimum Architecture Requirements* (available at <https://support.oracle.com> by searching on [Document ID 784630.1](#)) as required for Oracle to deliver the Services.
2. The Services do not include any activities that are not explicitly described in this Service Description.

MCS Oracle Managed Exadata Database Cloud Service for US Government Cloud

MCS Oracle Managed Exadata Database Cloud Service for US Defense Cloud

Part #:	Service Offering
B109113	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCS Standard Base per Rack
B109330	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCS Standard Base per Rack
B109110	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCS Bundled Base per Rack
B109327	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCS Bundled Base per Rack
B109111	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCS Cluster
B109328	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCS Cluster
B109112	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCS Managed Pluggable Database
B109329	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCS Managed Pluggable Database
B109109	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCC Standard Base per Rack
B109326	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCC Standard Base per Rack
B109106	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCC Bundled Base per Rack
B109323	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCC Bundled Base per Rack
B109107	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCC Cluster
B109324	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCC Cluster
B109108	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCC Managed Pluggable Database
B109325	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCC Managed Pluggable Database
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle will provide the following Oracle Managed Exadata Database Cloud Service (the “Exa DB Services”) for the Oracle’s database software executing with Oracle Database Exadata Cloud (ExaDB) Service on Oracle Cloud for US Government for which You have separately purchased a subscription (“Your Subscription”). The Exa DB Services are available only for the Exadata physical racks, VM clusters, and Pluggable Databases (PDBs) identified in the Managed Services Exhibit for Your Subscription (the “Managed Exa DB Environments”):

1. Provision and configure the Managed Exa DB Environments with network connectivity in accordance with the Managed Services Exhibit and the Service Maximums table.
2. Apply routine patches and updates of the compute node user domain (DomU).
3. Use the assigned Oracle Cloud Administrator roles and privileges to provide the Exa DB Services as described in the following Sections of [Exhibit 1: Oracle Managed Services for Oracle Cloud for US Government Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#) for Exa DB Services programs and Co-resident Third Party Programs.
 - b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#), consisting of managing administrative access for Your Subscription using the

Oracle Cloud Administrator role, including the following activities/tasks in accordance with the Maintenance Frequency Table below:

- i. Setting up new users and application privileges for each Exa DB Environment.
- ii. Administration (adding, removing, and changing) of users and application privileges for each Exa DB Environment
- c. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#), consisting of the following activities/tasks upon Your request in accordance with the Service Maximums Table below or at Oracle's sole discretion for events associated with critical or urgent business requirements:
 - i. Installation, configuration, and administration of the Exa DB Services software components and the Exa DB Environments
 - ii. Change tasks to existing configurations of the Exa DB Services and database connections
 - iii. Scaling or bursting of the compute capacity for Your Exa DB Environment.
 - iv. Installation of software patches which repair or modify existing functionality or maintain alignment with current business requirements.
 - v. Configure and monitor database High Availability ("HA") components.
- d. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#), including networking, platform, user, and task configurations in accordance with the Frequency Table.
- e. [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#), consisting of planning deployments of quarterly updates to the Exa DB Services and associated Oracle software that are intended to improve performance, security, availability, stability, manageability, or regulatory compliance. Bundled task and configuration changes may be deployed during maintenance windows requested by You and subject to the constraints identified in the Service Maximums table.
- f. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#), consisting of response and resolution of individual incidents, associated Service Request (SR) tracking, problem identification, and Root Cause Analysis.
- g. [Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy](#), using monitoring features that are made available a part of the Exa DB Services.
- h. [Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#) for Your Subscription.
- i. [Oracle Managed Services for Oracle Cloud for US Government Continuity Policy](#), including (i) weekly full and daily incremental backups and (ii) retention of archive logs for 30 days, limited to Production Environments and Production Support Environments, and requiring object storage for backups provided by You, which is usually 7 times the amount of database storage in use.
- j. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)

- k. [Oracle Managed Services for Oracle Cloud for US Government Service level and Availability Management Policy](#), excluding Service Request Resolution Time Service Level and including the following:

- **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
- **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.
- **Service Level Credit %.** The percentage of monthly recurring fees paid by You for the EXA DB Services to be credited based on the credit criteria.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
Platform Availability	99.5%	<99.5%	10%
	99.7% ¹	<99.7%	
Performance Against Service Description	Performance of the Exa DB Services in accordance with this section	As described in this Service Description	As indicated below

¹ Requires deployment on RAC at a primary and secondary data center and Oracle Database Exadata Cloud Service – Extreme Performance Edition with Oracle Active DataGuard

Platform Availability Service Level

The Platform Availability Service Level consists of the measurement of the percentage of time that the individual Managed Exa DB Environment is available for access and use by You to conduct production business operations (“Production Exa DB Environment”), and are measured by Oracle on a monthly basis and calculated in accordance with the following formula:

$$\left\{ \frac{\begin{aligned} &[\text{Total minutes in a calendar month} \times \text{number of Production Exa DB Environments} \\ &- \text{Sum of Unplanned Outage (caused by Exa DB Service failure)} \\ &\text{minutes measured for each Production Exa DB Environment in such month}] \end{aligned}}{\text{Total minutes in the calendar month} \times \text{number of Production Exa DB Environments}} \right\} \times 100$$

Only Severity Level 1 Unplanned Outages caused by Exa DB Services failures of a Production Exa DB Environment shall be used to calculate Oracle’s monthly performance against the Exa DB Environment Availability Service Level.

Incidents for which the root cause is subject to exclusion per [Oracle Managed Services Delivery Policies](#) or that occur in a Production Exa DB Environment during a Stabilization Period shall not be included in the Exa DB Environment Availability calculation. A Production Exa DB Environment must have at least one associated Production Support Environment for service level credits to be applicable.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the total fees paid by You for the specific Service for the month in which the Service Level Credit accrued, MINUS any Service Level Credit earned under the Exa DB Environment Availability Service Level in connection with the Exa DB Services provided in such month.

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the Exa DB Services for the month in which the Service Level Credit accrued.

Service Maximums

The Exa DB Services are subject to the following constraints (“Service Maximums”).

Service Maximums

Type	Quantity/Frequency		
	< 10 PDBs	>=11 and <50 PDBs	> 51 PDBs
Scaling requests per month	One (1)	Two (2)	Four (4)
Patching requests	One per quarter for each DomU + PDB		
High availability (HA) and Disaster Recovery (DR) Configuration	Two (2) per contract year		
Deployment Configuration	Single or multiple instance(s), non-clustered or clustered		
RAC	Included (with Enterprise Edition Extreme Performance Subscription or Oracle Active Data Guard (ADG) license for bring your own license (BYOL) Oracle Maximum Availability Architecture (Oracle MAA))		
Database Encryption	- Initial Transparent Data Encryption (TDE) configuration and Oracle Wallet configuration - One (1) key rotation per year for TDE databases (Keys are maintained in Oracle Wallet)		
Service Plan Update & Service Request Review Frequency	Quarterly		
Account & Service Review Frequency	Annual		
Availability Plan Frequency	Annual		

Supplemental Resources

If included in Your order, Oracle will provide additional resources, either on-site or remotely, up to the number of days¹ per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for *Oracle Managed Exadata Database Cloud Service for US Government Cloud or US Defense Cloud*:

1. Coordination and planning of Initiation Phase activities

2. Assistance with SRs related to the following:
 - a. Issue reproduction
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. For MCS - Oracle Managed Oracle Exadata Database Cloud Service for US Government Cloud – ExaCS Bundled Base per Rack (part # B109110) and ExaCC Bundled Base per Rack (part # B109106) or MCS - Oracle Managed Oracle Exadata Database Cloud Service for US Defense Cloud – ExaCS Bundled Base per Rack (part # B109327) and ExaCC Bundled Base per Rack (part # B109323) purchase and maintain for the duration of the Exa DB Services one or more of the following services (the “Pre-requisite Service”):

Part #	Service Offering
B109115	MCS - Oracle Managed Analytics Cloud Service for US Government Cloud – Standard Base
B109332	MCS - Oracle Managed Analytics Cloud Service for US Defense Cloud – Standard Base
B95474	MCS - Oracle Managed Application Cloud for US Government Cloud - Custom
B109092	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud - Base
B109309	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud - Base

2. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, [Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#), and this service description.
3. Procure and maintain for the duration of the Exa DB Services adequate capacity for the performance of the Exa DB Services and Your Subscription.
4. Perform all required end-2-end testing to validate that the Exa DB Service platform is configured securely, and correctly.
5. Separately purchase services to migrate content to the Managed Exa DB Environments, if required and subject to additional fees.
6. Develop applications and application logic.
7. Provide support and assistance to Oracle as required to perform the assigned Oracle Cloud Administrator roles and privileges.
8. Provide support and documented requirements to Oracle as necessary for Oracle to manage and configure the Managed Exa DB Environments.
9. Separately purchase upgrades for the database software subject to additional fees.

Service Assumptions

1. The Exa DB Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Managed IaaS Service for US Government Cloud

MCS - Oracle Managed IaaS Service for US Defense Cloud

Part #:	Service Offering
B109099	MCS - Oracle Managed IaaS Service for US Government Cloud – Standard Base
B109316	MCS - Oracle Managed IaaS Service for US Defense Cloud – Standard Base
B109100	MCS - Oracle Managed IaaS Service for US Government Cloud – OCPU
B109317	MCS - Oracle Managed IaaS Service for US Defense Cloud – OCPU
B109098	MCS - Oracle Managed IaaS Service for US Government Cloud – Bundled Base
B109315	MCS - Oracle Managed IaaS Service for US Defense Cloud – Bundled Base
B109120	MCS – Oracle Managed Services Supplemental Resources for US Government Cloud – Day
B109337	MCS – Oracle Managed Services Supplemental Resources for US Defense Cloud – Day

Description of Services

Oracle will provide the following Oracle Managed IaaS Service on Oracle Cloud for US Government (the “Services”) for virtual machines, operating systems, virtual cloud networking, and any related services or software included with Your separately purchased Oracle Infrastructure as a Service subscription (“Your Subscription”):

1. Provision and manage guest virtual machines (“Guest VMs”) and associated operating systems (“OS”), including, but not limited to, compute and storage, memory, and network connectivity, as applicable.
2. Make changes to the Guest VMs upon Your request (“Guest VM Provisioning Requests”), in accordance with the Service Maximums table (Service Maximums) below.
3. Provide the Services for the Guest VMs and associated OS as described in the following Sections of [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#).
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#)
 - b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#), consisting of management and control of access to infrastructure accounts, including OS accounts, providing administrative access where applicable, and creating and managing compartments in accordance with the Periodic Maintenance Plan table in Section A.3.e below.
 - c. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#), consisting of the following:
 - i. Installation and/or configuration of Oracle infrastructure software, including software required to provision operating system images using an Oracle Cloud Infrastructure image.
 - ii. Infrastructure and OS patches which repair or modify existing functionality or maintain currency alignment with business requirements (“Patch Application Requests”). Patch Application Requests may be applied during the maintenance windows specified in the Periodic Maintenance Plan table or, at Oracle’s sole discretion for events associated with critical or urgent business requirements. The

number of Patch Application Requests may not exceed the quantity specified in the Service Maximums table.

- d. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#), including networking, virtual machine, and operating system configurations, in accordance with the Periodic Maintenance Plan table.
- e. [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#), consisting of planning deployments of Guest VMs, networking, and operating system updates that are intended to improve performance, security, availability, stability, manageability, or regulatory compliance. Bundled updates are deployed during maintenance windows at a frequency based on the quantity of MCS - Oracle Managed IaaS Service for US Government Cloud – OCPU (part # B109100) or MCS - Oracle Managed IaaS Service for US Defense Cloud – OCPU (part # B109317) purchased by You, as indicated in the following Periodic Maintenance Plan table.

Periodic Maintenance Plan

	Maximum Available Maintenance Window Frequency		
	Quantity of MCS - Oracle Managed IaaS Service for US Government Cloud – OCPU (Part # B109100) or MCS - Oracle Managed IaaS Service for US Defense Cloud – OCPU (Part # B109317)		
Maintenance Window	< 50	>=50 and <200	>=200
Change Management	2 per month	5 per month	8 per month
Access Management	2 per month	5 per month	8 per month
OS Configuration	2 per month	5 per month	8 per month
Network Configuration	2 per month	5 per month	8 per month

- f. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#), consisting of response and resolution of individual incidents, associated Service Request (SR) tracking, problem identification, and Root Cause Analysis.
- g. [Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy](#), consisting of Guest VM monitoring, including networking, virtual machines, and operating systems.
- h. [Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#) for Your Subscription.
- i. [Oracle Managed Services for Oracle Cloud for US Government Continuity Policy](#), consisting of VM image backup (“VM Image Backup”) and volume level restore of the VM image from backup (“VM Image Restore”) in accordance with the Service Maximums table.
- j. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)
- k. [Oracle Managed Services for Oracle Cloud for US Government Service level and Availability Management Policy](#), excluding Application Availability, and including the following:

- **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
- **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.
- **Service Level Credit %.** The percentage of monthly recurring fees paid by You for the Services to be credited based on the credit criteria.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
Infrastructure Availability	99.5%	<99.5%	10%
Service Request Resolution Time	4 hours (Unplanned Outage caused by infrastructure and/or component)	<90% of SRs resolved within target	3%
Performance Against Service Description	Performance of the Services in accordance with this section	As described in this Service Description	As indicated below

Infrastructure Availability Service Level

The Infrastructure Availability Service Level consists of the measurement of the percentage of time that the Guest VMs are available for access and use by You to conduct production business operations (“Production Guest VMs”), and are measured by Oracle on a monthly basis and calculated in accordance with the following formula:

$$\left\{ \frac{\begin{aligned} &[\text{Total minutes in a calendar month} \times \text{number of Production Guest VMs}] \\ &- \text{Sum of Unplanned Outage (caused by component or infrastructure failure)} \\ &\text{minutes measured for each Production Guest VMs in such month} \end{aligned}}{\text{Total minutes in the calendar month} \times \text{number of Production Guest VMs}} \right\} \times 100$$

Only Severity Level 1 Unplanned Outages caused by Infrastructure and/or component failures of a Production Guest VM shall be used to calculate Oracle’s monthly performance against the Infrastructure Availability Service Level.

