



**Alternate Contract Source (ACS)
No. 43230000-NASPO-16-ACS
For
Cloud Solutions**

This Alternate Contract Source No. 43230000-NASPO-16-ACS; Cloud Solutions (Contract), is between the Department of Management Services ("Department" or "Participating Entity," as defined in the Master Agreement), an agency of the State of Florida (State), located at 4050 Esplanade Way, Tallahassee, FL 32399, and Oracle America, Inc. ("Contractor" or "Oracle"), located at 500 Oracle Parkway, Redwood Shores, CA 94065 collectively referred to herein as the "Parties."

WHEREAS, the Department is authorized by section 287.042(16), Florida Statutes:

To evaluate contracts let by the Federal Government, another state, or a political subdivision for the provision of commodities and contract services, and, if it is determined in writing to be cost-effective and the best value to the state, to enter into a written agreement authorizing an agency to make purchases under such contract.

WHEREAS, the State of Utah, acting by and through the National Association of State Procurement Officials (NASPO) ValuePoint, competitively procured Cloud Solutions and executed AR2487, Cloud Solutions (Master Agreement), with the Contractor;

WHEREAS, the Department evaluated the Master Agreement and determined that use of the Master Agreement is cost-effective and the best value to the state.

NOW THEREFORE, in consideration of the mutual promises contained herein, the receipt and sufficiency of which are hereby acknowledged, the Parties agree as follows:

1. Term and Effective Date.

The Master Agreement became effective March 1, 2017, and its term currently ends on September 15, 2026. The Master Agreement has no renewals available. The Contract will become effective on the date signed by all Parties. The Contract will expire on September 15, 2026, unless terminated earlier or renewed in accordance with Exhibit A, Contract Conditions.

2. Order of Precedence.

This Contract document and the attached exhibits constitute the Contract and the entire understanding of the Parties. Exhibits A, B, C, and this Contract document constitute the Participating Addendum ("Participating Addendum" or "Addendum" or "PA") to the Master

Agreement and modify or supplement the terms and conditions of the Master Agreement. All exhibits listed below are incorporated by reference into, and form part of, this Contract. In the event of a conflict, the following order of precedence shall apply:

- a) This Contract document
- b) Exhibit A: Contract Conditions
- c) Exhibit B: [Master Agreement](#), incorporated by reference (including any amendments made prior to the effective date of this Contract and any subsequent amendments added to this Contract in accordance with the Modifications Section listed below)
- d) Exhibit C: Contractor Selection Justification Form

Pursuant to Section 37 of the Master Agreement, the Parties agree that by executing the Participating Addendum, this Participating Addendum shall be governed by the laws of the Participating Entity's State which, for the avoidance of doubt, shall be the laws of the State of Florida. Refer to the Modification and Severability section of Exhibit A, Contract Conditions.

3. Purchases off this Contract.

Upon execution of this Contract, agencies, as defined in section 287.012, Florida Statutes, may purchase products and services under this Contract. Any Customer making a purchase off of this Contract acknowledges and agrees to be bound by the terms and conditions of this Contract. The Parties shall adhere to the mutually agreed-upon terms in writing included in any contract or purchase orders issued pursuant to this Contract. Each Customer shall be responsible for its compliance with and breach(es) of such terms and conditions. The terms of the Ordering Document, as defined in the Master Agreement, shall apply to the extent that the Oracle order terms and other mutually agreed upon terms will not materially reduce either party's obligations under this Contract. **CUSTOMERS ARE RESPONSIBLE FOR REVIEWING THE TERMS AND CONDITIONS OF THE PA AND ANY ORDERING DOCUMENT.**

Certain Oracle-authorized resellers ("Authorized Resellers" or "Fulfillment Partner") are eligible to resell Services to Customers under the Addendum. Such Authorized Resellers, if any, are authorized to take orders under the Addendum and invoice and receive payment from Customers. The parties agree that for any acquisitions made through an Authorized Reseller, any obligations which apply solely to Oracle in their capacity as a cloud service provider shall remain in effect. Oracle is responsible for any reports and/or fees that are required per the terms and conditions of the Master Agreement and/or the Addendum, unless expressly stated otherwise herein. Participation of Authorized Resellers, if any, will be in accordance with the terms and conditions set forth in the Master Agreement and the Addendum. Authorized Resellers under the Addendum, if any, are subject to the Department's approval which will be demonstrated by executing an Authorized Reseller Agreement with the Department. Approved Authorized Resellers will be listed on the Department's website.

Unless otherwise handled by an Authorized Reseller, Orders and payments may be made directly to Oracle. If an Authorized Reseller is authorized to receive payment from a Customer under this Addendum, then any dispute between the Contractor and the Authorized Reseller

regarding monies owed shall be resolved between the Contractor and the Authorized Reseller. Orders through an Authorized Reseller shall be submitted as directed to such Authorized Reseller. Orders placed directly with Oracle are to be submitted as directed to Oracle's sales representative.

4. Primary Contacts.

Department's Contract Manager:

Bradley Beech
Division of State Purchasing
Florida Department of Management Services
4050 Esplanade Way, Suite 360
Tallahassee, Florida 32399-0950
Telephone: (850) 487-9847
Email: Bradley.Beech@dms.fl.gov

Contractor's Contract Manager:

Dapo Lawal Contract Manager
Oracle America, Inc.
1910 Oracle Way
Reston, VA 20190
dapo.lawal@oracle.com

5. Cloud Computing Requirements.

Oracle products comply as stated in the documentation provided to a Customer related to an order from this Contract. Oracle acknowledges the Customer is subject to the requirements under Rule Titles 60FF and 60GG, Florida Administrative Code (F.A.C.), as applicable. The Contractor will provide information and work with the Customer in their attempts to meet these requirements.

6. Request for Quotes.

Customers purchasing Cloud Solutions from this Participating Addendum shall create a Request for Quote (RFQ), each time they desire to purchase Cloud Solutions. The Customer shall issue a detailed RFQ to the ACS Contractor(s) who offer(s) the applicable cloud solution(s). The specific format of the RFQ is left to the discretion of the Customer, but must contain the following:

- a) Applicable service and deployment model(s);
- b) Data security classification;
- c) Service level agreement requirements; and
- d) Exit strategy considerations.

7. Contractor Selection Justification Form.

Customers purchasing Cloud Solutions from this Participating Addendum shall attach to the purchase order a completed Contractor Selection Justification Form (Exhibit C) of this Participating Addendum, incorporated herein by reference and accessible at:
https://www.dms.myflorida.com/business_operations/state_purchasing/state_contracts_and_agreements/alternate_contract_source/cloud_solutions/forms.

8. Modifications.

Any amendments to this Contract must be in writing and signed by the Parties. If amendments are made to the Master Agreement after the effective date of this Contract, the Contractor shall notify the Department of such amendments.

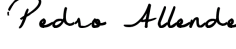
IN WITNESS THEREOF, the Parties hereto have caused this Contract to be executed by their duly authorized undersigned officials or signatories.

ORACLE AMERICA, INC.

**STATE OF FLORIDA,
DEPARTMENT OF MANAGEMENT SERVICES**

DocuSigned by:

B08D81052A88411...
**Michael Estrada,
Sr. Manager Deal Management**

DocuSigned by:

C94713929499485...
Pedro Allende, Secretary

6/27/2024 | 9:13 AM PDT

Date:

6/27/2024 | 3:42 PM EDT

Date:



EXHIBIT A **CONTRACT CONDITIONS**

The Contractor and Customers acknowledge and agree to be bound by the terms and conditions of the Master Agreement except as otherwise specified in the Department's Contract as modified and supplemented by these Contract Conditions.

In accordance with Rule 60A-1.002(7), F.A.C., Form PUR 1000 is included herein by reference but is superseded in its entirety by these Contract Conditions.

Contractor acknowledges that the Participating State is an agency of the State of Florida and as such, the Contract will include the terms and conditions in these Contract Conditions. All references to the Contract in these Contract Conditions include the terms and conditions herein.

SECTION 1. DEFINITION.

The following definition applies in addition to the definitions in Chapter 287, Florida Statutes (F.S.), and Rule Chapter 60A-1, Florida Administrative Code (F.A.C.):

1. Customer.

The agency or eligible user that purchases commodities or contractual services pursuant to the Contract. "Customer," shall also be referred to as "Purchasing Entity," as defined in the Master Agreement.

SECTION 2. CONTRACT TERM AND TERMINATION.

2.1 Initial Term.

The initial term will begin on the date set forth in the Contract documents or on the date the Contract is signed by all Parties, whichever is later.

2.2 Renewal.

Upon written agreement, the Department and Contractor may renew the Contract in whole or in part only as set forth in the Contract documents, and in accordance with section 287.057(14), F.S.

2.3 Suspension of Work and Termination.

2.3.1 Suspension of Work.

See section 7 (Termination) of Attachment A to the Master Agreement.

2.3.2 Termination for Convenience.

See section 7 (Termination) of Attachment A to the Master Agreement.

2.3.3 Termination for Cause.

See section 7 (Termination) of Attachment A to the Master Agreement.

SECTION 3. PAYMENT AND FEES.

3.1 Pricing.

The Contractor will not exceed the pricing set forth in the Contract documents. See section 6 (Discount Guarantee Period) of Attachment A and Attachment C to the Master Agreement.

3.2 Payment Invoicing.

See section 21 (FEES AND TAXES) of Attachment A to the Master Agreement and if applicable, shall adhere to the requirements of 287.058(1)(a), F.S.