Incidents for which the root cause is subject to exclusion per Appendix 1 (Oracle Managed Services Delivery Policies) or that occur in a Production Guest VM environment during a Stabilization Period shall not be included in the Infrastructure Availability calculation.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the total fees paid by You for the Services for the month in

which the Service Level Credit accrued, MINUS any Service Level Credit earned under the Infrastructure Availability Service Level MINUS any Service Level Credit earned under the Service Request Resolution Time Service Levels in connection with the Services provided in such month.

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the Services for the month in which the Service Level Credit accrued.

Service Maximums

The Services are subject to the following constraints ("Service Maximums").

Service Maximums

Type	Quantity/Frequency
Patch Application Requests	One (1) per month for each VM provided with Your Subscription
Guest VM Provisioning Requests	Up to five (5) per month for every ten (10) MCS - Oracle Managed IaaS Service for US Government Cloud – OCPUs (Part # B109100) or MCS - Oracle Managed IaaS Service for US Defense Cloud – OCPUs (Part # B109317) purchased by You
VM Image Backup	Weekly
VM Image Backup Retention Period	30 days
VM Image Restore	One (1) per month for every ten (10) MCS - Oracle Managed IaaS Service for US Government Cloud – OCPUs (Part # B109100) or MCS - Oracle Managed IaaS Service for US Defense Cloud – OCPUs (Part # B109317) purchased by You
Service Plan Update & Service Request Review Frequency	Quarterly
Account & Service Review Frequency	Annual
Availability Plan Frequency	Annual

Supplemental Resources

If included in Your order, Oracle will provide additional resources, either on-site or remotely, up to the number of days¹ per resource role set forth in Your order ("Supplemental Resources") to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for *Oracle Managed IaaS Services for US Government Cloud or US Defense Cloud*:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Issue reproduction
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR

3. Account and Service Reviews

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. For MCS - Oracle Managed IaaS Service for US Government Cloud – Bundled Base service (part #B10908) or MCS - Oracle Managed IaaS Service for US Defense Cloud – Bundled Base service (part #B109315) , purchase and maintain for the duration of the Services one or more of the following services (the “Pre-requisite Service”):
 - a. The following:

Part #	Service Offering
B109115	MCS – Oracle Managed Analytics Cloud for US Government Cloud – Standard Base
B109332	MCS – Oracle Managed Analytics Cloud for US Defense Cloud – Standard Base
B95474	MCS - Oracle Managed Application Cloud for US Government Cloud, Custom
B109092	MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud- Base
B109309	MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud- Base
B109109	MCS – Oracle Managed Exadata Database Cloud Service for US Government Cloud – ExaCC Standard Base per rack
B109326	MCS – Oracle Managed Exadata Database Cloud Service for US Defense Cloud – ExaCC Standard Base per rack
B109113	MCS – Oracle Managed Exadata Database Cloud Service for US Government Cloud – ExaCS Standard Base per rack
B109330	MCS – Oracle Managed Exadata Database Cloud Service for US Defense Cloud – ExaCS Standard Base per rack

- b. Any service/part number described by the following service descriptions within this *Oracle Managed Services for Oracle Cloud for US Government Service Description* document
 - i. MCS - Oracle Managed Applications Unlimited for US Government Cloud Services
 - ii. MCS - Oracle Managed Applications Unlimited for US Defense Cloud Services
 - iii. Oracle Managed Services IaaS and PaaS for US Government Cloud Services
 - iv. Oracle Managed Services IaaS and PaaS for US Defense Cloud Services
2. Be responsible for Your, Your Users’ and Your third parties’ use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, the Delivery Policies, and this service description.
3. Procure and maintain for the duration of the Services: adequate compute, storage, and networking capacity, and an Oracle Infrastructure as a Service subscription.
4. Procure and maintain for the duration of the Services the amount of object storage required for VM Image Backup, retention of VM Image Backups, and VM Image Restore.
5. Use the access privileges provided by Oracle to install and manage Your applications.
6. Be responsible for provisioning and managing Third Party Software other than Co-resident Third Party Programs, including the performance of such Third Party Software.

7. Acknowledge that operating system major release upgrades are not included in the Services and that You must separately purchase such services.

Service Assumptions

1. The Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Managed Identity and Access Management for US Government Cloud, Foundation

MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Foundation

Part #:	Service Offering
B111185	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Foundation
B111199	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Foundation
B95471	MCS-Oracle Managed Cloud Services Supplemental Resources-Senior Security Engineer – United States - Day

Description of Services

Oracle Managed Identity and Access Management, Foundation (“the Services”) consists of the following services for Your web-enabled applications utilizing OCI Identity and Access Management Identity Domains (the “OCI IAM Domains”) in accordance with the Managed Services Exhibit:

1. Designate a resource who will serve as Your primary point of contact to facilitate account management and service reviews.
2. Renew SAML signing certificates upon expiry and re-configure federation with new certificates in each of Your OCI IAM Domains.
3. Reconfigure SAML, Open ID, and SCIM connections with web applications as required during post refresh of applications in each of Your OCI IAM Domains.
4. Update Active Directory Bridge configurations as required for any customer Active Directory domain changes.
5. Advise You on User and User group management in OCI IAM Domain administration console.
6. Provide level 3 triage, troubleshooting, configuration fixes, and escalation support for Incidents related to the OCI IAM Domains.
7. Evaluate Oracle’s product development release schedules for Your OCI IAM Domains and make recommendations for configuration changes.
8. Use the OCI IAM Domain administration role to provide the Services as described in the following sections of [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#)
 - b. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy, consisting of change tasks to existing OCI IAM Domain configurations, excluding user administration tasks](#)
 - c. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#)
 - d. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#)

- e. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)
- f. [Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy](#)

Supplemental Resources

If included in Your order, Oracle will provide additional remote resources, up to the number of days per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for Oracle Managed Identity and Access Management, Foundation:

1. Coordination and planning of Initiation Phase activities.
2. Assistance with SRs related to the following:
 - a. Troubleshoot, escalation support and configuration fix
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Procure and maintain for the duration of the Services an OCI Identity and Access Management service subscription for the production OCI IAM Domain and production support OCI IAM Domain.
2. Provide Oracle with the Active Directory connection details.
3. Provide the SAML metadata of Your identified web applications for federated single sign on (SSO).
4. Provide a set of users to be configured in OCI IAM Domains as delegated user administrators.
5. Be responsible for user and user group administration in Your OCI IAM Domains and identified web applications integrated for federated SSO.
6. Be responsible for Your, Your Users’ and Your third parties’ use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, and this Service Description.
7. Provide level 1 and level 2 incident management support.
8. Use Oracle’s ticketing system to raise Service Requests and Requests for Change related to the Services.

MCS - Oracle Managed Identity and Access Management for US Government Cloud

MCS - Oracle Managed Identity and Access Management for US Defense Cloud

Part #:	Service Offering
B111186	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Standard
B111200	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Standard
B111187	MCS – Oracle Managed Identity and Access Management for US Government Cloud, Foundation Plus
B111201	MCS – Oracle Managed Identity and Access Management for US Defense Cloud, Foundation Plus
B95471	MCS-Oracle Managed Cloud Services Supplemental Resources-Senior Security Engineer – United States – Day
B109120	MCS – Oracle Managed Services Supplemental Resources for US Government Cloud – Day
B109337	MCS – Oracle Managed Services Supplemental Resources for US Defense Cloud – Day

Description of Services

Oracle Managed Identity and Access Management, Standard (“the Services”) consists of the following services for Your web-enabled applications utilizing OCI Identity and Access Management (“OCI IAM”) Identity Domains (the “OCI IAM Domains”) in accordance with the Managed Services Exhibit:

1. Designate a resource who will serve as Your primary point of contact to facilitate account management and service reviews.
2. Provide You with access URLs and administrative usernames and passwords for OCI IAM Domains.
3. Configure and enable the following for Your OCI IAM Domains, as required:
 - a. Synchronization of identities between Your Active Directory domain and the OCI IAM Domain repository;
 - b. Security Assertion Markup Language 2.0 (“SAML2”) compliant federated single sign-on or Open ID single sign-on for web applications identified by You;
 - c. Cross-domain Identity Management (SCIM) compliant web applications integration for user identity lifecycle management;
 - d. Multi-factor authentication of Your SAML2 integrations with web applications identified by You (the “SAML2 Integrations”);
 - e. Delegation of security and user administration capabilities for users identified by You;
 - f. Sign-in page and email template with branding logos provided by You;
 - g. Audit reports for user login and application access attempts;
 - h. Password policy in accordance with security requirements provided by You;
 - i. Network perimeters with a list of IP addresses identified by You and corresponding sign-on policies to either deny (blacklist) or allow (whitelist) access;
 - j. Adaptive security to analyze a user’s risk profile based on historical behavior and to enforce an appropriate remediation action, such as allowing or denying the user from accessing protected applications and resources or requiring the user to provide a second factor authentication;

- k. Multi-Factor Authentication using available authentication factors of mobile app passcode, mobile app notification, security questions, text message (SMS), email, bypass code and duo security;
 - l. Integration with any one of the social identity providers Facebook, Google, LinkedIn, Microsoft, OpenID Connect, and Twitter to enable users to log into OCI IAM Domains with social credentials;
 - m. Single sign-on using SAML for collaboration tools Slack, Zoom, Office 365, and Citrix.
4. Assist You with issues related to the Services identified during Your User Acceptance Testing (UAT).
 5. Upon Your successful completion and signoff of UAT, migrate configurations to Your production OCI IAM Domain.
 6. Evaluate Oracle's product development release schedules for Your OCI Identity and Access Management service and make recommendations for configuration changes.
 7. Provide level 3 triage, troubleshooting, and escalation support for Incidents related to the Services.
 8. Renew SAML signing certificates upon expiry and re-configure federation with new certificates in each of Your OCI IAM Domains.
 9. Reconfigure SAML, Open ID, and SCIM connections with web applications as required during post refresh of applications in each of Your OCI IAM Domains.
 10. Update Active Directory bridge configurations as required for any customer Active Directory domain changes.
 11. Advise You on User and User Group management in OCI IAM Domain administration console.
 12. Use the OCI IAM Domain administration role to provide the Services as described in the following Sections of [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#) for the Services
 - b. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#), consisting of Change tasks to existing OCI IAM Domain configurations, excluding user administration tasks, upon Your request in accordance with the Administrative Changes Per Month as defined in the Service Maximums table:
 - c. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#)
 - d. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#)
 - e. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)
 - f. [Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy](#).

Service Maximums

The Services are subject to the following constraints ("Service Maximums").

If You have purchased B111187 - MCS – Oracle Managed Identity and Access Management for US Government Cloud, Foundation Plus or B111201 - MCS – Oracle Managed Identity and Access Management for US Defense Cloud, Foundation Plus then your applicable Service Maximums are documented in the Managed Services Exhibit.

Type	Quantity/Frequency
Service Delivery Reviews	Quarterly
OCI IAM Domains	2 (Production and Production Support)
SAML2 Integrations	8
Active Directory domains	1

Supplemental Resources

If included in Your order, Oracle will provide additional remote resources, up to the number of days per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for Oracle Managed Identity and Access Management:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Troubleshooting, escalation support, and configuration fixes
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews
4. Configuration of Your OCI IAM Domains related to the following:
 - a. User identity synchronization between OCI IAM and supported enterprise applications
 - b. Single sign-on and provisioning connectors deployed on OCI
 - c. Authentication and authorization functions in OCI IAM administrative console
5. Guidance on OCI IAM deployment and configuration

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Procure and maintain for the duration of the Services an OCI Identity and Access Management service subscription for the production OCI IAM Domain and production support OCI IAM Domain.
2. Provide Oracle the Active Directory connection details.
3. Provide the SAML metadata of Your identified web applications for federated single sign on (SSO).
4. Provide a set of users to be configured in OCI IAM Domains as delegated user administrators.

- 
5. Be responsible for user administration in Your identified web applications integrated for federated SSO.
 6. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, and this Service Description.
 7. Provide level 1 and level 2 incident management support for Incidents related to the Services.
 8. Use Oracle's ticketing system to raise Service Requests and Requests for Change related to the Services.

MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced

MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced

Part #	Service Offering
B111188	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced
B111202	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced
B111189	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced Plus
B111203	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced Plus
B95471	MCS-Oracle Managed Cloud Services Supplemental Resources-Senior Security Engineer – United States - Day
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle Managed Identity and Access Management, Advanced (the “Services”) consists of the following managed identity and identity governance services for (i) Your web-enabled applications utilizing Oracle’s Identity and Access Management Identity Domains (“OCI IAM Domains”), and Oracle’s Identity Governance program (“OIG”) installed on Oracle Cloud Infrastructure (“OCI”) and (ii) Your OIG Environments integrated with OCI IAM Domains.