3.3 Purchase Order

A Customer may use purchase orders to buy contractual services pursuant to the Contract and, if applicable, the Contractor must provide contractual services pursuant to purchase orders. Purchase orders issued pursuant to the Contract must be received by the Contractor no later than the close of business on the last day of the Contract's term. The Contractor is required to accept timely purchase orders specifying delivery schedules that extend beyond the Contract term even when such extended delivery will occur after expiration of the Contract. Purchase orders shall be valid through their specified term and performance by the Contractor, and all terms and conditions of the Contract shall survive the termination or expiration of the Contract and apply to the Contractor's performance. The duration of purchase orders for recurring deliverables shall not exceed the expiration of the Contract by more than twelve months. Any purchase order terms and conditions conflicting with these Contract Conditions shall not become a part of the Contract.

3.4 Travel.

Travel expenses are not reimbursable unless specifically authorized by the Customer in writing in the applicable Ordering Document and may be reimbursed only in accordance with section 112.061, F.S.

3.5 Annual Appropriation.

Pursuant to section 287.0582, F.S., if the Contract binds the State of Florida or an agency for the purchase of services for a period in excess of one fiscal year, the State of Florida's performance and obligation to pay under the Contract is contingent upon an annual appropriation by the Legislature. Notwithstanding the foregoing, (a) for each of the whole or partial 12-month terms of the applicable Order, Customer must provide a purchase order, and (b) Customer's issuance of each whole or partial 12-month purchase order shall signify that all funds for the whole or partial 12-month term have been fully appropriated and encumbered for the applicable fiscal year. Customer agrees to pay for all services performed by Oracle prior to Oracle's or the Authorized Reseller's receipt of Customer's notice of non-appropriations.

Exhibit A, Contract Conditions

Oracle America, Inc. Contract No. 43230000-NASPO-16-ACS

Page 2 of 17

3.6 Transaction Fees

The State of Florida, through the Department of Management Services, has instituted MyFloridaMarketPlace, a statewide eProcurement system. Pursuant to Section 287.057(24), F.S., all payments shall be assessed a Transaction Fee of one percent (1.0%), or as may otherwise be established by law, which the vendor shall pay to the State.

For payments within the State accounting system (FLAIR or its successor), the Transaction Fee shall, when possible, be automatically deducted from payments to the vendor. If automatic deduction is not possible, the vendor shall pay the Transaction Fee pursuant to subsection 60A-1.031(2), F.A.C. By submission of these reports and corresponding payments, vendor certifies their correctness. All such reports and payments shall be subject to audit by the State or its designee.

The vendor shall receive a credit for any Transaction Fee paid by the vendor for the purchase of any item(s) if such item(s) are returned to the vendor through no fault, act, or omission of the vendor. Notwithstanding the foregoing, a Transaction Fee is non-refundable when an item is rejected or returned, or declined, due to the vendor's failure to perform or comply with specifications or requirements of the agreement.

Vendors will submit any monthly reports required pursuant to the rule. All such reports and payments will be subject to audit. Failure to comply with the payment of the Transaction Fees or submission of required reporting of transactions shall constitute grounds for declaring the Vendor in default.

3.7 Taxes.

Taxes, customs, and tariffs on commodities or contractual services purchased under the Contract will not be assessed against the Customer or Department unless authorized by Florida law.

3.8 Return of Funds.

Contractor will return any overpayments due to unearned funds or funds disallowed pursuant to the terms of the Contract that were disbursed to the Contractor. The Contractor must return any overpayment within forty (40) calendar days after either discovery by the Contractor, its independent auditor, or notification by the Department or Customer of the overpayment.

SECTION 4. CONTRACT MANAGEMENT.

4.1 Composition and Priority.

The Contractor agrees to provide contractual services to the Customer as specified in the Contract. Additionally, the terms of the Contract supersede the terms of all prior agreements between the Parties on this subject matter.

4.2 Notices.

All notices required under the Contract must be delivered to the designated Contract Manager.

4.3 Department's Contract Manager.

The Department's Contract Manager, who is primarily responsible for the Department's oversight of the Contract, will be identified in a separate writing to the Contractor upon Contract signing in the following format:

Department's Contract Manager Name
Department's Name
Department's Physical Address
Department's Telephone #
Department's Email Address

If the Department changes the Contract Manager, the Department will notify the Contractor. Such a change does not require an amendment to the Contract.

4.4 Contractor's Contract Manager.

The Contractor's Contract Manager, who is primarily responsible for the Contractor's oversight of the Contract performance, will be identified in a separate writing to the Department upon Contract signing in the following format:

Contractor's Contract Manager Name
Contractor's Name
Contractor's Physical Address
Contractor's Telephone #
Contractor's Email Address

4.5 Diversity.

4.5.1 Office of Supplier Diversity.

The State of Florida supports its diverse business community by creating opportunities for woman-, veteran-, and minority-owned small business enterprises to participate in procurements and contracts. The Department encourages supplier diversity through certification of woman-, veteran-, and minority-owned small business enterprises and provides advocacy, outreach, and networking through regional business events. For additional information, please contact the Office of Supplier Diversity (OSD) at osdinfo@dms.myflorida.com.

4.6 RESPECT.

If applicable, subject to the agency determination provided for in section 413.036, F.S., the following statement must be included in the Ordering Document:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES THAT ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM A NONPROFIT AGENCY FOR THE BLIND OR FOR THE SEVERELY HANDICAPPED THAT IS QUALIFIED PURSUANT TO CHAPTER 413, FLORIDA STATUTES, IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 413.036(1) AND (2), FLORIDA STATUTES; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT

SHALL BE DEEMED TO BE SUBSTITUTED FOR THE STATE AGENCY INSOFAR AS DEALINGS WITH SUCH QUALIFIED NONPROFIT AGENCY ARE CONCERNED.

Additional information about RESPECT and the commodities or contractual services it offers is available at <https://www.respectofflorida.org>.

4.7 PRIDE.

If applicable, subject to the agency determination provided for in sections 287.042(1) and 946.515, F.S., the following statement must be included in the Ordering Document:

IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT ANY ARTICLES WHICH ARE THE SUBJECT OF, OR REQUIRED TO CARRY OUT, THIS CONTRACT SHALL BE PURCHASED FROM THE CORPORATION IDENTIFIED UNDER CHAPTER 946, F.S., IN THE SAME MANNER AND UNDER THE SAME PROCEDURES SET FORTH IN SECTION 946.515(2) AND (4), F.S.; AND FOR PURPOSES OF THIS CONTRACT THE PERSON, FIRM, OR OTHER BUSINESS ENTITY CARRYING OUT THE PROVISIONS OF THIS CONTRACT SHALL BE DEEMED TO BE SUBSTITUTED FOR THIS AGENCY INSOFAR AS DEALINGS WITH SUCH CORPORATION ARE CONCERNED.

Additional information about PRIDE and the commodities or contractual services it offers is available at <https://www.pride-enterprises.org>.

SECTION 5. COMPLIANCE WITH LAWS.

5.1 Conduct of Business.

The Contractor must comply with all laws, rules, codes, ordinances, and licensing requirements that are directly applicable to the provision of products and services procured under this Contract, including those of federal, state, and local agencies having jurisdiction and authority. See section 17 (Laws and Regulations – Compliance with Laws) of Attachment A to the Master Agreement.

Nothing contained within this Contract shall be construed to prohibit the **Contractor** from disclosing information relevant to performance of the Contract or purchase order **to members or staff of the Florida Senate or Florida House of Representatives**.

Pursuant to section 287.057(26), F.S., the Contractor shall ensure a representative will be available to team members of the continuing oversight team.

The Contractor will comply with all applicable disclosure requirements set forth in section 286.101, F.S. In the event the Department of Financial Services issues the Contractor a final order determining a third or subsequent violation pursuant to section 286.101(7)(c), F.S., the Contractor shall, unless prohibited by law, promptly notify the Department and shall be disqualified from Contract eligibility.

5.2 Dispute Resolution, Governing Law, and Venue.

Notwithstanding applicable Florida Law, see sections 10 (Defaults and Remedies) and 37 (Governing Law and Venue) of Attachment A to the Master Agreement.

5.3 Department of State Registration.

Consistent with Title XXXVI, F.S., the Contractor and any subcontractors that assert status, other than a sole proprietor, must provide the Department with conclusive evidence of a certificate of status, not subject to qualification, if a Florida business entity, or of a certificate of authorization if a foreign business entity.

5.4 Convicted, Discriminatory, Antitrust Violator, and Suspended Vendor Lists.

In accordance with sections 287.133, 287.134, and 287.137, F.S., the Contractor is hereby informed of the provisions of sections 287.133(2)(a), 287.134(2)(a), and 287.137(2)(a), F.S. For purposes of this Contract, a person or affiliate who is on the Convicted Vendor List, the Discriminatory Vendor List, or the Antitrust Violator Vendor List may not perform work as a contractor, supplier, subcontractor, or consultant under the Contract. The Contractor must notify the Department if it or any of its suppliers, subcontractors, or consultants have been placed on the Convicted Vendor List, the Discriminatory Vendor List, or the Antitrust Violator Vendor List during the term of the Contract.

In accordance with section 287.1351, F.S., a vendor placed on the Suspended Vendor List may not enter into or renew a contract to provide any goods or services to an agency after its placement on the Suspended Vendor List.

A firm or individual placed on the Suspended Vendor List pursuant to section 287.1351, F.S., the Convicted Vendor List pursuant to section 287.133, F.S., the Antitrust Violator Vendor List pursuant to section 287.137, F.S., or the Discriminatory Vendor List pursuant to section 287.134, F.S., is immediately disqualified from Contract eligibility.