1. Designate a resource who will serve as Your primary point of contact to facilitate account management and service reviews.
2. Installation of OIG as required for the OCI IAM Domains.
3. Provide You with access URLs and administrative usernames and passwords as required for the Services
4. Configure and enable the following for Your OCI IAM Domains, as required:
 - a. Synchronization of identities between Your Active Directory domains and the OCI IAM Domain repository;
 - b. Security Assertion Markup Language (“SAML2”) compliant federated single sign-on for the web applications identified by You;
 - c. Multi-factor authentication of SAML2 integrations with web applications identified by You (the “SAML2 Integrations”);
 - d. Delegation of security and user administration capabilities for users identified by You; all OIG users will be managed under one OIG organization container, approver and certifier information will be managed in OIG as part of the OIG catalog data;
 - e. Sign-in page with branding logos provided by You;
 - f. OIG email templates with branding logos (the “Email Notification Template”) provided by You;
 - g. Audit reports of user login and application access attempts;
 - h. Password policy in accordance with security requirements provided by You;
 - i. Network perimeters with a list of IP addresses identified by You and corresponding sign-on policies to either deny (blacklist) or allow (whitelist) access;

- j. Adaptive security to analyze a user's risk profile based on historical behavior and to enforce an appropriate remediation action, such as allowing or denying the user from accessing protected applications and resources or requiring the user to provide a second factor authentication;
 - k. Multi-Factor Authentication using available authentication factors of mobile app passcode, mobile app notification, security questions, text message (SMS), email, bypass code and duo security;
 - l. Integration with any one of the social identity providers Facebook, Google, LinkedIn, Microsoft, OpenID Connect, and Twitter to enable users to log into OCI IAM Domains with social credentials;
 - m. Single sign-on using SAML for collaboration tools Slack, Zoom, Office 365, and Citrix.
5. Renew Security Assertion Markup Language (SAML) signing certificates upon expiry and re-configure federation with new certificates.
 6. Configure OIG, integrated with OCI IAM Domains, for the following:
 - a. Provisioning and reconciliation of accounts and groups using OCI IAM Domain connector.
 - b. Development of a custom identity connector in OIG (the "Custom Connector") for the onboarding of the target applications (the "Target Applications") in accordance with the Service Maximums table.
 - c. Integration with trusted authoritative sources to reconcile identity lifecycle events related to onboarding and off boarding of users (the "Trusted Authoritative Data Source").
 - d. Definition of named sets of parameters used to review user entitlements and access privileges (the "Certification Definitions") and certification campaigns for users, roles, and entitlements.
 - e. Segregation of duties violation checks of roles and entitlements for the number of identity audit rules in accordance with the Service Maximums table (the "Identity Audit Rules").
 - f. Approval workflows and policies for self-service requests (the "Self-Service Approval Workflows") for up to three email notifications to requesters, application owners, and managers regarding pending actions.
 - g. User, role, and entitlement reporting capabilities based on standard OIG report templates included with the OIG program.
 - h. A request catalogue to be populated with entitlements, roles, and Target Applications
 - i. Organizations and business duties and/or responsibilities to be granted to users in an organization ("Business Roles") identified by You.
 7. Perform a Production Assessment of the OIG integration with OCI IAM Domains.
 8. Assist You with issues related to the Services identified during Your User Acceptance Testing ("UAT").
 9. Upon Your successful completion and signoff of UAT, migrate the configurations to Your Production Environment.
 10. Evaluate Oracle's product development release schedules for Your Identity Cloud Service and make recommendations for configuration changes.

11. Evaluate product development release schedules and software certification for OIG and make recommendations for upgrades and patches.
12. Provide You with the following services for OIG on Oracle Cloud Infrastructure as described in the [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#)
 - b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#)
 - c. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#)
 - d. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#)
 - e. [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#)
 - f. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#)
 - g. [Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy](#)
 - h. [Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy](#), except for backup and removal of any software.

Service Maximums

The Services are subject to the following constraints ("Service Maximums").

Service Maximums

Maximums	MCS - Oracle Managed Identity and Access Management, Advanced	MCS - Oracle Managed Identity and Access Management, Advanced Plus
	B111188 B111202	B111189 B111203
Service Delivery Reviews	Quarterly	Quarterly
OIG/OCI IAM Domains	2 (Production and Production Support)	3 (Production, Production Support, Non-Production)
Application Environments	3 (Production, Production Support, or Non-Production)	4
Trusted Authoritative Data Sources	1	2
Target Applications	5	10
Business Roles	5	10
Certification Definitions	1	3
Identity Audit Rules	0	15
Self-service Approval Workflows	1	2

Maximums	MCS - Oracle Managed Identity and Access Management, Advanced	MCS - Oracle Managed Identity and Access Management, Advanced Plus
	B111188 B111202	B111189 B111203
Email Notification Templates	5	10
Custom Connectors	0	1
SAML2 Integrations	5	15

Supplemental Resources

If included in Your order, Oracle will provide additional resources, remotely, up to the number of days per resource role set forth in Your order ("Supplemental Resources") to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for Oracle Managed Identity and Access Management, Advanced or Advanced Plus:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Troubleshoot escalation support and configuration fix
 - b. Constructing a reproducible test case
 - c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews
4. Configuration of Your OCI IAM Domains related to the following:
 - a. Authentication and authorization functions in OCI IAM administrative console
 - b. User Identity synchronization between OCI IAM and supported enterprise applications
 - c. Provisioning and governance functions in OIG administrative console
 - d. Single sign-on and provisioning connectors deployed on OCI
5. Guidance on OCI IAM deployment and configuration

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Procure and maintain for the duration of the Services the following:
 - a. The amount of Oracle Compute Cloud Service and Oracle Storage Cloud Service required to provide adequate computing capacity for the performance of OIM associated with the Services
 - b. Oracle Identity Governance license
 - c. Oracle Database licenses as required for the Services
 - d. Oracle Identity and Access Management Cloud Service subscriptions for production, production support, and development OCI IAM Domains, as required

2. Provide to Oracle the Active Directory connection details.
3. Provide to Oracle the target application environments connection details.
4. Provide to Oracle Business Roles to be defined in OIG.
5. Provide the SAML metadata of any web applications hosted by You for federated single sign-on.
6. Provide a list of approvers to be configured in the self-service approval workflows.
7. Provide a list of certification reviewers to be configured in Certification Definitions.
8. Provide a list of rules to be defined for Segregation of Duties violation checks.
9. Provide cleansed and high quality identity data sets that mirror production data for the purpose of UAT in the production support OCI IAM Domain.
10. Provide data such as business classification and tagged entitlements and roles to enrich the request catalog data.
11. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, and this Service Description.
12. Use Oracle's ticketing system to raise Service Requests and/or Requests for Change related to the Services.

Service Assumptions

1. The Services do not include fetching approver and certifier data from external systems.
2. The Services do not include advanced configuration and customization of OIG, such as creation of custom OIG UDFs (User defined fields) to capture Your company specific identity attributes, implementation of post processing rules using Event Handlers, pre-populate adapters, process task adapters and scheduled jobs.
3. The Services are not available for Disaster Recovery Environments in accordance with the Service Maximums table.
4. A Custom Connector is any connector that is not listed at <http://www.oracle.com/technetwork/middleware/id-mgmt/downloads/connectors-101674.html>

MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced – Enhanced Recovery Service

MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced – Enhanced Recovery Service

Part #	Service Offering
B111190	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced – Enhanced Recovery Service
B111204	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced – Enhanced Recovery Service

Description of Services

Oracle Managed Identity and Access Management, Advanced – Enhanced Recovery Service (“the Services”) consists of:

1. Enhanced Recovery Services for Oracle Identity Governance as described in the [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#) and in accordance with and to supplement the established maximums of the following services separately purchased by You (hereinafter “Pre-requisite Service”):

Pre-requisite Service

Part #	Service Offering
B111188	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced
B111202	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced
B111189	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced Plus
B111203	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced Plus

Service Maximums

The Services are subject to the following constraints (“Service Maximums”).

Service Maximums		
Enhanced Recovery Services	RPO	1 hour
	RTO	12 hours
	Testing Frequency	Annual

Your Obligations

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Procure and maintain for the duration of the Services the following:

- 
- a. The amount of Oracle Compute Cloud Service and Oracle Storage Cloud Service required to provide adequate computing capacity for the performance of OIG associated with the Services;
 - b. Oracle's Identity Governance license;
 - c. Oracle Database licenses, as required for the Services;
 - d. One of the Pre-requisite Services listed above.

MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited Connector

MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited Connector

Part #	Service Offering
B111191	MCS - Oracle Managed Identity and Access Management for US Government Cloud – Integrated Applications Unlimited Connector – Managed Hosted Environment
B111205	MCS - Oracle Managed Identity and Access Management for US Defense Cloud – Integrated Applications Unlimited Connector – Managed Hosted Environment

Description of Services

Oracle will install, configure, and manage one or more of the following Oracle Identity and Access Management connectors (the “Connector(s)”) as required to integrate one (1) of Your web-enabled Applications Unlimited programs (the “Integrated Application”) with OCI Identity and Access Management service (cumulatively, the “Services”):

- Oracle E-Business Suite Asserter (“EBS Asserter”)
- Oracle Application Gate (“App Gate”)

Oracle will provide the following as part of the Services:

1. Provide the services below to supplement one or more of the following services separately purchased by You (hereinafter “Managed Application Pre-requisite Service”):

Managed Applications Pre-requisite Service

Part #	Service Offering
B95474	MCS - Oracle Managed Application Cloud for OCI Government Cloud – United States, Custom
B109092	MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud - Base
B109309	MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud - Base
B109091	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two Minimum Complexity
B109308	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two Minimum Complexity
B109090	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two Low Complexity
B109307	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two Low Complexity
B109089	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two High Complexity
B109306	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two High Complexity
B109088	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier One Minimum Complexity

Part #	Service Offering
B109305	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier One Minimum Complexity
B109087	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier One Low Complexity
B109304	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier One Low Complexity
B109086	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier One High Complexity
B109303	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier One High Complexity

- Services below are intended to supplement one or more of the following services separately purchased by You (hereafter “Managed Identity and Access Management Pre-Requisite Service”):

Managed Identity and Access Management Pre-Requisite Service

Part #	Service Offering
B111186	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Standard
B111200	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Standard
B111185	MCS – Oracle Managed Identity and Access Management for US Government Cloud, Foundation
B111199	MCS – Oracle Managed Identity and Access Management for US Defense Cloud, Foundation
B111187	MCS – Oracle Managed Identity and Access Management for US Government Cloud, Foundation Plus
B111201	MCS – Oracle Managed Identity and Access Management for US Defense Cloud, Foundation Plus
B111188	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced
B111202	MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Advanced
B111189	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced Plus
B111203	MCS - Oracle Managed Identity and Access Management for US Government Cloud, Advanced Plus

- Install either EBS Asserter on Oracle Java Cloud Service ("JCS") or App Gate on Oracle Cloud Infrastructure (each referred to herein as the “Connector Environment”) for up to two (2) Connector Environments as required for the integration between Oracle Identity and Access Management Identity Domains (“OCI IAM Domains”) and Your Integrated Application (the “Connector Integration”).
- Upon successful installation of the Connector Environment(s), enable the Connector Integration for up to two (2) OCI IAM Domains.

5. Designate a resource who will serve as Your primary point of contact to facilitate account management and service reviews.
6. Perform quarterly Service Delivery Reviews.
7. Provide You with architecture, a data flow diagram, and sizing recommendations for the Connectors.
8. Set the Connector as a confidential application for authentication into OCI IAM Domains.
9. Configure access policies in the Connector for single sign-on authentication.
10. Perform Production Assessment activities for Connector Integration with OCI IAM Domains.
11. Assist You with issues identified during Your User Acceptance Testing (“UAT”) of the Connector Integration.
12. Upon Your successful completion of UAT and Your sign off, migrate the configurations to the Production Environment.
13. Evaluate product development release schedules for the Connector and make recommendations for configuration changes.
14. Evaluate product development release schedules and software certification for the Connector and make recommendations for upgrades and patches.
15. Provide You with the following lifecycle management services for the Connector installed on Oracle Cloud Infrastructure as described in [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#)
 - b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#), consisting of management of administrator privileges, and access to the operating system, database, and middleware
 - c. [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#), consisting of (a) installation/instantiation and/or configuration programs; (b) software patches which repair or modify existing functionality or maintain currency alignment with business requirements; and (c) application server parameter changes
 - d. [Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy](#)
 - e. [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#), consisting of planning of deployment of updates that are intended to improve performance, security, availability, stability, manageability, or regulatory compliance
 - f. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#), consisting of response and resolution of individual Incidents, associated Service Request (SR) tracking, problem identification, and Root Cause Analysis
 - g. [Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy](#)
 - h. [Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy](#), excepting backup and/or removal of any software

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Purchase and maintain for the duration of the Services, one or more Managed Applications Pre-requisite Service and one or more Managed Identity and Access Management Pre-Requisite Service.
2. Procure and maintain the amount of Oracle Compute Cloud Service, Oracle Java Cloud Service Enterprise Edition and Oracle Storage Cloud Service required to provide adequate computing capacity for the performance of the Connectors.
3. Perform UAT of the Connector Integration.

Service Assumptions

1. The following Oracle Applications Unlimited programs are supported for integration using the Connectors: Oracle E-Business Suite, PeopleSoft, Siebel, Oracle Hyperion, and Oracle Business Intelligence Enterprise Edition. Only Oracle Programs certified with Oracle Access Governance will be supported.
2. Oracle Access Manager is not required for this service.

MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited Environment – Integration Service

MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited Environment – Integration Service

Part #	Service Offering
B111192	MCS - Oracle Managed Identity and Access Management for US Government Cloud – Integrated Applications Unlimited Environment – Integration Service
B111206	MCS - Oracle Managed Identity and Access Management for US Defense Cloud – Integrated Applications Unlimited Environment – Integration Service

Description of Services

Oracle will provide You with integration (the “Services”) between one (1) Applications Unlimited program (the “Integrated Application”) and OCI Identity and Access Management Identity Domain (“OCI IAM Domain”).