5.5 Scrutinized Companies - Termination by the Department.

The Department may, at its option, terminate the Contract if the Contractor is found to have submitted a false certification as provided under section 287.135(5), F.S., or been placed on the Scrutinized Companies with Activities in Sudan List or the Scrutinized Companies with Activities in the Iran Terrorism Sectors List, or been engaged in business operations in Cuba or Syria, or to have been placed on the Scrutinized Companies that Boycott Israel List or is engaged in a boycott of Israel.

5.6 Cooperation with Inspector General.

Pursuant to section 20.055(5), F.S., the Contractor understands and will comply with its duty to cooperate with the Inspector General in any investigation, audit, inspection, review, or hearing.

5.7 Foreign Country of Concern Attestation.

If the Contract or Customer's purchase order issued pursuant to this Contract grants the Contractor access to an individual's personal identifying information as defined in section 501.171, F.S., the Customer shall provide the Form PUR 1355, "Foreign Country of Concern Attestation Form," available at: <http://www.flrules.org/Gateway/reference.asp?No=Ref-15958> to the Contractor, and

the Contractor must, prior to execution, extension, or renewal of this Contract or Customer purchase order, complete and submit to the applicable Governmental Entity the Form PUR 1355.

SECTION 6. MISCELLANEOUS.

6.1 Subcontractors.

The Contractor will not subcontract any work for professional or consulting services under the Contract without prior written consent of the Department. The Contractor is fully responsible for the completion of all subcontracted work for professional or consulting services in accordance with an applicable Statement of Work. The Department supports diversity in its procurements and contracts, and requests that the Contractor offer subcontracting opportunities to certified woman-, veteran-, and minority-owned small businesses. The Contractor may contact the OSD at osdhelp@dms.myflorida.com for information on certified small business enterprises available for subcontracting opportunities.

6.2 Assignment.

See section 5 (Assignment/Subcontracts) of Attachment A to the Master Agreement.

6.3 Independent Contractor.

In the event of any assignment, the Contractor remains responsible for any obligations it has under the Contract prior to the effective date of the assignment.

See section 14 (Independent Contractor) of Attachment A to the Master Agreement.

6.4 Inspection and Acceptance of Commodities.

6.4.1 Risk of Loss.

The provisions of this section (6.4.1 Risk of Loss) apply only to hardware associated with Cloud at Customer (C@C) Cloud Services ordered under the Contract. Matters of inspection and acceptance are addressed in section 215.422, F.S. Until acceptance, risk of loss or damage will remain with the Contractor. The Contractor will be responsible for filing, processing, and collecting all damage claims. To assist the Contractor with damage claims, the Customer will: record any evidence of visible damage on all copies of the delivering carrier's bill of lading; report damages to the carrier and the Contractor; and provide the Contractor with a copy of the carrier's bill of lading and damage inspection report.

6.5 Ombudsman.

A Vendor Ombudsman has been established within the Department of Financial Services. The duties of this office are found in section 215.422, F.S., which include disseminating information relative to prompt payment and assisting contractors in receiving their payments in a timely manner from a Customer. The Vendor Ombudsman may be contacted at (850) 413-5516.

6.6 Waiver.

See section 33 (Waiver of Breach) of Attachment A to the Master Agreement.

6.7 Modification and Severability.

Purchase Orders issued in accordance with this agreement, and any subsequent written agreements may only be modified by written agreement between the Customer and the Contractor. This Contract may only be modified by written agreement between the Department and the Contractor.

See section 44.k(i) of Attachment A to the Master Agreement.

6.8 Cooperative Purchasing.

Pursuant to their own governing laws, and subject to the agreement of the Contractor, governmental entities that are not Customers may make purchases under the terms and conditions contained herein, if agreed to by Contractor. Such purchases are independent of the Contract between the Department and the Contractor, and the Department is not a party to these transactions. Agencies seeking to make purchases under this Contract are required to follow the requirements of Rule 60A-1.045(6), F.A.C.

SECTION 7. LIABILITY AND INSURANCE.

See section 16 (Insurance) of Attachment A to the Master Agreement.

7.1 Indemnification.

To the extent not prohibited by Florida law, section 13 (Indemnification) of Attachment A to the Master Agreement shall apply.

7.2 Limitation of Liability.

To the extent not prohibited by Florida law, 44.f (Limitation of Liability) of Attachment A to the Master Agreement shall apply.

SECTION 8. PUBLIC RECORDS, TRADE SECRETS, DOCUMENT MANAGEMENT, AND INTELLECTUAL PROPERTY.

8.1 Public Records.

8.1.1 Termination of Contract.

The Department may terminate the Contract for refusal by the Contractor to allow access to public records, as defined in Chapter 119, F. S., made or received by the Contractor in conjunction with the Contract unless the records are exempt from s. 24(a) of Art. I of the State Constitution and section 119.071(1), F.S.

8.1.2 Statutory Notice.

Pursuant to section 119.0701(2)(a), F.S. if applicable, for contracts for services with a contractor acting on behalf of a public agency, as defined in section 119.011(2), F.S., the following applies:

IF THE CONTRACTOR HAS QUESTIONS REGARDING THE APPLICATION OF CHAPTER 119, FLORIDA STATUTES, TO THE CONTRACTOR'S DUTY TO PROVIDE PUBLIC RECORDS RELATING TO THIS CONTRACT, CONTACT THE DEPARTMENT'S CONTRACT MANAGER LISTED IN SECTION 4.3 OF THE CONTRACT CONDITIONS.

Pursuant to section 119.0701(2)(b), F.S., for contracts for services with a contractor acting on behalf of a public agency as defined in section 119.011(2), F.S., the Contractor shall:

(a) Keep and maintain public records required by the public agency to perform the service.

(b) Upon request from the public agency's custodian of public records, provide the public agency with a copy of the requested records or allow the records to be inspected or copied within a reasonable time at a cost that does not exceed the cost provided in Chapter 119, F.S., or as otherwise provided by law.

(c) Ensure that public records that are exempt or confidential and exempt from public records disclosure are not disclosed except as authorized by law for the duration of the Contract term and following the completion of the Contract if the Contractor does not transfer the records to the public agency.

(d) Upon completion of the Contract, transfer, at no cost, to the public agency all public records in possession of the Contractor or keep and maintain public records required by the public agency to perform the service. If the Contractor transfers all public records to the public agency upon completion of the Contract, the Contractor shall destroy any duplicate public records that are exempt or confidential and exempt from public records disclosure requirements. If the Contractor keeps and maintains public records upon completion of the Contract, the Contractor shall meet all applicable requirements for retaining public records. All records stored electronically must be provided to the public agency, upon request from the public agency's custodian of public records, in a format that is compatible with the information technology systems of the public agency.

8.2 Protection of Trade Secrets or Otherwise Confidential Information.

See section 8 (Confidentiality, Non-Disclosure, and Injunctive Relief) of Attachment A to the Master Agreement.

8.2.1 Contractor Designation of Trade Secrets or Otherwise Confidential Information.

If the Contractor considers any portion of materials to be trade secret under section 688.002 or 812.081, F.S., or otherwise confidential under Florida or federal law, the Contractor must

clearly designate that portion of the materials as trade secret or otherwise confidential when submitted to the Department.

8.2.2 Indemnification Related to Confidentiality of Materials.

If an action is brought pursuant to Chapter 119 of the Florida Statutes or the "Public Records Law," to compel the Department to disclose information marked trade secret or otherwise confidential under Florida or federal law, the Contractor agrees that it will intervene in the action through its counsel, provided that the Department notifies the Contractor promptly in writing, not later than 30 days after the Department receives notice of the claim (or sooner if required by applicable law). Provided that the Department provides notice as described in the prior sentence, the Contractor will defend, indemnify and hold harmless the Department for claims, costs, damages, fines, and attorney's fees awarded against the Department in such an action and costs and expenses related to the cause of action brought by a third party.

8.3 Document Management.

See section 26 (Records Administration and Audit) of Attachment A to the Master Agreement.

8.4 Intellectual Property.

See section 1(Data Ownership and Rights Granted) of Exhibits 1, 2, 3 to Attachment A to the Master Agreement.

SECTION 9. DATA SECURITY.

The Contractor will maintain appropriate technical and organizational security measures as identified in this section and identified in the Contractor's product-specific and/or service-specific documentation for the Processing of Your Content designed to prevent accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Information. These security measures govern all areas of security applicable to the Services, including physical access, system access, data access, transmission and encryption, input, data backup, data segregation and security oversight, enforcement and other security controls and measures.

For Cloud Services, Your Content will be stored in the data center region You choose and as specified in Your Order for such services or, if applicable, the geographic region that You have selected when activating such Services, and Your Content stays within such region unless You choose to move Your Content outside the region. The Contractor shall maintain multiple regions within the continental United States, and the Customer shall select the United States data center region. Pursuant to FAC 60GG-4.002(6), the Contractor will not host, store, or move where any State of Florida data is hosted or stored outside the United States.

The Contractor has implemented controls and policies designed to detect and promptly respond to incidents that create suspicion of or indicate destruction, loss, alteration, unauthorized disclosure or access to Your Content (as such term is defined in the Master Agreement) transmitted, stored or otherwise Processed. The Contractor will promptly define escalation paths to investigate such incidents in order to confirm if an Information Breach has occurred, and to take reasonable measures designed to identify the root cause(s) of the Information Breach, mitigate any possible adverse effects and prevent a recurrence.

The Contractor will notify you of a confirmed Information Breach without undue delay but at the latest within 24 hours. As information regarding the Information Breach is collected or otherwise reasonably becomes available to the Contractor, the Contractor will also provide You with (i) a description of the nature and reasonably anticipated consequences of the Information Breach; (ii) an anticipated timeline of the measures taken to mitigate (which may include remediation or cure) and any possible adverse effects and prevent a recurrence; and (iii) where possible, information about the types of information that were the subject of the Information Breach.

Additionally, the Contractor must adhere to the applicable requirements for reporting of data breaches as defined in Section 501.171, F.S.

See Section 8 (Confidentiality, Non-Disclosure, and Injunctive Relief) of Attachment A to Master Agreement and the Services Specifications (as defined in Section 2 (Definitions) of the Master Agreement), which include Hosting and Delivery Policies, and the Data Processing Agreement.

SECTION 10. GRATUITIES, LOBBYING, AND COMMUNICATIONS.

10.1 Gratuities.

The Contractor will not, in connection with this Contract, directly (1) offer, give, or agree to give anything of value to anyone as consideration for any State of Florida officer's or employee's decision, opinion, recommendation, vote, other exercise of discretion, or violation of a known legal duty, or (2) offer, give, or agree to give to anyone anything of value for the benefit of, or at the direction or request of, any State of Florida officer or employee.

10.2 Lobbying.

In accordance with sections 11.062 and 216.347, F.S., Contract funds are not to be used for the purpose of lobbying the Legislature, the judicial branch, or the Department. Pursuant to section 287.058(6), F.S., the Contract does not prohibit the Contractor from lobbying the executive or legislative branch concerning the scope of services, performance, term, or compensation regarding the Contract after the Contract is executed and during the Contract term.

10.3 Communications.

10.3.1 Contractor Communication or Disclosure.

The Contractor shall not make any public statements, press releases, publicity releases, or other similar communications concerning the Contract, its subject matter, or any information that pertains to the potential work or activities covered by the Contract, without first notifying the Contract Manager and securing the Customer's prior written consent.

SECTION 11. CONTRACT MONITORING.

11.1 Performance Standards.

The Contractor agrees to perform all applicable tasks, deliverables, and services as set forth in the Contract and the applicable Ordering Document. The Department and the Customer will be entitled at all times, upon request, to be advised as to the status of work being done by the Contractor and of the details thereof.

11.2 Performance Deficiencies and Financial Consequences of Non-Performance.

11.2.1 Proposal of Corrective Action Plan.

See section 10 (Defaults and Remedies) of Attachment A to the Master Agreement.

11.2.2 Retainage for Unacceptable Corrective Action Plan or Plan Failure.

See section 10 (Defaults and Remedies) of Attachment A to the Master Agreement.11.3
Performance Delay.

11.3 Performance Delay.

11.3.1 Notification.

See section 31 (Warranties, Disclaimers, and Exclusive Remedies) of Attachment A to the Master Agreement.

11.3.2 Liquidated Damages.

See sections 10 (Defaults and Remedies) and 31 (Warranties, Disclaimers, and Exclusive Remedies) of Attachment A to the Master Agreement.

11.4 Force Majeure, Notice of Delay, and No Damages for Delay.

The Contractor will not be entitled to an increase in the Contract price or payment of any kind from the Department for direct, indirect, consequential, impact or other costs, expenses or damages, including but not limited to costs of acceleration or inefficiency, arising because of any failure or delay in performance of the Contract that is beyond the reasonable control and without the fault or negligence of the Department.

See section 12 (Force Majeure) of Attachment A to the Master Agreement.

SECTION 12. CONTRACT AUDITS.

12.1 Performance or Compliance Audits.

The Department may conduct or have conducted performance and/or compliance audits of the Contractor and subcontractors as determined by the Department. The Department may conduct an audit of Contractor's compliance with its obligations under this Master Agreement and any applicable purchase orders. The Department shall limit the number of audits of Contractor per fiscal year to a reasonable amount.

12.2 Payment Audit.

See section 26 (Records Administration and Audit) of Attachment A to the Master Agreement.

12.3 Document Inspection.

In accordance with section 216.1366, F.S., the Department is authorized to inspect the: (a) financial records, papers, and documents of the Contractor that are directly related to the

Exhibit A, Contract Conditions

Oracle America, Inc. Contract No. 43230000-NASPO-16-ACS

Page 12 of 17

performance of the Contract or the expenditure of state funds; and (b) programmatic records, papers, and documents of the Contractor which the Department determines are necessary to monitor the performance of the Contract or to ensure that the terms of the Contract are being met. The Contractor shall provide such records, papers, and documents requested by the Department within 10 Business Days after the request is made. Notwithstanding the foregoing, Oracle shall not be compelled to produce any confidential or proprietary information unrelated to the Contract.

SECTION 13. BACKGROUND SCREENING AND SECURITY.

13.1 Background Check.

Oracle, or its agent, performs a background check at the Contractor's expense on employees hired on or after January 1, 2003 in the United States. As of the effective date of this Participating Addendum, the background check is used to attempt to: (i) ascertain an employee's previous employment with up to three (3) employers within the five (5) years preceding the date of the check; (ii) ascertain an employee's highest degree earned; (iii) assess any public criminal records uncovered for an employee within the seven (7) years preceding the date of the check; and (iv) check for matches on the Office of Foreign Asset Control's Specially Designated Nationals and Foreign Sanctions Evaders Lists. The background check is adjudicated by Oracle. While all criminal records are individually assessed in accordance with applicable laws and agency guidance, generally, significant crimes involving violence, dishonesty, and certain drug-related offenses are considered disqualifiers, except where a diversion program was successfully completed and/or the case was discharged or judicially dismissed. In general, international transfers and individuals with valid United States government issued security clearance are not subject to a background check. Processing and procedural variances may apply to students/interns, university recruiting hires, and to employees of companies acquired by Oracle. Any additional background screening or re-screening terms or requirements will be mutually agreed upon with the Contractor and Customer in the Ordering Document.

13.2 E-Verify.

The Contractor shall register with and use the U.S. Department of Homeland Security's (DHS) E-Verify system to verify the work authorization status of all new employees of the contractor in accordance with section 448.095, F.S. If subcontractors are used, the Contractor shall flow down the following term to the subcontractor in any subcontracting agreement and maintain a copy of the subcontractor's affidavit for the duration of the contract:

"Subcontractor shall register with and use the U.S. Department of Homeland Security's (DHS) E-Verify system to verify the work authorization status of all new employees of subcontractor in accordance with section 448.095, F.S. Subcontractor shall provide to Contractor an affidavit in accordance with paragraph (5)(b) of section 448.0985."

13.3 Confidentiality.

See section 8 (Confidentiality, Non-Disclosure, and Injunctive Relief) of Attachment A to the Master Agreement. The provisions of section 8 of Attachment A to the Master Agreement shall, for purposes of this Participating Addendum and any subsequently issued Purchase Orders, also apply to customer data which is otherwise confidential under Florida or federal law.

SECTION 14. WARRANTY OF CONTRACTOR'S ABILITY TO PERFORM.

The Contractor warrants that, to the best of its knowledge, there is no pending or threatened action, proceeding, or investigation, or any other legal or financial condition, that would in any way prohibit, restrain, or diminish the Contractor's ability to satisfy its Contract obligations. The Contractor warrants that neither it nor any affiliate is currently on the Suspended Vendor List, Convicted Vendor List, or the Discriminatory Vendor List, or on any similar list maintained by any other state or the federal government. The Contractor shall immediately notify the Department in writing if its ability to perform is compromised in any manner during the term of the Contract.

SECTION 15. CONTRACT REPORTING.

The Contractor shall provide the following reports associated with this Contract:

15.1 Contract Quarterly Sales Reports.

The Contractor shall submit Quarterly Sales Reports in the manner and format required by the Department within 30 calendar days after the close of each State fiscal quarter (the State's fiscal quarters close on September 30, December 31, March 31, and June 30).

The Quarterly Sales Report template can be found here: [Quarterly Sales Report Format / Vendor Resources / State Purchasing / Business Operations / Florida Department of Management Services - DMS \(myflorida.com\)](#). Initiation and submission of the Quarterly Sales Report posted on the DMS website is the responsibility of the Contractor without prompting or notification from the Department. If no sales are recorded in two consecutive quarters, the Contractor may be placed on probationary status, or the Department may terminate the Contract. Failure to provide the Quarterly Sales Report, or other reports requested by the Department, will result in the imposition of financial consequences and may result in the Contractor being found in default and the termination of the Contract.

15.2 Certified and Minority Business Enterprises Reports.

Oracle will, after the Department or Customer's written request sent to supplierdiversity_us@oracle.com, email the Department or Customer at the email address provided, the following information about the US dollar amount of indirect procurement spend paid by Oracle to diverse suppliers who supply to Oracle in the United States. Oracle will share the aggregate quarterly spend paid by Oracle to such diverse suppliers in the most recent quarter for which such information is available. Indirect procurement spend is the expenditure on goods and services for day-to-day internal business operations (e.g., office supplies, printers, computer, maintenance, etc.). Diverse suppliers are suppliers who identify themselves to Oracle as woman-owned, minority-owned, veteran-owned, disabled veteran-owned and/or HubZoned business enterprises.

15.3 Ad Hoc Sales Reports.

The Department may request additional Contract sales information that is directly related to the Contract, such as copies of purchase orders or ad hoc sales reports. The Contractor shall submit these documents and reports within the timeframe specified by the Department.

15.4 MFMP Transaction Fee Reports.

The Contractor shall submit complete monthly MFMP Transaction Fee Reports to the Department. Reports are due 15 calendar days after the end of each month. Information on how to submit MFMP Transaction Fee Reports online can be located at https://www.dms.myflorida.com/business_operations/state_purchasing/myfloridamarketplace/mfmp_vendors/transaction_fee_and_reporting. Assistance with transaction fee reporting is also available from the MFMP Customer Service Desk by email at feeprocessing@myfloridamarketplace.com or telephone at 866-FLA-EPRO (866-352-3776) from 8:00 a.m. to 6:00 p.m. Eastern Time.