Oracle will provide the Services for one (1) Connector Integration utilizing one of the following OCI IAM Domain connectors (the “Connector”):

- Oracle E-Business Suite Asserter (“EBS Asserter”)
- Oracle Application Gate (“App Gate”)

Oracle will provide the following as part of the Services:

1. Services below are intended to supplement the following service separately purchased by You (hereinafter the “Pre-requisite Service”):

Pre-requisite Service

Part #	Service Offering
B111191	MCS - Oracle Managed Identity and Access Management for US Government Cloud – Integrated Applications Unlimited Connector
B111205	MCS - Oracle Managed Identity and Access Management for US Defense Cloud – Integrated Applications Unlimited Connector

2. Designate a resource who will serve as Your primary point of contact to facilitate account management and service reviews.
3. Provide You with access URLs and administrative usernames and passwords as required for the Services.
4. Configure a connection in EBS Asserter to the Oracle E-Business Suite database for creation of authenticated user sessions, as required.
5. Configure the Connector with Integrated Application-specific HTTP header response attributes to return following successful authentication of a given User, as required.
6. Configure HTTP rewrite rules in the Integrated Application web layer to enable the re-direction of login to the OCI IAM Domain login page.
7. Assist You with issues identified by You during User Acceptance Testing (“UAT”) of the Connector Integration.
8. Upon Your successful completion of UAT and Your sign off, migrate the configurations for the Connector Integration to the production OCI IAM Domain.
9. Create a production runbook to document the configurations and troubleshooting steps for each Connector Integration.

10. Perform Production Assessment activities for the Connector Integration.
11. Re-configure EBS Asserter following a Refresh of an Oracle E-Business Suite Integrated Application.

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Provide connection details of an external directory server as required for App Gate for user and group lookups.
2. Create user accounts in the Integrated Application.
3. Procure and maintain for the duration of the Services the Pre-Requisite Service.
4. Perform UAT of the Connector Integration.

MCS - Oracle Managed Identity and Access Management for US Government Cloud - Integrated Applications Unlimited Connector - Enhanced Recovery Service

MCS - Oracle Managed Identity and Access Management for US Defense Cloud - Integrated Applications Unlimited Connector - Enhanced Recovery Service

Part #	Service Offering
B111193	MCS - Oracle Managed Identity and Access Management for US Government Cloud – Integrated Applications Unlimited Connector - Enhanced Recovery Service
B111207	MCS - Oracle Managed Identity and Access Management for US Defense Cloud – Integrated Applications Unlimited Connector - Enhanced Recovery Service

Description of Services

Oracle will provide Enhanced Recovery Services as described in Appendix 1: Oracle Managed Services Delivery Policies (the “Services”) in accordance with, and to supplement, the following services separately purchased by You (hereinafter “Pre-requisite Services”):

Pre-requisite Services

Part #	Service Offering
B111192	MCS - Oracle Managed Identity and Access Management for US Government Cloud – Integrated Applications Unlimited Environment
B111206	MCS - Oracle Managed Identity and Access Management for US Defense Cloud – Integrated Applications Unlimited Environment
B111191	MCS - Oracle Managed Identity and Access Management for US Government Cloud – Integrated Applications Unlimited Connector
B111205	MCS - Oracle Managed Identity and Access Management for US Defense Cloud – Integrated Applications Unlimited Connector

1. Designate a resource who will serve as Your primary point of contact to facilitate account management and service reviews.
2. Provide the Services for one (1) Oracle E-Business Suite Asserter (“EBS Asserter”) connector environment or one (1) Oracle Application Gate (“App Gate”) connector environment in accordance with the following table:

Enhanced Recovery Service

Service	Type
RPO	1 hour
RTO	12 hours
Testing Frequency	Annual

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Procure and maintain the amount of Oracle Compute Cloud Service, Oracle Java Cloud Service Enterprise Edition and Oracle Storage Cloud Service required to provide adequate computing capacity for the performance of EBS Asserter and App Gate associated with the Services.
2. Procure and maintain for the duration of the services the Pre-Requisite Services.

MCS - Oracle Managed Integration Cloud Service for US Government Cloud

MCS - Oracle Managed Integration Cloud Service for US Defense Cloud

Part #:	Service Offering
B111194	MCS - Oracle Managed Integration Cloud Service for US Government Cloud - Bundled Base
B111208	MCS - Oracle Managed Integration Cloud Service for US Defense Cloud - Bundled Base
B111195	MCS - Oracle Managed Integration Cloud Service for US Government Cloud - Standard Base
B111209	MCS - Oracle Managed Integration Cloud Service for US Defense Cloud - Standard Base
B111196	MCS - Oracle Managed Integration Cloud Service for US Government Cloud - Hosted Environment
B111210	MCS - Oracle Managed Integration Cloud Service for US Defense Cloud - Hosted Environment
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle will provide the following Oracle Managed Integration Cloud Service (the “OIC Services”) for the Oracle Integration Cloud (OIC) Service for which You have separately purchased a subscription (“Your Subscription”) and for the number of hosted environments identified in Your order (the “Managed OIC Environments”) in accordance with the Service Maximums table below:

1. Provision each Managed OIC Environment with standard administrative users and integration instances.
2. Provision virtual machines (“VMs”) with OIC agents, if required, and manage the OIC agents. Management of the VMs may be provided under the Oracle Managed IaaS Service separately purchased by You.
3. If you have separately purchased Autonomous Transaction Processing (“ATP”) or Database Cloud Service (“DBCS”), provision and enable Visual Builder and File Server for the Oracle Integration instance.
4. Configure each Managed OIC Environment with custom end points and connectivity of agents, upload and install certificates on connectivity agent machines and restrict instance access and File Server access based on requirements provided by You.
5. Provision users, user groups and policies, and assign integration roles based on requirements submitted by You.
6. Provide start/stop services for Production Environments and Non-Production Environments.
7. Resize the Managed OIC Environments (scale up/down) as requested by You via an RFC.
8. Backup and restore OIC agents in accordance with the Maintenance Frequency table below.
9. Patch the agent machines in accordance with the Maintenance Frequency Table below.
10. Monitor the integration instance URLs and agent machines.
11. Use the assigned Oracle Cloud Administrator roles and privileges to provide the OIC Services as described in the following Sections of [Appendix 1: Oracle Managed Services for Oracle Cloud for US Government Service Delivery Policies](#):
 - a. [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#) for OIC Service programs.
 - b. [Oracle Managed Services for Oracle Cloud for US Government Access Management Policy](#), consisting of managing administrative access for Your Subscription using the Oracle Cloud Administrator role, including the following activities/tasks in accordance with the Frequency Table below:

- i. Add, remove, and change administrative users, groups, and policies for each OIC Environment.

Maintenance Frequency Table

Activity/Task	Quantity/Frequency
User Access Administration	Up to 5 times per month
Scale up / Scale down	Twice per month
Agent machine backup	Twice Daily backup retained for 30 days
Agent machine Patching	Once per Quarter

- c. [Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy](#), consisting of response and resolution of individual incidents related to OIC agents and agent machines managed by Oracle, and associated SR tracking and routing to proper resolution queues.
- d. [Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy](#) for Your Subscription.
- e. [Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy](#)
- f. [Oracle Managed Services for Oracle Cloud for US Government Service Level and Availability Management Policy](#), excluding Service Request Resolution Time Service Level and including the following:
 - **Service Level Target.** The level of performance under the applicable Service Level that Oracle endeavors to achieve on a monthly basis.
 - **Credit Criteria.** If the monthly performance measured for a Service Level is below the Service Level Target, then the credit criteria are used to determine the applicable Service Level Credit.
 - **Service Level Credit %.** The percentage of monthly recurring fees paid by You for the OIC Services to be credited based on the credit criteria.

Service Level	Service Level Target	Credit Criteria	Service Level Credit %
OIC Environment Availability	99.5%	<99.5%	10%
Performance Against Service Description	Performance of the OIC Services in accordance with this section	As described in this Service Description	As indicated below

Oracle OIC Environment Availability Service Level

The OIC Environment Availability Service Level consists of the measurement of the percentage of time that the individual Managed OIC Environment is available for access and use by You to conduct production business operations (“Production OIC Environment”), and are measured by Oracle on a monthly basis and calculated in accordance with the following formula:

$$\left\{ \frac{\begin{aligned} &[\text{Total minutes in a calendar month} \times \text{number of Production OIC Environments} \\ &- \text{Sum of Unplanned Outage (caused by OIC Service failure)} \\ &\text{minutes measured for each Production OIC Environment in such month}] \end{aligned}}{\text{Total minutes in the calendar month} \times \text{number of Production OIC Environments}} \right\} \times 100$$

Only Severity Level 1 Unplanned Outages caused by OIC Service failures of a Production OIC Environment shall be used to calculate Oracle's monthly performance against the OIC Environment Availability Service Level.

Incidents for which the root cause is subject to exclusion per [Oracle Managed Services Delivery Policies](#) or that occur in a Production OIC Environment during a Stabilization Period shall not be included in the OIC Environment Availability calculation. A Production OIC Environment must have at least one associated Production Support Environment for service level credits to be applicable.

Performance Against Service Description Service Level

The Service Level Credit for Performance Against Service Description Service Level is ten percent (10%) of the total fees paid by You for the OIC Services for the month in which the Service Level Credit accrued, MINUS any Service Level Credit earned under the OIC Environment Availability Service Level in connection with the OIC Services provided in such month.

Maximum Aggregate Service Level Credit

The aggregate maximum Service Level Credit is ten percent (10%) of the total fees paid for the OIC Services for the month in which the Service Level Credit accrued.

Service Maximums

The OIC Services are subject to the following constraints ("Service Maximums").

Additional Service Maximums are documented in the Managed Services Exhibit, as applicable.

Service Maximums

Type	Quantity/Frequency
Service Plan Update & Service Request Review Frequency	Quarterly
Account & Service Review Frequency	Annual
Availability Plan Frequency	Annual

Supplemental Resources

If included in Your order, Oracle will provide additional resources, either on-site or remotely, up to the number of days¹ per resource role set forth in Your order ("Supplemental Resources") to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order for *Oracle Managed Integration Cloud Service*:

1. Coordination and planning of Initiation Phase activities
2. Assistance with SRs related to the following:
 - a. Issue reproduction
 - b. Constructing a reproducible test case

- c. Guidance related to potential workarounds
 - d. Guidance related to recommendations documented in the SR
3. Account and Service Reviews
4. Local language support

Your Cooperation and Service Assumptions

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. For MCS - Oracle Managed Oracle Integration Cloud Service for US Government Cloud – Bundled Base (part # B111194) or MCS - Oracle Managed Oracle Integration Cloud Service for US Defense Cloud – Bundled Base (part # B111208), purchase and maintain for the duration of the OIC Services one or more of the following services (the “Pre-requisite Service”):
 - a. The following:

Part #	Service Offering
B109115	MCS - Oracle Managed Analytics Cloud Service for US Government Cloud - Standard Base
B109332	MCS - Oracle Managed Analytics Cloud Service for US Defense Cloud - Standard Base
B95474	MCS - Oracle Managed Application Cloud for US Government Cloud, Custom
B109103	MCS - Oracle Managed Database as a Service for US Government Cloud - Standard Base
B109320	MCS - Oracle Managed Database as a Service for US Defense Cloud - Standard Base
B109092	MCS - Oracle Managed Enterprise Application Cloud for US Government Cloud - Base
B109309	MCS - Oracle Managed Enterprise Application Cloud for US Defense Cloud - Base
B109109	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCC Standard Base per Rack
B109113	MCS - Oracle Managed Exadata Database Cloud Service for US Government Cloud - ExaCS Standard Base per Rack
B109326	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCC Standard Base per Rack
B109330	MCS - Oracle Managed Exadata Database Cloud Service for US Defense Cloud - ExaCS Standard Base per Rack

- b. Any service/part number described by the MCS - Oracle Managed Applications Unlimited for US Government Cloud Service or MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service service description within this Oracle Managed Services Service Description document.
2. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, Oracle Managed Services Delivery Policies, and this service description.
3. Procure and maintain for the duration of the OIC Services adequate capacity for the performance of the OIC Services and Your Subscription.
4. Follow the Oracle Managed Services Minimum Architecture Guidelines (available at <https://support.oracle.com> by searching on [Document ID 784630.1](#)).
5. Be responsible for making necessary network changes as required for the OIC Services.
6. Allow Oracle Enterprise Manager Ops Center instance to monitor the Managed OIC Environment(s).

7. Perform all required end-2-end testing to validate that the OIC Service platform is configured securely, and correctly.
8. Separately purchase services to migrate content to the Managed OIC Environments, if required and subject to additional fees.
9. Separately purchase and maintain for the duration of the OIC Services Managed ATP or DBCS required for Visual Builder.
10. For OIC Agent VMs managed by Oracle, separately purchase and maintain for the duration of the OIC Services the Managed IaaS Service to support the OIC Agent deployments.
11. Develop applications and application logic.
12. Provide support and assistance to Oracle as required to perform the assigned Oracle Cloud Administrator roles and privileges.
13. Provide support and documented requirements to Oracle as necessary for Oracle to manage and configure the Managed OIC Environments.
14. Be responsible for managing end user access and application privileges.

Service Assumptions

1. Users are setup and authenticated with Oracle Identity Access Management (“IAM”) unless You have separately purchased and maintain for the duration of the OIC Services one of the following:
 - a. MCS - Oracle Managed Identity and Access Management for US Government Cloud, Standard – B111186
 - b. MCS – Oracle Managed Identity and Access Management for US Defense Cloud, Standard – B111200
 - c. MCS – Oracle Managed Identity and Access Management for US Government Cloud, Foundation Plus – B111187.
 - d. MCS - Oracle Managed Identity and Access Management for US Defense Cloud, Foundation Plus
2. The OIC Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Managed Security Data Masking Service for US Government Cloud

MCS - Oracle Managed Security Data Masking Service for US Defense Cloud

Part #	Service Offering
B111197	MCS - Oracle Managed Security Data Masking Service for US Government Cloud
B111211	MCS - Oracle Managed Security Data Masking Service for US Defense Cloud
B111198	MCS - Oracle Managed Security Data Masking Service for EBS for US Government Cloud
B111212	MCS - Oracle Managed Security Data Masking Service for EBS for US Defense Cloud

Description of Services

Oracle will perform the following activities designed to mask sensitive production data while preserving the integrity of the database (the “Services”), in accordance with the Service Maximums documented in Your order. Oracle will provide the Services for one (1) non-production Oracle Database for which You have separately purchased one (1) of the following services (each, a “Prerequisite Service”).

Prerequisite Service

Part #	Service Offering
B95474	MCS - Oracle Managed Application Cloud for US Government Cloud, Custom
B109092	MCS – Oracle Managed Enterprise Application Cloud for US Government Cloud - Base
B109309	MCS – Oracle Managed Enterprise Application Cloud for US Defense Cloud - Base
B109091	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two Minimum Complexity
B109308	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two Minimum Complexity
B109090	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two Low Complexity
B109307	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two Low Complexity
B109089	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier Two High Complexity
B109306	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier Two High Complexity
B109088	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service, Tier One Minimum Complexity
B109305	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service, Tier One Minimum Complexity
B109087	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier One Low Complexity
B109304	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier One Low Complexity
B109086	MCS - Oracle Managed Applications Unlimited for US Government Cloud Service Tier One High Complexity
B109303	MCS - Oracle Managed Applications Unlimited for US Defense Cloud Service Tier One High Complexity

1. Designate a resource who will act as Your primary point of contact for the Services.
2. Validate the shape and size of the target non-production Oracle Database of Your Applications Unlimited environment managed by Oracle (the “Target Database”) and inform You if additional compute resources are required for the execution of the data masking scripts.
3. Document the Target Database and each database object column, identified by You that needs to be masked (“Data Element”).
4. Define and document the mask formats for each Data Element, such as address column or bank account column (“Mask Formats”).
5. Develop data masking scripts based on the Mask Formats in Your Target Database.
6. Deploy and test the data masking scripts in Your Target Database and verify data integrity.
7. Document and maintain the data masking scripts.
8. Provide break fixes for data masking scripts that fail during execution.
9. Update existing data masking scripts as needed for Your Target Database upgrades.
10. Execute the data masking scripts for the duration of the Services (“Data Masking Script Execution”).

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to the obligations in the Policies:

1. Purchase and maintain for the duration of the Services a Prerequisite Service, including one of the following for the Target Database:
 - a. Oracle Compute Cloud Service
 - b. Oracle Database Cloud Service
 - c. Oracle Database Exadata Cloud Service
2. If You have purchased TBD - MCS - Oracle Managed Security Data Masking Service for EBS for US Government Cloud or MCS - Oracle Managed Security Data Masking Service for EBS for US Defense Cloud, then purchase and maintain the license for Oracle Data Masking and Subsetting Pack for Oracle Enterprise Management.
3. Purchase additional resources if, in Oracle’s sole discretion, it is determined that the shape and size of Your Target Database environment is not sufficient for the execution of the data masking scripts.
4. Identify the Target Database and Data Elements.
5. Be responsible for Your, Your Users’ and Your third parties’ use of and access to networks, systems, and all environments, including use of and access to Your Content and for compliance by Your and such third parties with the terms of the Agreement, order, and this Service Description.
6. Use Oracle’s ticketing system to raise SRs or RFCs related to the Services.

Service Assumptions

The Services do not include any activities that are not explicitly described in this Service Description.

MCS - Oracle Operational Readiness for Oracle Cloud Guard Service for US Government Cloud

MCS - Oracle Operational Readiness for Oracle Cloud Guard Service for US Defense Cloud

Part #	Service Offering
B111213	MCS – Oracle Operational Readiness for Oracle Cloud Guard Service for US Government Cloud
B111214	MCS – Oracle Operational Readiness for Oracle Cloud Guard Service for US Defense Cloud
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle will provide guidance for baseline operational tuning and security configuration for Oracle Cloud Guard deployed in one (1) Oracle Cloud Infrastructure (“OCI”) Tenancy by performing the following activities (the “Services”):

1. Designate a resource who will act as Your primary point of contact to facilitate the Services.
2. Enable Oracle Cloud Guard (“Cloud Guard”) for the target OCI Tenancy.
3. Review the logical security requirements, including compartment and resource policies, in Your target OCI Tenancy.
4. Validate the high-level design of Your Cloud Guard deployment in Your OCI Tenancy (the “Cloud Guard Targets”).
5. Review the Cloud Guard detector recipes that are used to scan Your Cloud Guard Targets.
6. Advise on the potential use of one (1) custom detector recipe for Your Cloud Guard Targets based on Your specific security requirements.
7. Advise on the functionality of up to five (5) standard Cloud Guard responders that may meet Your requirements for deployment in Your OCI Tenancy.
8. Provide a high-level analysis of issues identified in Your Cloud Guard Targets, including recommended actions to remediate the identified issues.
9. Provide guidance and recommendations on the usage of Cloud Guard capabilities.
10. Provide a report of findings, in a format determined by Oracle and subject to Oracle’s Security Vulnerability Disclosure Policies, which are available at <https://www.oracle.com/corporate/security-practices/assurance/vulnerability/disclosure.html>.
11. Conduct a final meeting to review the report of findings and Oracle’s recommendations.

Supplemental Resources

If included in Your order, Oracle will provide additional resources, either on-site or remotely, up to the number of days¹ per resource role set forth in Your order (“Supplemental Resources”) to assist with one or more of the following activities, as applicable for the identified resource role, in furtherance of the services provided under Your order:

1. Coordination and planning of Initiation Phase activities

2. Advisory activities related to the following:
 - a. Adoption of custom detector recipes for the defined Oracle Cloud Guard targets
 - b. Functionality of standard Cloud Guard responders
 - c. Usage and configuration of Oracle Cloud Guard capabilities
 - d. Oracle Cloud Guard issues and potential workarounds

Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to those in the Policies:

1. Procure and maintain for the duration of the Services Your OCI subscription.
2. Define the target OCI Tenancy and Cloud Guard Targets.
3. Authorize Oracle to enable Cloud Guard.
4. Provide Oracle resources with access to Cloud Guard as required to deliver the Services.
5. Designate Your security point of contact who will communicate with Oracle related to the Services.
6. Provide to Oracle Your specific security requirements for Cloud Guard custom detector recipes and responders.
7. Be responsible for Your, Your Users' and Your third parties' use of and access to networks, systems, and all Environments, including use of and access to Your Content and for compliance by You and such third parties with the terms of the Agreement, order, and this Service Description.

Unused Services

The Services must be used within six (6) months from the date Your order is placed. Any Services not used within the six (6) months from the date Your order is placed will be automatically forfeited by You, with no further action required of either party, and You will not be entitled to a refund, or any credit toward additional or other Services, for any unused portion of the fees paid for any unused Services. You may not use the fees for any Services other than the Operational Readiness for Oracle Cloud Guard Services stated herein.

MCS – Security Account Manager for US Government Cloud

MCS – Security Account Manager for US Defense Cloud

Part #	Service Offering
N/A	MCS – Security Account Manager for US Government Cloud
N/A	MCS – Security Account Manager for US Defense Cloud

Description of Services

Oracle will assign an account manager as Your primary contact for security and compliance regarding Your combined use of Oracle products and Oracle services (“Security Account Manager”). The Security Account Manager will perform the following activities:

1. Develop and maintain a security roadmap that aligns Your security and compliance requirements across Your Oracle products and Oracle services (the “Security Roadmap”).
2. Support You during external security audits and provide guidance on regulatory compliance and any associated changes to Your security policies and Security Roadmap.
3. Analyze new Oracle products and/or Oracle services for inclusion in Your Security Roadmap.
4. Coordinate the delivery of any security and compliance services provided by Advanced Customer Services that You have separately purchased and provide input to align Your specific security configurations with Oracle’s security practices and standards.
5. Address Your security related questions and requests for assistance or information.
6. Advise You on availability of security related training and coordinate any identified training that may help You with Your adoption of Oracle products and Oracle services and any related security services.

Oracle Cloud Infrastructure Accelerator Service for US Government Cloud Advantage

Oracle Cloud Infrastructure Accelerator Service for US Defense Cloud Advantage

Part #	Service Offering
B109119	MCS - Oracle Cloud Infrastructure Accelerator Service for US Government Cloud Advantage
B109336	MCS - Oracle Cloud Infrastructure Accelerator Service for US Defense Cloud Advantage
B109120	MCS - Oracle Managed Services Supplemental Resources for US Government Cloud - Day
B109337	MCS - Oracle Managed Services Supplemental Resources for US Defense Cloud - Day

Description of Services

Oracle Cloud Infrastructure Accelerator Service Advantage for Oracle Cloud for US Government (the “Accelerator Services”) consists of the following activities for Your Oracle Cloud for US Government tenancy or the identified workload in Your Oracle Cloud for US Government tenancy for the Cloud Services, for which You have separately purchased a subscription, in accordance with the Service Maximums documented in Your order:

1. Service Delivery Management

Oracle will assign a Technical Account Manager (“TAM”) who will serve as Your primary contact for the following activities:

a. Service Initiation:

- i. Conduct an orientation with You to introduce the TAM and the other resources who will assist with service setup, configuration, review, and other applicable processes of the Accelerator Services.
- ii. Identify and document (i) the key Oracle contacts; (ii) Your technical primary contacts designated by You to communicate with Oracle regarding the Accelerator Services (“Customer Contacts”); and (iii) Oracle’s escalation procedures.
- iii. Manage the creation of a joint plan (the “Delivery Plan”) that will identify and document (i) Your Cloud Services; (ii) Oracle’s access requirements to Your Cloud Services; (iii) your processes and procedures for release management, including Cloud Services update cycles; (vi) pre-defined environment assessments; and (v) Oracle certification programs and labs available under this service description.

b. Service Management and Governance:

- i. Prepare and maintain quarterly service delivery progress reports.
- ii. Maintain the Delivery Plan.
- iii. Perform quarterly service reviews.
- iv. Review and provide a trend analysis for all SRs opened with Oracle Support related to Oracle workloads on Oracle Cloud for US Government, for which You have an active cloud subscription.
- v. Prepare and maintain monthly SR reports.
- vi. Track and report Your monthly consumption and balance of Service Days. A Service Day is defined as one technical account manager or one technical resource working

one dayⁱ to (i) perform activities listed in the Innovation Guidance and Technical Assistance section; (ii) assist with Critical SRs as described in the Escalation Management section; or (iii) assist with Severity 1 SRs as described in the Command Center Escalation Assistance section.

c. Escalation Management

- i. Serve as Your designated point of contact for escalations initiated by You for Severity 1 SRs and those Severity 2 SRs that You and Oracle agree are critical (collectively, “Critical SRs”) and incidents affecting Your Cloud Services. The severity levels that apply to the Accelerator Services are defined in the Oracle Cloud Hosting and Delivery Policies, which are available at www.oracle.com/contracts.
- ii. In Oracle’s sole discretion, engage technical resources to review configurations of Oracle workloads on Oracle Cloud for US Government and provide assistance with Critical SRs.

2. Innovation Guidance and Technical Assistance

Upon Your request, Oracle will provide one or more of the following activities as submitted by You in an SR:

- a. Check the configurations of Your workload environments on Oracle Cloud for US Government against Oracle’s recommended practices for one (1) of the following components: database, compute, storage, network, or Oracle Cloud for US Government security practices (each a “Configuration Check”).
- b. Review configurations of Your operational processes against Oracle’s recommended practices for one (1) of the following components: backup and recovery, high availability, disaster recovery or scalability (each an “Environment Review”).
- c. Review Your existing Oracle Cloud for US Government architecture against Oracle’s recommended practices for Oracle Cloud for US Government (“Architecture Review”).
- d. Make recommendations related to Your configurations based on the results of Configuration Checks, Environment Reviews, and/or Architecture Reviews.
- e. Provide You with technical guidance for configuration changes and adoption of recommendations identified by Oracle cloud tools, such as Cloud Advisor, Oracle Cloud Guard, Cloud Dashboards, and Cloud Observability and Management Platform.
- f. Provide technical guidance for issues related to scalability, integrations, configurations, CEMLI, automations, performance, patch analysis, and lifecycle management processes for Oracle workloads on Oracle Cloud for US Government (“Technical Assistance”).
- g. Assist You with the implementation or operationalization of recommended actions provided by Oracle as a result of Configuration Checks, Environment Reviews, Architecture Reviews, or Technical Assistance.
- h. Review Your migration plan to evaluate Your readiness to move additional workloads from Your premises to Oracle Cloud for US Government.
- i. Review Your readiness to commence production operations for Your planned business events and milestones, including upgrades and migrations.
- j. Assist You with the evaluation of newly available Cloud services that may benefit You in Your adoption of Oracle Cloud for US Government.

3. Command Center Escalation Assistance - Proactive Support

If Command Center Escalation Assistance is included in Your order, at the request of Your Approver (as defined below), the TAM will escalate a Severity 1 SR to Oracle's command center as follows:

- a. Initiate a web conference session with Oracle's command center team.
 - b. Review the SR with Your Customer Contact(s), including the following:
 - i. Review potential workarounds.
 - ii. Discuss possible corrective actions.
 - iii. Identify Oracle workload or Cloud Services on Oracle Cloud for US Government that may be contributing to the issue.
 - c. Engage additional Oracle support teams or resources as needed to address the issue.
 - d. Ask Your Customer Contact(s) to engage third party providers for the specific Cloud Services on Oracle Cloud for US Government, as needed.
 - e. Document the incident and provide periodic updates to Your Customer Contacts.
 - f. Disengage the command center when (i) an action plan to resolve the incident has been identified and initiated or (ii) You de-escalate the SR.
- ### 4. Oracle Cloud Digital Learning
- a. Provide You with, and facilitate Your access to, select Oracle Cloud certification programs that are part of Oracle Cloud training and certification subscriptions provided by Oracle University as documented in Your order.
 - b. Provide You with, and facilitate Your access to, Oracle Cloud labs that are part of Oracle Cloud training and certification subscriptions provided by Oracle University as documented in Your order.