SECTION 16. FINANCIAL CONSEQUENCES.

Financial Consequences: The Department reserves the right to impose financial consequences when the Contractor fails to comply with the requirements of the Contract. The following financial consequences will apply for the Contractor's non-performance under the Contract. The Customer and the Contractor may agree to add additional Financial Consequences on an as-needed basis beyond those stated herein to apply to that Customer's resultant contract or purchase order. The State of Florida reserves the right to withhold payment or implement other appropriate remedies, such as Contract termination or nonrenewal, when the Contractor has failed to comply with these provisions of the Contract. The Contractor and the Department agree that the financial consequences for non-performance are an estimate of damages which are difficult to ascertain and are not penalties.

The financial consequences will be paid via check or money order and made out to the Department of Management Services in U.S. dollars within 30 calendar days after the required report submission date. These consequences are individually assessed for failures over each target period beginning with the first full month or quarter of the contract performance and every month or quarter, respectively, thereafter.

Financial Consequences Chart

Deliverable	Performance Metric	Performance Due Date	Financial Consequence for Non-Performance
Contractor will timely submit complete Quarterly Sales Reports	All Quarterly Sales Reports will be submitted timely with the required information	Reports are due on or before the 30 th calendar day after the close of each State fiscal quarter	\$250 Per Calendar Day Late/Not Received by the Contract Manager
Contractor will timely complete MFMP Transaction Fee Reports	All MFMP Transaction Fee Reports will be submitted timely with the required information	Reports are due on or before the 15 th calendar day after the close of each month	\$100 Per Calendar Day Late/Not Received by the Contract Manager

No favorable action will be considered when Contractor has outstanding Contract Quarterly Sales Reports, MFMP Transaction Fee Reports, or any other documentation owed to the Department or Customer, to include fees / monies, that is required under this Contract.

SECTION 17. ADDITIONAL TERMS.

- A. Orders: Contractor must be able to accept MyFloridaMarketPlace (MFMP) purchase orders and the State of Florida Purchasing Card for single transactions up to five thousand dollars (\$5,000).
- B. Contractor and applicable Subcontractors, Affiliates, Partners, Resellers, Distributors, and Dealers: By execution of a Contract, the Contractor acknowledges that it will not be released of its contractual obligations to the Department because of any failure of a subcontractor, reseller, distributor, or dealer. The Contract terms are applicable to subcontractors, resellers, distributors, and dealers and shall apply to the Contractor's applicable Subcontractors, Affiliates, Partners, Resellers, Distributors, and Dealers providing commodities and performing services in furtherance of the Contract. The Contractor is fully responsible for satisfactory completion of all work performed under the Contract.
- C. Purchases Prerequisites: Before fulfilling any Customer purchases and receiving payment, the Contractor and applicable Subcontractors, Affiliates, Partners, Resellers, Distributors, and Dealers must have met the following requirements, unless further notated below:
- Have an active registration with the Florida Department of State, Division of Corporations (www.sunbiz.org), or, if exempt from the registration requirements, provide the Department with the basis for such exemption.
 - Be registered in the MFMP Vendor Information Portal (<https://vendor.myfloridamarketplace.com>) *only required by applicable Subcontractors, Affiliates, Partners, Resellers, Distributors, and Dealers if receiving payment.
 - Not be on the State's Convicted, Suspended, or Discriminatory Vendor lists (http://www.dms.myflorida.com/business_operations/State_purchasing/vendor_information/convicted_suspended_discriminatory_complaints_vendor_lists)
 - Have a copy of e-Verify Status on file.
 - Have a current W-9 filed with the Florida Department of Financial Services (<https://flvendor.myfloridacfo.com>) *only required by applicable Subcontractors, Affiliates, Partners, Resellers, Distributors, and Dealers if receiving payment.
- D. MFMP Electronic Invoicing: The Contractor may supply electronic invoices in lieu of paper-based invoices for those transactions processed through MFMP. Electronic invoices may be submitted to the agency through one of the mechanisms as listed below:
- 1) EDI (Electronic Data Interchange)
This standard establishes the data contents of the Invoice Transaction Set (810) for use within the context of an Electronic Data Interchange (EDI) environment. This transaction set can be used for invoicing via the Ariba Network (AN) for catalog and non-catalog goods and services.
 - 2) PO Flip via AN
This online process allows Contractors to submit invoices via the AN for catalog and non-catalog goods and services. Contractors have the ability to create an invoice directly from

their inbox in their AN account by simply "flipping" the PO into an invoice. This option does not require any special software or technical capabilities.

The Contractor warrants and represents that it is authorized and empowered to and hereby grants the State and the third-party provider of MFMP, a State contractor, the right and license to use, reproduce, transmit, distribute, and publicly display within MFMP. In addition, the Contractor warrants and represents that it is authorized and empowered to and, hereby grants the State and the third-party provider the right to reproduce and display within MFMP the Contractor's trademarks, logos, trade names, or other branding designations.

The Contractor will work with the MFMP management team to obtain specific requirements for the electronic invoicing if needed.

- E. Business Review Meetings: Both the Department and Customer reserve the right to schedule business review meetings. The Department or Customer will provide the format for the Contractor's agenda. In the event the Department or Customer schedules a business review meeting, the Contractor shall submit the completed agenda to the Department or Customer for review and acceptance prior to the meeting. The Contractor shall address the agenda items and any of the Department's or Customer's additional concerns at the meeting. At a minimum, the agenda items may include:
- a. Contract compliance
 - b. Savings report (in dollar amount and cost avoidance)
 - c. Spend reports by Customer
 - d. Recommendations for improved compliance and performance



Exhibit B - Master Agreement Cloud Solutions

Contract No. **43230000-NASPO-16-ACS** Contract # **AR2487**

STATE OF UTAH COOPERATIVE CONTRACT

1. **CONTRACTING PARTIES:** This contract is between the Division of Purchasing and the following Contractor:

Oracle America, Inc.

Name

1910 Oracle Way

Address

Reston

VA

20190

City

State

Zip

LEGAL STATUS OF CONTRACTOR

- ☐ Sole Proprietor
☐ Non-Profit Corporation
☒ For-Profit Corporation
☐ Partnership
☐ Government Agency

Contact Person Elizabeth Hwang Phone #703-364-0282 Email elizabeth.hwang@oracle.com

Vendor #VC0000147700 Commodity Code #920-05

2. **GENERAL PURPOSE OF CONTRACT:** Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed
3. **PROCUREMENT PROCESS:** This contract is entered into as a result of the procurement process on Bid#CH16012.
4. **CONTRACT PERIOD:** Effective Date: 3/1/2017 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.
5. **Administrative Fee,** as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services invoiced during the calendar quarter.
6. **ATTACHMENT A:** NASPO ValuePoint Master Terms and Conditions, including the Exhibits and Addenda referenced therein and attached thereto.
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012, which is attached solely for reference purposes only.
ATTACHMENT E: Contractor's Sample Ordering Document, which is attached solely for reference purposes only.

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

7. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR
Elizabeth Hwang
 Elizabeth Hwang (Mar 1, 2017)

Mar 1, 2017

Contractor's signature

Date

Elizabeth Hwang, Manager, Public Sector Deal Management

Type or Print Name and Title

STATE

Christopher Hughes
 Director, Division of Purchasing

3.1.2017
 Date

Christopher Hughes

Division of Purchasing Contact Person

801-538-3254

Telephone Number

Fax Number

christopherhughes@utah.gov

Email

(Revision 16 June 2016)



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

- (i) Oracle Ordering Document, which shall incorporate the applicable Hosting and Delivery Policies. A copy of the Oracle's Hosting and Delivery Policies, current as of the effective date of this Master Agreement, is attached hereto as Addendum 1 for reference purposes only and is subject to change at Oracle's discretion. The version of these policies, current as of the Cloud Services start date set forth in each applicable Order, is available at www.oracle.com/contracts.
- (ii) A Participating Entity's Participating Addendum¹ ("PA").
- (iii) NASPO ValuePoint Master Agreement Terms & Conditions, including the following Exhibits:
 - (1) Exhibit 1: Software-as-a-Service;
 - (2) Exhibit 2: Platform-as-a-Service; and
 - (3) Exhibit 3: Infrastructure-as-a-Service.

The Lead State agrees that this Master Agreement and the information which is incorporated into this Master Agreement by written reference (including reference to information contained in a URL or referenced policy), together with the applicable Order and Participating Addendum, is the complete agreement for the Services ordered by the Purchasing Entity and supersedes all prior or contemporaneous agreements or representations, written or oral, regarding such Services.

It is expressly agreed that the documents in the order of precedence above (unless otherwise provided below) shall supersede the terms in any purchase order, procurement internet portal, or other similar non-Oracle document and no terms included in any such purchase order, portal, or other non-Oracle document shall apply to the Services ordered. In the event of any inconsistencies between the terms of an Order and the Master Agreement, the Order shall take precedence; however, unless expressly stated otherwise in an Order, the terms of the Data Processing Agreement (a copy of which, current as of the effective date of this Master Agreement, is attached hereto as Addendum 2 for reference purposes only and is subject to change at

¹ A Sample Participating Addendum will be published after the contracts have been awarded.

Oracle's discretion) shall take precedence over any inconsistent terms in an Order. The version of the Data Processing Agreement that is current as of the Cloud Services start date set forth in each applicable Ordering Document is available at www.oracle.com/contracts. No third party beneficiary relationships are created by this Master Agreement.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Ancillary Software means any software agent or tool that Oracle makes available to the Purchasing Entity for download for purposes of facilitating the Purchasing Entity's access to, operation of, and/or use with, the Services Environment.