Supplemental Resources

If included in Your order and upon Your request, Oracle will provide additional remote resources up to the number of daysⁱ per resource role set forth in Your order ("Supplemental Resources") to assist with one or more of the following activities in furtherance of the services provided under Your order for the Accelerator Services:

1. Lead, participate in, or facilitate meetings with You.

Your Cooperation and Assumptions

1. Your Cooperation

Subject to the terms in the Policies, the following obligations apply in addition to those in the Policies:

- a. Identify each of Your Customer Contacts by name, phone number, e-mail address and other appropriate contact methods, including a designated Customer Contact with the appropriate level of authority to set priorities, coordinate activities and resolve conflicts between Your teams ("Approver").
- b. Provide Oracle with necessary user and role access required to deliver the Accelerator s.
- c. Provision any tools and associated compute and storage as requested by Oracle and required for Oracle to deliver activities documented under the Innovation - Guidance and Technical Assistance section.

- d. Implement, or submit a request for Oracle to implement, recommended actions provided to You by Oracle as documented in the Innovation – Guidance and Technical Assistance section above.
 - e. Be solely responsible for the impact that the implementation of recommended actions may have on Your environments.
 - f. Separately purchase additional services for Oracle University certifications or Oracle Cloud labs in addition to the documented Service Maximums above, as needed.
2. Assumptions
- a. At Oracle's discretion, the TAM assigned to You may communicate with You in Your local language; however, the TAM will not provide translation support related to the Accelerator Services on Your behalf.
 - b. The Accelerator Services will be provided by remote delivery resources (not on Your work premises).
 - c. The Accelerator Services may not be available for all Oracle Cloud Services.
 - d. Any services not expressly identified herein are considered out of scope.

APPENDIX 1: ORACLE MANAGED SERVICES FOR ORACLE CLOUD FOR US GOVERNMENT DELIVERY POLICIES

Unless otherwise stated, these Oracle Managed Services for Oracle Cloud for US Government Delivery Policies (the “Delivery Policies”) describe the Managed Services ordered by You for use in conjunction with Oracle Cloud for US Government (“Services”) if referenced in the applicable service description. These Delivery Policies do not govern Oracle Cloud for US Government. Any use of Oracle Cloud for US Government in the delivery of the Services are governed by the *Oracle Cloud Hosting and Delivery Policies* and the Oracle PaaS and IaaS Public Cloud Services pillar document, which may be viewed at www.oracle.com/contracts, and the [applicable US Government Provisional Authorities to Operate \(P-ATO\) and Authority to Operate \(ATO\)](#).

These Delivery Policies may reference other Oracle Managed Cloud Policy documents; any reference to "Customer" in these Delivery Policies or in such other policy documents shall be deemed to refer to “You” as defined in the ordering document. For the purpose of the Services ordered by You, “Services Environment” refers to the combination of software components, from the guest virtualization layer up through the application administration layer in the Oracle Cloud for US Government environment in which the Services operate for the Oracle Programs and Required Software that are owned, licensed, or managed by Oracle and to which Oracle grants You and Your Users access.

Overview and Table of Contents

The Services described herein are provided under the terms of the agreement, order, and related service specifications including these Delivery Policies. Oracle’s delivery of the Services is conditioned on You and Your users’ compliance with Your obligations and responsibilities defined in such documents and incorporated policies. These Delivery Policies, and the documents referenced herein, are subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of performance, security, or availability of the Services provided during the Services Period of Your order.

The Delivery Policies include the following:

1. Oracle Managed Services for Oracle Cloud for US Government Security Policy
2. Oracle Managed Services for Oracle Cloud for US Government Access Management Policy
3. Oracle Managed Services for Oracle Cloud for US Government Change Management Policy
4. Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy
5. Oracle Managed Services for Oracle Cloud for US Government Release Management Policy
6. Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy
7. Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy
9. Oracle Managed Services for Oracle Cloud for US Government Service Level and Availability Management Policy
10. Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy
11. Oracle Managed Services for Oracle Cloud for US Government Service Continuity Policy
12. Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy
13. Oracle Managed Services for Oracle Cloud for US Government Enhanced Recovery Policy
14. Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy

Oracle Managed Services for Oracle Cloud for US Government Hours of Operation

The Services are designed to be available 24 hours a day, 7 days a week, 365 days a year except during maintenance periods and as otherwise set forth in the agreement, the order, and these Delivery Policies.

Oracle Managed Services for Oracle Cloud for US Government Security Policy

Scope

Oracle provides reasonable and appropriate security measures designed to protect the confidentiality, integrity, and availability of Your Content hosted in the Services Environment utilizing the Services governed by these Delivery Policies. Oracle continually works to strengthen and improve security controls and practices for the Services.

Oracle Managed Cloud Services for Oracle Cloud for US Government security policies are aligned with the process defined in NIST 800-37, the security controls defined in NIST 800-53, the ISO/IEC 27002:2005 (formerly known as ISO/IEC 17799:2005) and ISO/IEC 27001:2005 standards, govern all areas of security applicable to the Services and may exceed requirements mandated by other Oracle security policies referenced in these Delivery Policies.

Upon Customer's reasonable written request, Oracle will provide a description of the functional properties of the controls used on the Services Environment. The description of the functional properties of the controls is intended to provide sufficient detail to permit analysis and testing of the controls.

The general Oracle security management activities relevant to the Services governed by these Delivery Policies are enumerated and summarized in the following table:

Table 1

Organizational Security	<i>Oracle Security Organization Policy</i> describes and clarifies the roles and responsibilities of various teams and individuals involved in information security at Oracle.
Organizational Security Infrastructure	<i>Information Security Policy</i> describes the principles for development, executive approval, implementation, and maintenance of all information security policies and practices at Oracle
Asset Classification and Control	<i>Information Protection Policy</i> provides guidelines for Oracle personnel regarding information classification schemes and handling requirements, <i>Desktop and Laptop Security Policy</i> describes mandatory use of anti-virus and firewall software and recommended use of automatic update software. <i>Oracle Acceptable Use Policy for Company Resources</i> sets requirements for use of the Oracle corporate network, computer systems, telephony systems, messaging technologies, Internet access, and other company resources.
Human Resources Security	<i>Code of Ethics and Business Conduct</i> covers the areas of legal and regulatory compliance and business conduct and relationships as well as compliance-tracked training every two years that also addresses sensitive information handling.
Physical and Environmental Security	<i>Facility Classification and Minimum Security Standards</i> sets forth requirements for physical protection and access to information systems.
Communications and Operations Management	<i>Server Security Policy</i> sets forth the physical and logical security requirements for all Internet-facing and production Servers, <i>Logging and Log Analysis Policy</i> describes mandatory practices for log retention, review, and analysis, <i>Transport Layer Security Policy</i> describes TLS-based session security for web-based applications, <i>Network Scanning Request Procedure</i> govern restricted network scanning and vulnerability testing of Oracle networks and systems.

Access Control	<i>Logical Access Controls Policy</i> covers authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined users with access to Oracle systems which are not Internet-facing, publicly accessible systems. <i>Password Policy</i> requires use of strong password controls where passwords are being used as a method of authentication.
Systems Development and Maintenance	<i>CPU and Security Alerts Implementation Policy</i> describes requirements and timelines for implementation of updates and patches and associated recommendations. The <i>Release Media Sanitization and Disposal Policy</i> provides guidelines on secure erasure of information from all types of electronic media.
Compliance	<i>Oracle Services Privacy Policy</i> describes treatment of data that resides on Oracle, customer or Third Party Vendor systems, <i>Information Security Incident Reporting and Response Policy</i> describes timely and efficient practices for incident response, and <i>Security Breach Disclosure Policy</i> provides internal notification requirements in the event of suspected unauthorized access to personally identifiable information.
Exceptions	You may be required to sign a <i>Risk Acceptance Memo</i> detailing any security policy exception acknowledging the related risk to You, Oracle, and other parties (as applicable).

The detailed Oracle security policies identified in [Table 1](#) are confidential and not generally available for review by customers or third parties.

In addition to the general security activities described in [Table 1](#), Oracle will perform the following for the Services:

1. Conduct security compliance tests to identify and address key issues that may impact system performance following Production Go-Live.
2. Log security-related information from activities on operating systems, applications, middleware, and databases and retain such logs in accordance with the Service Maximums table in the Oracle Managed Services for Oracle Cloud for US Government Service Description and may retain if an anomalous event or series of events occur that constitute an information security incident.
3. Follow Your instructions to enable standard database auditing functionality.
4. Secure the default installation of operating systems deployed in the Services Environment by eliminating any system services, configurations, accounts, network protocols and user access rights not required for the virtual server to perform its duties, as well as enable default log file settings for auditing critical events.
5. Address vulnerabilities confirmed by Oracle as valid and follow recommended changes applicable within the scope of the Services.
6. Provide enforcement of the Oracle security policies, procedures, and practices through a combination of periodic security reviews and assessments to confirm compliance.
7. Work with You to identify additional encryption options for the Services not already provided as part of Oracle Cloud for US Government, or otherwise prohibited by Oracle for use with Oracle Cloud for US Government, to protect Your Content from unauthorized access.

Subject to Your Order, Oracle reserves the right to suspend the Services if Oracle detects activity in the Services Environment which appears to be malicious in nature or which could negatively impact the Services or other customer's services. Subject to Your Order, Oracle may disclose data located on Oracle systems, including the Services Environment, as required by law without Your prior consent. When reasonably practicable and lawfully permitted, we will provide You with

advance notice of any such disclosure. Oracle may store Your contact information in any country where Oracle does business for internal use and to communicate with You.

Customer Responsibilities

1. Complete Your own Certification and Accreditation (“C&A”) package for the Services as configured for Your Services Environment.
2. Conduct any additional technical testing required to support C&A activities, including but not limited to verification of compliance to the Department of Defense Security Technical Implementation Guidelines (“DoD STIG”) or other configuration baseline, NIST guidance documents, or any other agency specific requirements. Any technical testing or audit of Oracle Infrastructure will require advance notice and approval and the activity will be performed in accordance with the Requirements for Oracle Customer Security Assessments.
3. Implement Your own security policies, practices, and procedures.
4. Support Oracle recommendations on system/Service hardening, including authorizing prompt application of security patches and configuration Changes.
5. Authorize changes to Your Content as required for performance of the Services.
6. Determine appropriate classification and control levels for Your Content and provide any appropriate notices and/or obtain required consents relating to its collection and use, including any consents necessary for Oracle to provide the Services.
7. Maintain personnel security for Your employees and contractors.
8. Promptly notify Oracle of any employee-related security issues or concerns that could impact security.
9. Provide anti-virus and firewall security to protect against malicious code at Your workstations and servers used to access the Services.
10. If required, assist Oracle with functional setup for database audit logging.
11. Follow Oracle file transfer procedures when transferring data to the Services.
12. Promptly report to Oracle security Incidents and suspicious activity related to Your use of the Services.
13. Cooperate with Oracle on security Incident management and investigations as well as manage any associated security Incident-related activities including, but not limited to, communication with Your customers.
14. Be solely responsible for Your regulatory compliance in Your use of the Services and make Oracle aware of any relevant obligations prior to contract signature.
15. Notify Oracle of any audit requirements and provide Oracle any audit reports generated in connection with an approved audit of the Services, unless prohibited by law.
16. Provide the Oracle Cloud log-in credentials and private keys generated as part of Oracle Cloud for US Government to use on Your behalf.
17. Be solely responsible for the results of Your non-compliance with Managed Cloud Services for Oracle Cloud for US Government security requirements including, but not limited to, any impact from such non-compliance.

Oracle Managed Services for Oracle Cloud for US Government Access Management Policy

Scope

Oracle will secure access to the operating systems and administrator privileges to the Oracle Programs, Required Software, and Co-resident Third Party Programs in the Services Environment (collectively, the “Managed Software”) within Your Tenancy (the “Oracle Managed Tenancy”) or within the Compartment(s) assigned to Oracle by You within Your Tenancy (the “Oracle Managed Compartment”) pursuant to the [Oracle Managed Services for Oracle Cloud for US Government Security Policy](#) described above.

For the Services, Oracle will:

1. Assist You with determining the required Oracle Managed Tenancy and/or Oracle Managed Compartment(s) and associated access rights and privileges.
2. For Oracle Managed Compartments, identify additional Oracle Cloud for US Government components and/or software to be implemented as required for Oracle to provide the Services.
3. For Oracle Managed Compartment(s), use the assigned access and privileges to manage all resources (including user management) in the Oracle Managed Compartments for the Services under these Delivery Policies.
4. For Oracle Managed Tenancies, use Oracle Cloud log-in credentials and private keys generated as part of Oracle Cloud for US Government on Your behalf for the Services under these Delivery Policies.
5. Manage operating system accounts, administrator account and application privileges and maintain secure login procedures as required to provide security, service level and availability management for the Oracle Managed Tenancies and/or Oracle Managed Compartment(s) as described in these Delivery Policies.
6. Limit direct administrative access to the Oracle Managed Tenancies and/or Oracle Managed Compartment(s) to only those Oracle employees who are U.S. citizens. For avoidance of doubt, individuals born in the United States, Puerto Rico, Guam, Northern Mariana Islands, Virgin Islands, American Samoa, or Swain’s Island; foreign-born children, under age 18, residing in the United States with their birth or adoptive parents, at least one of whom is a United States citizen by birth or naturalization; and individuals granted citizenship status by Immigration and Naturalization Services (INS) are considered U.S. citizens.
7. Limit user access rights as an appropriate operating system hardening measure.
8. Control Your write access to the Production Environment(s) database within the Oracle Managed Tenancies and/or Oracle Managed Compartment(s) with the exception that You have the ability to grant an End User access to update interface tables and CEMLI schema objects.
9. Grant You and Your Implementer management rights and write access to Production Support Environment(s) and based on role, to the custom database schemas in the Production Support Environments.

Customer Responsibilities

1. Consult with Oracle to determine the Oracle Managed Compartment(s) that You need to create within Your Tenancy as required for Oracle to provide the Services under these Delivery Policies.

2. For Oracle Managed Tenancies, provide the log-in credentials and private keys You receive during the provisioning of Your Oracle Cloud for US Government services to facilitate delivery of the Services.
3. For Oracle Managed Compartments,
 - a. Be solely responsible for the administration of Your Oracle Cloud for US Government Tenancy.
 - b. Purchase the additional Oracle Cloud for US Government cloud and software components identified by Oracle and required for providing services in Oracle Managed Compartments.
 - c. Create a user group for Oracle administrators with privileges to manage all resources, including user management, within the Oracle Managed Compartment(s).
 - d. Create a user group for Your administrators with read-only access to the Oracle Managed Compartment(s).
 - e. Strictly enforce the access restrictions to the Oracle Managed Compartment(s) to protect the resources and instances within the Oracle Managed Compartment(s) from unauthorized access and changes.
 - f. Ensure that no changes are made to the Oracle Managed Compartment(s) and/or the user group assigned to Oracle administrators unless expressly authorized by Oracle.
 - g. Provide security, including workload and network, to ensure the stability and availability of the resources and instances within the Oracle Managed Compartment(s).
 - h. Manage resources that are commonly used by Oracle and You in such a manner to avoid any disruption to the availability and stability of the resources within the Oracle Managed Compartment(s):
 - i. Network and connectivity resources, including but not limited to virtual cloud network (“VCN”), FastConnect, subnets, dynamic routing gateway (“DRG”), access rules, and virtual private network (“VPN”).
 - ii. Sufficient storage and common services, such as database backup service and LBaaS that must be available to Oracle at all times for delivery of the Oracle Managed Services.
 - i. Acknowledge that as the Tenancy owner You will be solely responsible for any action or event outside of Oracle’s control that may result in data loss and/or data corruption, performance instability, and/or access breaches within the environments located in the Oracle Managed Compartment(s).
 - j. Notify Oracle immediately of any security, access, and/or stability issues or breaches detected within Your Tenancy.
 - k. Utilize Oracle Cloud for US Government audit to monitor and manage access, compliance, integrity, and security alerts with Your Tenancy.
 - l. Provide Oracle with access to Oracle Cloud for US Government audit logs for Your Tenancy.
4. Notify Oracle if there are statutory or regulatory compliance requirements regarding Oracle personnel that may access Your Services.

5. Manage, and end as appropriate, all access, role and responsibility definition, non-administrator privileges as well as operating systems access for Your End Users and Implementer.
6. Ensure all End Users follow agreed controls and practices for access management to provide security, service level and availability management as described in these Delivery Policies.

Oracle Managed Services for Oracle Cloud for US Government Change Management Policy

Scope

Oracle will provide Change Management for the Managed Software pursuant to the Oracle Managed Services for Oracle Cloud for US Government Security Policy above.

For the Services, Oracle will:

1. Install the Managed Software for Your use and provide triage support for installation issues.
2. Authorize or reject Your installation of any Co-resident Third Party Programs in the Services Environment.
3. Provide self-service tools as available for You to promote CEMLI Changes into the Production Environment.
4. Apply software patches and make configuration or data Changes approved by You for the Managed Software which repair or modify existing functionality (including Changes to address performance, availability, and security), Changes to maintain currency with legislative requirements (including payroll and sales tax updates), and Changes to introduce or modify CEMLI in the Services Environment where Oracle determines the self-service tools provided by Oracle for promoting CEMLI cannot be used.
5. Provide a Back Out Plan for Changes made by Oracle.
6. Assist You with Change bundling analysis to reduce the frequency and length of the time required to apply Changes.
7. Control Changes to the Production Environment and Production Support Environment(s) and apply Changes when access restrictions prevent You from applying the Change.
8. Define and support operating system printer queues and application printer definition when access restrictions prevent You from establishing and managing printers.

Customer Responsibilities

1. Work with Oracle to determine schedules for Changes.
2. Apply software patches and configuration or data Changes in Non-Production Environments following initial installation of the Managed Software for which You have purchased Oracle Managed Services for Oracle Cloud for US Government Services.
3. Execute application functional setup Changes as required.
4. Test and validate completed Changes.
5. Obtain and maintain licenses and technical support for the Managed Software.
6. Assist Oracle as needed for any Change Management of Co-resident Third Party Programs.
7. Use self-service tools provided by Oracle to promote CEMLI Changes to the Production Environment and Production Support Environment.

8. Maintain CEMLI code and documentation and comply with Oracle practices when creating or modifying CEMLI to be installed in the Services Environment.
9. Perform performance testing of the Managed Software prior to Production Go-Live where not prohibited by Oracle Cloud for US Government policies.
10. Establish and manage printers, including monitoring of printer queues.
11. Submit and update a Request for Change (RFC) for all Change Management activities.
12. Notify Oracle in advance of all planned changes to Your Tenancy where the Oracle Managed Compartment(s) reside.

Oracle Managed Services for Oracle Cloud for US Government Configuration Management Policy

Scope

Oracle will manage configuration data for the Oracle Programs and Required Software.

For the Services, Oracle will:

1. Maintain and document changes for all configuration items.
2. Maintain architecture documents that represent the current configuration of the Services.

Customer Responsibilities

1. Maintain and document changes to version information for all configuration items for Co-resident Third Party Programs.
2. Provide Oracle information on configuration and architecture of Co-resident Third Party Programs.
3. Ensure Changes to architecture components managed by You that could impact Your Services are communicated to Oracle in advance of such Changes, including Changes to Your Oracle Cloud for US Government cloud services.

Oracle Managed Services for Oracle Cloud for US Government Release Management Policy

Scope

Oracle will provide Release Management for the Oracle Programs and Required Software in an effort to improve performance, functionality, security, availability, stability, or manageability. In addition to the Oracle Cloud for US Government Maintenance Windows, Oracle reserves a monthly four-hour Maintenance Window and a quarterly eight-hour Maintenance Window.

For the Services, Oracle will:

1. Develop a Periodic Maintenance Plan ("PMP").
2. Perform periodic Refreshes of Production Support Environment(s) and Non-Production Environment(s) from the Production Environment.
3. Execute Changes in a Release Plan for the Managed Software when access restrictions prevent You from applying the Change.
4. Perform Emergency Release Management for the Services as necessary, at its discretion, to resolve critical availability, performance, or security issues.

Customer Responsibilities

1. Approve the PMP schedule.
2. Provide a Release Plan for each Release.
3. Execute Changes in a Release Plan for Co-Resident Third Party Programs and any other responsibilities in the Release Plan designated for You.
4. Submit and update a Service Request for all Release Management activities.

Oracle Managed Services for Oracle Cloud for US Government Incident and Problem Management Policy

Scope

Oracle will provide a Managed Cloud Service Desk to serve as the initial point of contact for the Oracle Programs and Required Software for Incident and Problem resolution requests as well as Change requests. SRs for Changes and any resolution or work around for Problems will be processed in accordance with the [Oracle Managed Services for Oracle Cloud for US Government Change Management Policy](#) or [Oracle Managed Services for Oracle Cloud for US Government Release Management Policy](#) described herein.

For the Services, Oracle will:

1. Receive, acknowledge, classify, and manage SRs and determine the type of request(s).
2. Route SRs to proper resolution queues.
3. Analyze recurring Incidents, including those that result in Outages or Service Interruptions within Your Services, and classify such recurring Incidents as Problems.
4. Use commercially reasonable efforts to implement a resolution or establish a workaround for Problems in accordance with these Delivery Policies.
5. Use commercially reasonable efforts to provide You with a written Root Cause Analysis for all Problems resulting in Severity Level 1 Production Environment Outages.
6. Track and manage Incidents, Problem SRs, and Requests for Change (RFCs) through to resolution.
7. Work on Incidents and changes related to the Supported Programs in a Non-Production Environments during standard business hours (between 8:00 a.m. and 5:00 p.m. in the North America time zone of Your site and/or location).

Customer Responsibilities

1. Be responsible for Your Help Desk services and End User training.
2. Assign Super Users to address functional issues involving Oracle Programs (e.g., “how to” questions) raised by Your End Users.
3. Submit SRs for all activities under these Delivery Policies requiring coordination and communication with Oracle and assist with resolution and closure of all SRs related to the Services.
4. Use the Request System for all SRs.
5. Assist Oracle with the identification of recurring Incidents.
6. Assist Oracle with analysis and resolution of Problems.

Severity Definitions

Each SR shall be assigned one of the following defined Severity Levels:

Table 2

Severity Level	Type	Environment	Severity Level Definition
1	Unplanned Outage (Caused by Infrastructure and/or Component)	Production	You experience an Unplanned Outage of a Production Environment. Use of the Oracle Programs to conduct business operations cannot reasonably continue, the operation is mission critical to the business and the situation is an emergency. A Severity Level 1 Incident results from an Infrastructure Outage or a component (system process) level failure, and has one or more of the following characteristics: • Production Environment is down and/or inaccessible to all of Your End Users • Data is corrupted, resulting in a complete halt to Your business operations in a Production Environment • Production Environment hangs indefinitely, causing indefinite delays for critical resources or application response
<u>1</u>	Unplanned Outage (Caused by Infrastructure)	Non-Production	You experience an Unplanned Outage of Infrastructure supporting a Non-Production Environment
<u>1</u>	Service Interruption (Functional Failure)	Production	You experience a Service Interruption within a Production Environment that causes a critical impact to Your use of the Oracle Programs in one area of Your business but is not the result of an Infrastructure Outage or component (system process) level failure. No acceptable workaround is available, and business operations related to the affected functionality cannot continue. The Incident is generally characterized by Oracle Program functionality issues, such as an inability to run a critical process during a close period.
2	N/A	Any	You experience an error in expected or documented functionality of Oracle Programs that has a severe impact on Your ability to use the Oracle Programs for business operations. No acceptable workaround is available; however, business operations in the Environment can continue in a restricted fashion.
3	N/A	Any	You experience an error in expected or documented functionality of Oracle Programs that has a moderate impact on Your ability to use the Oracle Programs for business operations. A workaround may be required to restore functionality.

Severity Level	Type	Environment	Severity Level Definition
4	N/A	Any	You experience a minor or no loss in expected or documented functionality of Oracle Programs. Severity Level 4 Service Requests may also represent requests for information, an enhancement, or documentation clarification regarding the Oracle Programs.

Service Request Escalation

You may view the progress of a resolution of an SR by viewing the SR in the Request System.

For the Services, Oracle will:

1. Assist You with escalating SRs as needed.
2. Track and monitor any formally escalated SRs and Requests for Change (“RFCs”) through to resolution.
3. Manage escalated SRs and RFCs arising from or related to Oracle-initiated Infrastructure events.

Customer Responsibilities:

1. Initiate an escalation when the urgency of an Incident has increased due to business requirements.
2. Provide Oracle with information and cooperation as requested by Oracle regarding escalated SRs and RFCs.
3. Respond to requests for information and cooperation in a timely manner as determined by the urgency of the escalation.

Oracle Managed Services for Oracle Cloud for US Government Monitoring Policy

Scope

Oracle will establish monitoring and utilize monitoring event data available through Your use of Oracle Cloud for US Government to obtain information on the operational state, performance and configuration of the Oracle Programs and Required Software.

For the Services, Oracle will:

1. Install and configure monitoring software required by Oracle for delivery of the Services.
2. Initiate an Incident when a monitored event violates an established threshold.
3. Promptly report Outages and Service Interruptions to You when identified.
4. Provide start/stop services for the Production Environment and provide You single-command scripts to execute start/stop services for Production Support Environment(s) prior to Go-Live.

Customer Responsibilities

1. Promptly report Outages and Service Interruptions to the Managed Cloud Service Desk when identified.
2. Authorize access for the Managed Cloud Service Desk to all Oracle Cloud for US Government monitoring event data associated with the Services.

Oracle Managed Services for Oracle Cloud for US Government Service Level and Availability Management Policy

Scope

The Service Levels described in these Delivery Policies apply to the Oracle Programs and Required Software of the Production Environment(s). The change control process shall apply to any changes to the number or types of Production Environments that are subject to the Service Levels under these Delivery Policies. The performance of the Services shall be measured against the following three Service Levels: Application Availability, Service Request Resolution Time, and Performance Against Service Description.

Application Availability

The Application Availability Service Level consists of the measurement of the percentage of time that Production Environments are available for access and use by You to conduct business operations, and are measured by Oracle on a monthly basis, and calculated in accordance with the following formula:

$$\left\{ \frac{[\text{Total minutes in a calendar month} \times \text{number of Production Environments}] - \text{Sum of Unplanned Outage (caused by component or Infrastructure failure) minutes measured for each Production Environment in such month}}{\text{Total minutes in the calendar month} \times \text{number of Production Environments}} \right\} \times 100$$

Only Severity Level 1 Unplanned Outages caused by Infrastructure and/or component failures of a Production Environment shall be used to calculate Oracle's monthly performance against the Application Availability Service Level.