Cloud Services means, collectively, the Oracle cloud services (e.g., Oracle software as a service offerings and related Oracle Programs) listed in Purchasing Entity's Order and defined in the Service Specifications. The term "Cloud Services" does not include Professional Services.

Confidential Information has the meaning ascribed to it in Section 8 (Confidentiality, Non-Disclosure, and Injunctive Relief) below.

Contractor means Oracle America, Inc.

Data Center Region refers to the geographic region in which the Services Environment is physically located. The Data Center Region applicable to the Cloud Services is set forth in Purchasing Entity's Order.

Fulfillment Partner The Participating Addendum may set forth the extent to which a third party may resell the Services under the terms of this Master Agreement.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

Incident means an incident that creates suspicion of unauthorized access to or handling of Personal Data.

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State of Utah.

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

Master Agreement means this agreement executed by and between the Lead State,

acting on behalf of NASPO ValuePoint, and the Contractor, together with Exhibit 1 (Software-as-a-Service), Exhibit 2 (Platform-as-a-Service), and Exhibit 3 (Infrastructure-as-a-Service), each of which is attached hereto and incorporated herein, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Oracle means Oracle America, Inc., the Contractor.

Oracle Programs refers to the software products owned or licensed by Oracle to which Oracle grants Purchasing Entity access as part of the Cloud Services, including Program Documentation, and any program updates provided as part of the Cloud Services.

Order or **Ordering Document** means Contractor's or Contractor's authorized reseller's standard ordering document signed by Purchasing Entity when placing an order for Services pursuant to this Master Agreement.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means any information relating to an identified or identifiable natural

person that customer or its end users provide to Oracle as part of the Cloud Services; an identified or identifiable natural person (a “data subject”) is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

Professional Services means, collectively, the Cloud Services-related consulting and other professional services which Purchasing Entity has ordered. Professional Services include any deliverables described in Purchasing Entity’s Order and delivered by Oracle to Purchasing Entity under the Order. The term “Professional Services” does not include Cloud Services.

Program Documentation refers to the user manuals referenced within the Service Specifications for Cloud Services, as well as any help windows and readme files for the Oracle Programs that are accessible from within the Services. The Program Documentation describes technical and functional aspects of the Oracle Programs. Purchasing Entity may access the documentation online at <http://oracle.com/contracts> or such other address specified by Oracle.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Security Breach for the specific purpose of handling an Incident in the Data Processing Agreement means the misappropriation of Personal Data located on Oracle systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such information. Oracle will inform Customer within 72 hours if Oracle determines that Personal Data has been subject to a Security Breach (including by an Oracle employee) or any other circumstance in which Customer is required to provide a notification under applicable law, unless otherwise required by law.

Services means, collectively, the Cloud Services and Professional Services ordered by the Purchasing Entity.

Services Environment refers to the combination of hardware and software components owned, licensed or managed by Oracle to which Oracle grants Purchasing Entity and Purchasing Entity’s Users access as part of the Cloud Services which Purchasing Entity has ordered. As applicable and subject to the terms of this Master Agreement and Purchasing Entity’s Order, Oracle Programs, Third Party Content, Your Content and Your Applications may be hosted in the Services Environment.

Service Specifications means the descriptions on www.oracle.com/contracts, or such other address specified by Oracle, that are applicable to the Services under Purchasing Entity’s Order, including any Program Documentation, hosting, support and security policies (for example, Oracle Cloud Hosting and Delivery Policies), and other

descriptions referenced or incorporated in such descriptions or Purchasing Entity's Order.

Services Period refers to the period of time for which Purchasing Entity has ordered Cloud Services as specified in Purchasing Entity's Order.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

Third Party Content means all text, files, images, graphics, illustrations, information, data, audio, video, photographs and other content and material, in any format, that are obtained or derived from third party sources outside of Oracle and made available to Purchasing Entity through, within, or in conjunction with Purchasing Entity's use of, the Cloud Services. Examples of Third Party Content include data feeds from social network services, rss feeds from blog posts, and data libraries and dictionaries and marketing data.

Users means those employees, contractors, and end users, as applicable, authorized by the Purchasing Entity or on the Purchasing Entity's behalf to use the Cloud Services in accordance with this Master Agreement and Purchasing Entity's Order. For Cloud Services that are specifically designed to allow the Purchasing Entity's clients, agents, customers, suppliers or other third parties to access the Cloud Services to interact with the Purchasing Entity, such third parties will be considered "Users" subject to the terms of this Master Agreement and Purchasing Entity's Order.

Your Applications means all software programs, including any source code for such programs, that the Purchasing Entity or the Purchasing Entity's Users provide and load onto, or create using, any Oracle "platform-as-a-service" or "infrastructure-as-a-service" Cloud Services. Services under this Master Agreement, including Oracle Programs and Services Environments, Oracle intellectual property, and all derivative works thereof, do not fall within the meaning of the term "Your Applications."

Your Content means all text, files, images, graphics, illustrations, information, data (including Personal Data as that term is defined in the Data Processing Agreement for Oracle Cloud Services described in Section 8.b of the Master Agreement), audio, video, photographs and other content and material (other than Your Applications), in any format, provided by the Purchasing Entity or on behalf of Purchasing Entity's Users that reside in, or run on or through, the Services Environment.

3. Term of the Master Agreement: The initial term of this Master Agreement is for ten (10) years with no renewal options.

4. Amendments: Except as otherwise permitted in Section 44.b (Service Specifications) and Section 44.g (Third Party Web Sites) of this Master Agreement and Section 2 (Data Protection) and Section 3 (Data Location) of Exhibits 1, 2, and 3 to the Master Agreement, this Master Agreement and Orders placed hereunder may not be modified and the rights and restrictions may not be altered or waived except in a writing signed by authorized representatives of the Lead State and of Oracle. The terms of this Master Agreement shall not be waived, altered, modified, supplemented or amended in any manner whatsoever without prior written approval of the Lead State and Contractor.

5. Assignment/Subcontracts: Except in the event of a merger, consolidation, acquisition, internal restructuring, or sale of all or substantially all of the assets of Oracle, Contractor shall not assign, this Master Agreement, in whole or in part, without the prior written approval of the WSCA-NASPO Master Agreement Administrator. The Lead State may not assign the Master Agreement and no Participating State or Participating Entity may assign its Participating Addendum, in whole or in part, without the prior written approval of Contractor. No Purchasing Entity may give or transfer the Services ordered under an Ordering Document to another individual or entity.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under only net new Orders under this Master Agreement in the event that Oracle's commercial list price for the Services decreases. A price or rate reduction reflected in Oracle's commercial list price will apply automatically to the Master Agreement for purposes of net new Orders only, and an amendment is not necessary.

7. Termination: Unless otherwise stated, this Master Agreement may be terminated by either party upon 60 days written notice prior to the effective date of the termination. Further, any Participating Entity may terminate its Participating Addendum upon 30 days written notice, unless otherwise limited or stated in the Participating Addendum.

Any termination under this provision shall not affect the rights and obligations that survive termination or expiration of this Master Agreement, such as those relating to limitation of liability, indemnification, payment and others which by their nature are intended to survive.

Termination of the Master Agreement or any Participating Addendum will not affect Orders that are outstanding at the time of termination. Those Orders will be performed according to their terms as if this Master Agreement or the Participating Addendum were still in full force and effect. However, those Orders may not be renewed subsequent to termination of this Master Agreement.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. By virtue of this Master Agreement, the parties may have access to information that is confidential to one another ("**Confidential Information**"). We each agree to disclose only information that is required for the performance of obligations under this Master Agreement. Confidential information shall be limited to the terms and pricing under this Master Agreement, Your Content and Your Applications residing in the Services Environment, and all information clearly identified as confidential at the time of disclosure.

b. A party's Confidential Information shall not include information that: (i) is or becomes a part of the public domain through no act or omission of the other party; (ii) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (iii) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (iv) is independently developed by the other party.

c. We each agree not to disclose each other's Confidential Information to any third party other than as set forth in the following sentence for a period of three years from the date of the disclosing party's disclosure of the Confidential Information to the receiving party; however, Oracle will hold the Purchasing Entity's Confidential Information that resides within the Services Environment in confidence for as long as such information resides in the Services Environment. We each may disclose Confidential Information only to those employees, agents or subcontractors who are required to protect it against unauthorized disclosure in a manner no less protective than required under this Master Agreement. Oracle will protect the confidentiality of Your Content or Your Applications residing in the Services Environment in accordance with the Oracle security practices defined as part of the Service Specifications applicable to the Purchasing Entity's Order. In addition, the Purchasing Entity's Personal Data will be treated in accordance with the terms of Section 2 (Data Protection) of Exhibits 1, 2, and 3 to the Master Agreement. Nothing shall prevent either party from disclosing the terms or pricing under this Master Agreement or Orders placed under this Master Agreement in any legal proceeding arising from or in connection with this Master Agreement or from disclosing the Confidential Information to a governmental entity as required by law.

d. Injunctive Relief. Each party acknowledges that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information and that the disclosing party shall be entitled, without waiving any other rights or remedies under this Master Agreement, to seek such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

e. Purchasing Entity Law. The parties acknowledge and agree that the Purchasing Entities and this Master Agreement are subject to applicable freedom of information or open records law. Except as may otherwise be agreed to in the applicable Participating Addendum, if the Lead State, any Participating Entity, or any Purchasing Entity receives a request to disclose Oracle Confidential Information under the applicable freedom of information or open records law, each such entity agrees to promptly notify Oracle in

writing and give Oracle an opportunity to request confidentiality protection for any Confidential Information to which such entity may deny access under law.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement, including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or any Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

Oracle may orally refer to this Master Agreement, and the potential work and activities covered by this Master Agreement, and may orally reference the Lead State or a Participating Entity as a customer in sales presentations and activities.