Incidents for which the root cause is subject to exclusions listed below, or that occur in a Production Environment during a Stabilization Period (as defined in below), shall not be included in the Application Availability calculation.

Service Request Resolution Time

The Service Request Resolution Time Service Level measures the elapsed time within which an SR for an Incident affecting a Production Environment is resolved (i.e., downgraded to a lower Severity Level or closed by Oracle). The resolution time commences when one of the following occurs:

- The submission of the SR via [the Request System](#)
- Oracle detects the Incident and logs the Incident as an SR in [the Request System](#)
- An SR is upgraded from Severity Level 3 or 4 to Severity Level 1 or 2

The Service Request Resolution Time Service Level shall be measured on a monthly basis for each SR Severity Level set forth in the Oracle Managed Services for Oracle Cloud for US Government Service Descriptions and calculated in accordance with the following formula:

$$\left\{ \frac{\text{(Total number of all SRs related to Production Environments for the applicable Severity Level which meet the time to close or downgrade such SRs in a calendar month)}}{\text{Total number of all SRs related to Production Environments for the applicable Severity Level in such calendar month}} \right\} \times 100$$

SRs for which the root cause is subject to exclusions listed below or that occur in a Production Environment during a Stabilization Period shall not be included in the Service Request Resolution Time calculation.

Performance Against Service Description Service Level

If You demonstrate that Oracle failed to perform Services in accordance with the applicable Service Description during a month, You shall be entitled to a Service Level Credit (as defined in the *Oracle Managed Services for Oracle Cloud for US Government - Service Descriptions*) for such failure for such month. Incidents for which the root cause is subject to exclusion listed below, or Incidents addressed by another Service Level under this section, shall not be included in the Performance Against Service Description Service Level.

Service Level Applicability

The Performance Against Service Description Service Level applies throughout the Services lifecycle.

The applicability of, and Oracle's obligations with respect to the measurement of, Oracle's performance of the Services against the Service Levels, and Service Level Credits for the Application Availability and Service Request Resolution Time Service Levels, during the three phases of the Services life cycle is outlined in the following table.

Table 3

Phase	Applicability of Service Levels and Credits for Application Availability and Service Request Resolution Time Service Levels
Prior to Production Go-Live	Service Levels will not be measured and do not apply prior to Production Go-Live, and Service Level Credits will not be paid to You.
Stabilization Period	Service Levels will be measured and reported during a ramp period following Changes to a Production Environment ("Stabilization Period"), but Service Level Credits will not be paid during such period. The following Changes require a Stabilization Period: (a) initial system implementation or migration, (b) Point Releases and Major Upgrades of application software, (c) introduction of CEMIs, (d) introduction of Third Party Software, (d) introduction of additional modules.
Production	Service Levels will be measured and reported during the production phase, and Your eligibility to receive Service Level Credits shall be in accordance with the terms of these Delivery Policies.

Each Stabilization Period will be sixty (60) calendar days in duration, commencing on the day that the Change is first made to the applicable Production Environment. However, depending on the nature of the Change and the impact on the applicable Production Environment, Oracle and You

may, as part of the Change Management process, mutually agree on a Stabilization Period of different scope or duration. Notwithstanding anything to the contrary in the applicable Service Description, for purposes of measuring and reporting Oracle's performance against Service Levels and calculating any applicable Service Level Credits for a calendar month in which a Stabilization Period occurs: (1) the Stabilization Period shall be deemed to commence on the first day of such calendar month; and (2) the Stabilization Period shall be deemed to end on the last day of such calendar month.

Service Level Objectives

The Service Request Response Time Service Level Objective measures the elapsed time from the submission of a Service Request in the Request System to Oracle's automated acknowledgement of the receipt of the SR in the Request System for an Incident affecting an Oracle Managed IaaS or PaaS Production Environment ("Time to Respond").

The Time to Respond objectives are set forth in the guidelines below and are not subject to any Service Level Credits, unless otherwise specifically defined in the applicable service description.

Service Level Objective	Service Level Target	Credit Criteria
Service Request Response Time	Severity Level 1 <= 15 minutes	<90% of Service Requests responded to within target
	Severity Level 2: <= 1 hour	
	Severity Level 3: Next business day	
	Severity Level 4: Next business day	

SRs for which the root cause is subject to the exclusions below or that occur in a Production Environment during a Stabilization Period shall not be included in the Time to Respond calculation.

Exclusions

Notwithstanding any provision or interpretation of these Delivery Policies to the contrary, Oracle's obligation to provide Service Level Credits shall be excused to the extent the failure to meet the applicable Service Levels: (a) occurs during a Planned Outage or during any other period in which the Services are temporarily suspended under the order; (b) is caused by changes to or failures of any equipment, hardware or Infrastructure component, including Oracle Managed Compartment(s), not provided or managed by Oracle as part of the Services under these Delivery Policies, including equipment owned or provided by You; (c) is caused by the Internet or any other connectivity or communication facility, which is outside of Oracle's control; (d) is caused by actions, omissions, delays or any type of failure of a Third Party Vendor retained by You, a third party service provider retained by You, or any Third Party Software, including Co-resident Third Party Programs; (e) is caused by a force majeure event; (f) is caused by a declared Disaster; (g) is caused by CEMLI or other customizations; (h) is caused by Your failure to perform the activities indicated in these Delivery Policies; (i) results from any software bugs; (j) occurs within a Non-Production Environment; (k) is the result of application functional setup, configuration or functionality issues that are not within the scope of the Services; (l) results from Your request to limit Oracle work to resolve a Severity Level 1 Service Request to time periods that are less than 24 hours per day, seven days per week; (m) occurs prior to the successful completion of a Production Managed Services for Oracle Cloud for US Government - Service Descriptions_v03242025

Assessment resulting in Production Ready Status (PR) for the applicable Production Environment(s); (n) results from recurrence of a Problem for which Oracle has identified and recommended a Release, patch or other fix that You have not allowed Oracle to implement in the Production Environment; (o) is the result of Your failure to follow any Oracle recommendation to add capacity to the Services or make architecture changes to achieve Service Levels; or (p) is the result of Your changes to access controls for the Services established by Oracle under these Delivery Policies.

Service Level Credit Allocations

Service Level targets, credit criteria, and fee credits (“Service Level Credits”) are identified in the applicable description within the Oracle Managed Services for Oracle Cloud for US Government Service Descriptions.

Oracle Managed Services for Oracle Cloud for US Government Capacity Management and Performance Advisory Policy

Scope

Capacity Management and Performance Advisory services are designed to enable and support joint Performance Management of the Oracle Programs, Required Software, and Co-resident Third Party Programs by resolving and preventing performance-related Incidents and Problems.

For the Services, Oracle will:

1. Provide general architecture and sizing guidelines for the Oracle Programs and Required Software for Your use to determine the appropriate amount of Oracle Cloud for US Government to achieve desired performance of the Services.
2. Analyze performance-related Incidents to identify factors adversely impacting performance and provide You with recommendations, as needed, for review of architecture configuration and capacity.
3. Resolve performance-related Incidents where possible through configuration changes to the Oracle Programs and Required Software or CEMLI code deactivation.
4. Provide performance advisory guidance specific to the Services as part of a capacity management plan updated periodically on a mutually agreed schedule.

Customer Responsibilities

1. Define, manage, schedule, monitor, purge, terminate and cancel Customer- developed batch jobs in accordance with business requirements.
2. Modify CEMLI as required to resolve a performance Incident or Problem.
3. Analyze and resolve Incidents caused by Co-resident Third Party Programs.
4. Follow general and specific guidance provided by Oracle regarding architecture or capacity required to resolve or prevent a Performance Incident or Problem.
5. Ensure desktop and network bandwidth connectivity meets the minimum requirements for performance of the Oracle Programs and Required Software.

Oracle Managed Services for Oracle Cloud for US Government Service Continuity Policy

Scope

Service continuity measures for the Managed Software in the Services are required in an effort to ensure the Services can be recovered in the event of hardware failure or human error.

For the Services, Oracle will:

1. Configure the Services for automated backup, including configuration of Oracle Cloud for US Government components.
2. Assist You to recover database and application functionality from backups as required.

Customer Responsibilities

1. Not purge any data from the Environment during periods designated for performing backups.
2. If applicable for the program being backed up, ensure that no users, including administrators, use the Services during periods designated for performing backups.
3. Archive Your Content.

Oracle Managed Services for Oracle Cloud for US Government Continual Service Improvement Policy

Scope

Oracle will provide account, service, and project governance services for the ongoing management of the Services and will make commercially reasonable efforts to work with You to improve Service utilization and performance using Service objective goals, reporting means and reporting frequency mutually agreed upon between You and Oracle.

For the Services, Oracle will:

1. Identify a management lead who will serve as Your primary point of contact for service governance.
2. Provide You with documentation and guidance on Oracle processes and standards and organize training on My Oracle Support.
3. Work with Your change control board to plan and schedule strategic business and technology events that affect delivery of the Services.
4. In an effort to support achievement of a mutually agreed Continuous Service Improvement objective, provide account reviews detailing services delivered and identifying potential additional services that may improve the Services.
5. Identify events and/or scenarios that may require You to purchase additional Oracle licenses, services and/or capacity.
6. Monitor, measure and report the operational performance of the Services.
7. Identify, prepare, and facilitate completion of corrective action via a service plan designed to address the operational performance of the Services.
8. Coordinate tactical business and technology events with You in an effort to minimize impact to the availability of Your Production Environment.
9. Track and monitor Planned Outages and Unplanned Outages as well as coordinate tactical business and technology events with You in an effort to meet availability and Continuous Service Improvement targets identified in the jointly developed availability plan.

10. Prepare, manage, and report status on, and perform Oracle-assigned activities for, projects for Infrastructure maintenance or upgrade events initiated by Oracle.
11. Assist You to escalate SRs, as appropriate.

Customer Responsibilities

1. Establish a change control board that consists of Your personnel authorized to make decisions about the Services.
2. Identify, and communicate to Oracle, Your business requirements with respect to the Services, including key business events that may affect the scheduling of Oracle-initiated activities.
3. Review and assess Your capacity and consumption details to identify any additional Oracle licenses, services, and/or capacity that You may need to purchase.
4. Provide to Oracle a single point of contact who Oracle can communicate with regarding the Services.

Oracle Managed Services for Oracle Cloud for US Government Enhanced Recovery Policy

Scope

Enhanced Recovery Services are designed to recover the Managed Software from a primary data center location to a secondary data center location in the event of a Disaster.

For the Services, Oracle will:

1. Advise You on architecture and capacity of the Services Environment located at a secondary data center location for the purpose of recovering the Production Environment, and on the method of data replication and synchronization relative to Your Recovery Time Objective and Recovery Point Objective.
2. Work jointly with You to develop, review, and approve a Disaster Recovery Plan.
3. Assign a Project Manager to coordinate development of the Disaster Recovery Plan and execution of annual testing of procedures.
4. Manage recovery activities for the Production Environment during a disaster recovery test or actual Disaster.
5. Provide a report following conclusion of a disaster recovery test.
6. In the event of a Disaster, re-establish the Production Environment(s), including recovering production data, on the Secondary Site Oracle Cloud for US Government compute resources purchased by You for recovery. Upon restoration of the Services at the Secondary Site following a Disaster, production use of such Services may be degraded or only partially available.
7. Work jointly with You to restore use of the Production Environment at the primary data center location.

Customer Responsibilities

1. Work jointly with Oracle to create and approve the Disaster Recovery Plan.
2. Purchase the amount of Oracle Cloud for US Government sufficient to achieve disaster recovery service objectives.

3. Schedule a disaster recovery test with Oracle at least four months in advance.
4. Provide the disaster recovery test plan to Oracle no less than four weeks prior to the disaster recovery test date.
5. Manage all aspects of business continuity for Your End Users, including management of reduced usage of the Services in the event the capacity purchased for the secondary data center is less than the primary data center for the Production Environment.
6. In the event You cancel a scheduled DR test with less than thirty (30) days' prior notice, such scheduled DR test shall be deemed a completed DR test.

Oracle Managed Services for Oracle Cloud for US Government Service Decommission Policy

Scope

Oracle will provide limited transition support associated with decommissioning the Services.

For the Services, Oracle will:

1. Identify an Oracle Decommission Contact and work with You to establish the departure date.
2. Confirm Your decommission and the Oracle Decommission Contact in writing after receipt of Your request to terminate the Services.
3. Following Your submission of an SR to complete decommission, perform a complete system password change, and provide You with interim password values.
4. On the departure date, remove any software programs provided by Oracle as part of the Services and cease all services in these Delivery Policies except for making the Oracle Decommission Contact available for one week after the departure date to answer Your questions related to the Services.
5. On the departure date, cease using the Oracle Cloud log-in credentials and private keys generated as part of Oracle Cloud for US Government on Your behalf for the Services.

Customer Responsibilities

1. Notify Oracle in writing of Your intent to terminate the Services.
2. Obtain qualified applications database administration (DBA) and Oracle DBA resources to assist with the decommission and to assume Your responsibility for all backups of Your system following termination of the Services.
3. At least two weeks prior to Departure Date:
 - a. Identify a Decommission Contact from Your organization.
 - b. Confirm the final departure date with Oracle.
 - c. Complete and return to the Oracle Decommission Contact the Managed Cloud Services Decommission Customer Agreement and Managed Cloud Services Decommission Transition Plan indicating expected completion dates for each of Your tasks in the plan.
 - d. Have the option to submit an SR to obtain a list of operating system, database, and applications user accounts managed by Oracle and used by You as well as backup schedules associated with the Services.
4. At least one week prior to the departure date, submit an SR to complete decommission.

5. Perform a complete system password change to values unknown to Oracle.

ⁱ A “day” is defined as one (1) resource working up to eight (8) hours per day.