10. Defaults and Remedies:

If any party to (i) this Master Agreement, (ii) a Participating Addendum, or (iii) an Ordering Document breaches a material term of this Master Agreement and fails to correct the breach within 30 days of written specification of the breach, then the breaching party is in default and the non-breaching party may terminate the Order under which the breach occurred. If Oracle terminates the Order as specified in the preceding sentence, the Purchasing Entity must pay within 30 days all amounts that have accrued prior to such termination, as well as all sums remaining unpaid for the Services under such Order plus related taxes and expenses. Except for nonpayment of fees, the nonbreaching party may agree in its sole discretion to extend the 30 day period for so long as the breaching party continues reasonable efforts to cure the breach. If a Purchasing Entity is in default under this Master Agreement, the applicable Participating Addendum, or the applicable Ordering Document, the Purchasing Entity may not use those Services ordered.

In the event of any dispute or disagreement between the parties arising out of or relating to (i) this Master Agreement, (ii) a Participating Addendum, or (iii) an Ordering Document (the "dispute"), the parties will endeavor to resolve the dispute in accordance with this section. Either party may invoke this section by providing the other party written notice of its decision to do so, including a description of the issues subject to the dispute. Each party will appoint a Managing Director (or the equivalent) to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief, may begin until the Managing Directors (or the equivalent) conclude, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. The parties shall refrain from exercising any termination right and shall continue to perform their respective obligations under this

Master Agreement and the applicable Participating Addendum and Ordering Document, if any, while the parties endeavor to resolve the dispute under this section, provided that, any party alleged to be in breach promptly makes good faith efforts to cure the breach and pursues the cure in good faith. The period of dispute resolution after notice will not exceed thirty (30) days, unless both parties agree to an extension.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes to the Contractor's Contract Manager, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes to the Contractor's Contract Manager.

12. Force Majeure: Neither party to (i) this Master Agreement, (ii) a Participating Addendum, or (iii) an Ordering Document shall be in default by reason of any failure or delay in performance of this Contract in accordance with reasonable control and without fault or negligence on their part. Such causes may include, but are not restricted to, acts of nature or the public enemy, restrictive acts of the government (including the denial or cancelation of any export, import, or other license) in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather, but in every case the failure to perform such must be beyond the reasonable control and without the fault or negligence of the party. The parties will both use reasonable efforts to mitigate the effect of a force majeure event. If such event continues for more than 30 days, either party may cancel unperformed Services and affected Orders upon written notice. This Section does not excuse either party's obligation to take reasonable steps to follow its normal disaster recovery procedures or Purchasing Entity's obligation to pay for the Services.

13. Indemnification

a. Subject to the terms of this Section 13 (Indemnification), if a third party makes a claim against the Purchasing Entity ("Recipient"), that any information, design, specification, instruction, software, service, data, hardware, or material (collectively, "Material") furnished by Oracle ("Provider") and used by the Recipient infringes the third party's intellectual property rights, the Provider, at the Provider's sole cost and expense, will, to the extent not prohibited by law, defend the Recipient against the claim and indemnify the Recipient from the damages, liabilities, costs and expenses awarded by the court to the third party claiming infringement or the settlement agreed to by the Provider, if the Recipient does the following:

- (i) notifies the Provider promptly in writing, not later than 30 days after the Recipient receives notice of the claim (or sooner if required by applicable law);
- (ii) gives the Provider sole control of the defense and any settlement negotiations, to the extent permitted by law; and
- (iii) gives the Provider the information, authority and assistance the Provider needs to defend against or settle the claim.

b. If the Provider believes or it is determined that any of the Material may have violated a third party's intellectual property rights, the Provider may choose to either modify the Material to be non-infringing (while substantially preserving its utility or functionality) or obtain a license to allow for continued use, or if these alternatives are not commercially

reasonable, the Provider may end the license for, and require return of, the applicable Material and refund any unused, prepaid fees the Recipient may have paid to the other party for such Material. If such return materially affects Oracle's ability to meet its obligations under the relevant Order, then Oracle may, at its option and upon 30 days prior written notice, terminate the Order. If such Material is third party technology and the terms of the third party license do not allow Oracle to terminate the license, then Oracle may, upon 30 days prior written notice, end the Services associated with such Material and refund to Purchasing Entity any unused, prepaid fees for such Services.

c. The Provider will not indemnify the Recipient if the Recipient (i) alters the Material or uses it outside the scope of use identified in the Provider's user or program documentation or Service Specifications, (i) uses a version of the Material which has been superseded, if the infringement claim could have been avoided by using an unaltered current version of the Material which was made available to the Recipient, or (iii) continues to use the applicable Material after the end of the license to use that Material. The Provider will not indemnify the Recipient to the extent that an infringement claim is based upon any information, design, specification, instruction, software, service, data, hardware or material not furnished by the Provider. Oracle will not indemnify Purchasing Entity for any portion of an infringement claim that is based upon the combination of any Material with any products or Services not provided by Oracle. Oracle will not indemnify the Purchasing Entity to the extent that an infringement claim is based on Third Party Content or any Material from a third party portal or other external source that is accessible or made available to Purchasing Entity within or by the Services (e.g., a social media post from a third party blog or forum, a third party Web page accessed via a hyperlink, marketing data from third party data providers, etc. Oracle will not indemnify the Purchasing Entity for infringement caused by the Purchasing Entity's actions against any third party if the Services as delivered to the Purchasing Entity and used in accordance with the terms of this Master Agreement would not otherwise infringe any third party intellectual property rights. Oracle will not indemnify the Purchasing Entity for any intellectual property infringement claim(s) known to the Purchasing Entity at the time Services rights are obtained.

d. This Section 13(a)-(d) provides the Purchasing Entity's exclusive remedy for any infringement claims or damages.

e. Oracle (“**Indemnitor**”) shall defend and indemnify the Purchasing Entity (“**Indemnitee**”) against any and all claims of bodily injury (including wrongful death) and/or tangible personal property damage resulting from negligent or intentionally wrongful actions or omissions of the Indemnitor or a person employed by the Indemnitor (i.e., as an employee or independent contractor) while performing or participating in services under an Ordering Document at your site, if such actions or omissions were not proximately caused by the action or omission of the Indemnitee or any third party; provided however, that (i) the Indemnitee notifies the Indemnitor within thirty (30) days of the Indemnitee’s receipt of a claim; (ii) the Indemnitor has sole control of the defense and all related settlement negotiations; and (iii) the Indemnitee gives the Indemnitor the information, authority and reasonable assistance necessary to perform the above ; reasonable out-of-pocket expenses incurred by the Indemnitee in providing such assistance will be reimbursed by the Indemnitor. As used in this Section, the term “tangible personal property” shall not include software, documentation, data or data files. The Indemnitor shall have no liability for any claim of bodily injury and/or tangible personal property damage arising from use of software or hardware. **This Section 13(e) states Oracle’s entire liability and the Purchasing Entity’s exclusive remedy for bodily injury and property damage.**

14. Independent Contractor: The Contractor shall be an independent contractor. Contractor shall have no authorization, express or implied, to bind the Lead State, Participating States, other Participating Entities, or Purchasing Entities to any agreements, settlements, liability or understanding whatsoever, and agrees not to hold itself out as agent except as expressly set forth herein or as expressly agreed in any Participating Addendum. The parties agree that no partnership or joint venture relationship exists between us. We are each responsible for paying our own employees, including employment related taxes and insurance. The Lead State and each Purchasing Entity understand that Oracle’s business partners and other third parties, including any third parties with which Oracle has an integration or that are retained by a Purchasing Entity to provide consulting or implementation services or applications that interact with the Cloud Services, are independent of Oracle and are not Oracle’s agents. Oracle is not liable for, bound by, or responsible for any problems with the Services, Your Content or Your Applications arising due to any acts of any such business partner or third party, unless the business partner or third party is providing Services as an Oracle subcontractor on an engagement ordered under this Master Agreement and, if so, then only to the same extent as Oracle would be responsible for Oracle resources under this Master Agreement.

15. Individual Customers: Except to the extent modified by a Participating Addendum, each Purchasing Entity shall follow the terms and conditions of the Master Agreement and applicable Participating Addendum and will have the same rights and responsibilities for its purchases as the Lead State has in the Master Agreement, including but not limited to, any indemnity or right to recover any costs as such right is defined in the Master Agreement and applicable Participating Addendum for its purchases. Each Purchasing Entity will be responsible for its own charges, fees, and liabilities. The Contractor will apply the charges and invoice each Purchasing Entity individually.

16. Insurance

Oracle shall take out and maintain the following minimum insurance at its expense for the duration of this Master Agreement covering locations where Oracle is to perform work on Purchasing Entity's premises:

- a. Workmen's Compensation – As required by the statute of states where Services are being performed;
- b. Employer's Liability – \$2,000,000 each occurrence;
- c. Comprehensive General Liability Insurance – \$5,000,000 per occurrence/aggregate bodily injury and \$5,000,000 per occurrence/aggregate property damage; and
- d. Automobile Liability Insurance – \$5,000,000 – per occurrence, bodily injury and tangible property damage combined.

In addition, the minimum insurance coverage required for data breach and privacy/cyber liability shall be as indicated in the following table:

Level of Risk	Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions Minimum Insurance Coverage
Low Risk Data	\$2,000,000
Moderate Risk Data	\$5,000,000
High Risk Data	\$10,000,000

Nothing in this Master Agreement shall be deemed to preclude Oracle from selecting a new insurance carrier or carriers or obtaining new or amended policies at any time, as long as the above insurance coverage is maintained. This provision is not intended to, and does not, increase or decrease Oracle's liability under the Limitation of Liability provision of this Master Agreement.

17. Laws and Regulations – Compliance with Laws: Oracle shall comply with all laws to the extent that such laws, by their terms, are expressly applicable to Oracle's provision of Services under the Master Agreement and impose obligations directly upon Oracle in its role as an information technology services provider with respect to the Services. The Purchasing Entity may not provide Oracle access to any health, payment card or other sensitive personal information that requires the application of specific regulatory, legal or industry data security obligations unless the applicable obligations are specified in the applicable Ordering Document. Your Content and Your Applications, including personal information, may be maintained in one of several Oracle data centers globally and/or accessed by Oracle's global personnel as required to provide the Services.

18. Reserved.

19. Ordering

a. Reserved.

b. This Master Agreement permits Purchasing Entities to define project-specific requirements and informally compete the requirement among other firms having a Master Agreement on an “as needed” basis. This procedure may also be used when requirements are aggregated or other firm commitments may be made to achieve reductions in pricing. This procedure may be modified in Participating Addenda and adapted to Purchasing Entity rules and policies. The Purchasing Entity may in its sole discretion determine which firms should be solicited for a quote. The Purchasing Entity may select the quote that it considers most advantageous, cost and other factors considered.

c. Each Purchasing Entity will identify and utilize its own appropriate purchasing procedure and documentation. If the Purchasing Entity provides the necessary information to Contractor, Contractor is expected to become familiar with the Purchasing Entities’ rules, policies, and procedures regarding the ordering of supplies and/or services contemplated by this Master Agreement.

d. Contractor shall not begin providing Services without a valid Ordering Document.

e. Orders may be placed consistent with the terms of this Master Agreement during the term of the Master Agreement.

f. All Orders pursuant to this Master Agreement, at a minimum, shall include:

- (i) The services or supplies being delivered;
- (ii) The name, phone number, and address of the Purchasing Entity representative; and
- (iii) The Master Agreement identifier and the Participating State contract identifier.

g. Communications concerning administration of Orders placed under this Master Agreement shall be furnished to the authorized purchasing agent within the Purchasing Entity’s purchasing office, or to such other individual identified in writing in the Order.

h. Orders must be placed pursuant to this Master Agreement prior to the termination date of this Master Agreement.

i. Notwithstanding the expiration or termination of this Master Agreement, Contractor agrees to perform Orders then outstanding at the time of such expiration or termination. Contractor shall not honor any Orders attempted after the expiration or termination of this Master Agreement. Orders from any separate indefinite quantity, task orders, or other form of indefinite delivery order arrangement priced against this Master Agreement may not be placed after the expiration or termination of this Master Agreement, notwithstanding the term of any such indefinite delivery order agreement.

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating

Addendum acceptable to the Participating Entity and Contractor is executed. The Master Agreement terms and conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the Ordering Document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Reserved.

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Participating States are financially obligated for the orders placed by the departments or other state agencies and institutions of the Participating State. Participating States incur no financial obligations on behalf of political subdivisions to the extent not otherwise specified in an Ordering Document.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor. This shall not prohibit the Lead State from negotiating different terms and conditions in its Participating Addendum.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have

the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement.

21. FEES AND TAXES

a. All fees payable to Oracle are due within thirty (30) days from the invoice date. Once placed, Purchasing Entity's Order is non-cancelable and the sums paid nonrefundable, except as provided in this Master Agreement or Purchasing Entity's Order. Purchasing Entity will pay any sales, value-added or other similar taxes imposed by applicable law that Oracle must pay based on the Services Purchasing Entity ordered, except for taxes based on Oracle's income. Also, Purchasing Entity will reimburse Oracle for reasonable expenses related to providing any Professional Services. Fees for Services listed in an Order are exclusive of taxes and expenses.

b. Purchasing Entity understand that Purchasing Entity may receive multiple invoices for the Services Purchasing Entity ordered. Invoices will be submitted to Purchasing Entity pursuant to Oracle's Invoicing Standards Policy, which may be accessed at <http://oracle.com/contracts>.

c. Purchasing Entity agree and acknowledge that Purchasing Entity has not relied on the future availability of any Services, programs or updates in entering into the payment obligations in Purchasing Entity's Order; however, the preceding does not relieve Oracle of its obligation during the Services Period to deliver Services that Purchasing Entity has ordered per the terms of this Master Agreement.

22. Data Access Controls: Reserved. See the *Technical and Organizational Measures* section of the Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

23. Operations Management: Reserved.

24. Public Information: Subject to the requirements of Section 8 (Confidentiality, Non-Disclosure, and Injunctive Relief) and, in particular, Section 8(e), this Master Agreement and related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

25. Purchasing Entity Data:

Purchasing Entity retains all ownership and intellectual property rights in and to Your Content and Your Applications. Oracle or its licensors retain all ownership and intellectual property rights to the Services, including Oracle Programs and Ancillary Software, and derivative works thereof, and to anything developed or delivered by or on behalf of Oracle under this Master Agreement and the applicable Order.

Oracle may use tools, scripts, software, and utilities (collectively, the "Tools") to monitor and administer the Services and to help resolve the Purchasing Entity's Oracle service requests. The Tools will not collect or store any of Your Content or Your Applications

residing in the Services Environment, except as necessary to provide the Services or troubleshoot service requests or other problems in the Services. Information collected by the Tools (excluding Your Content and Your Applications) may also be used to assist in managing Oracle's product and service portfolio, to help Oracle address deficiencies in its product and service offerings, and for license and Services management.

26. Records Administration and Audit.

a. For a period of six (6) years from the effective date of an Ordering Document under this Master Agreement, Participating Entity shall have the right to audit records relating to invoices and payments for the services provided to Participating Entity thereunder, upon reasonable written notice to Oracle, no more than one time per year, at Participating Entity's cost, and provided that such audit does not unreasonably interfere with Oracle's normal business operations. Participating Entity shall have the right to contract a third-party audit firm to conduct such an audit, provided that such third-party audit firm agrees to Oracle's standard nondisclosure terms and to utilize standard audit software.

Oracle may audit the Purchasing Entity's use of the Services (e.g., through use of software tools) to assess whether the Purchasing Entity's use of the Services is in accordance with the Purchasing Entity's Order and the terms of this Master Agreement. The Purchasing Entity agrees to cooperate with Oracle's audit and provide reasonable assistance and access to information. Any such audit shall not unreasonably interfere with the Purchasing Entity's normal business operations. The Purchasing Entity agrees to pay within 30 days of written notification any fees applicable to the Purchasing Entity's use of the Services in excess of the Purchasing Entity's rights. If the Purchasing Entity does not pay, Oracle can end the Purchasing Entity's Services and/or the Purchasing Entity's Order. The Purchasing Entity agrees that Oracle shall not be responsible for any of the Purchasing Entity's costs incurred in cooperating with the audit.

See also *Audit Rights* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or

the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: Reserved. See Section 31: Warranties, Disclaimers, and Exclusive Remedies.

29. Title to Product: Oracle may provide the Purchasing Entity with on-line access to download certain Ancillary Software for use with the Services. If Oracle licenses Ancillary Software to the Purchasing Entity and does not specify separate terms for such Ancillary Software, then, subject to the Purchasing Entity's payment obligations, (a) the Purchasing Entity has the non-exclusive, non-assignable, worldwide limited right to use such Ancillary Software solely to facilitate the Purchasing Entity's access to, operation of, and/or use of the Services Environment, subject to the terms of this Master Agreement and the Purchasing Entity's Order, including the Services Specifications, (b) Oracle will maintain such Ancillary Software as part of the Cloud Services, and (c) the Purchasing Entity's right to use such Ancillary Software will terminate upon the earlier of Oracle's notice (which may be through posting on <https://support.oracle.com> or such other URL designated by Oracle) or the end of the Cloud Services associated with the Ancillary Software. If Ancillary Software is licensed to the Purchasing Entity under separate third party license terms, then the Purchasing Entity's use of such software is subject solely to such separate terms.

30. Data Privacy: Reserved. See Oracle Services Privacy Policy, which is subject to change from time to time at Oracle's discretion.

31. Warranties, Disclaimers, and Exclusive Remedies

a. Oracle warrants that, as of the effective date of the applicable Ordering Document, it has the right to enter into the Master Agreement and the applicable Ordering Document; Oracle's infringement indemnification obligations under the Indemnification Provision of the Master Agreement states the Purchasing Entity's exclusive remedy and Oracle's entire liability for any breach of this particular warranty.

b. Oracle warrants that it will perform (i) Cloud Services in all material respects as described in the Service Specifications, and (ii) Professional Services in a professional manner in accordance with the Service Specifications. If the Services provided to Purchasing Entity were not performed as warranted, Purchasing Entity must promptly provide written notice to Oracle that describes the deficiency in the Services (including, as applicable, the service request number notifying Oracle of the deficiency in the Services).

c. ORACLE DOES NOT GUARANTEE THAT (A) THE SERVICES WILL BE PERFORMED ERROR-FREE OR UNINTERRUPTED, OR THAT ORACLE WILL CORRECT ALL SERVICES ERRORS, (B) THE SERVICES WILL OPERATE IN COMBINATION WITH YOUR CONTENT OR YOUR APPLICATIONS, OR WITH ANY OTHER HARDWARE, SOFTWARE, SYSTEMS, SERVICES OR DATA NOT

PROVIDED BY ORACLE, AND (C) THE SERVICES WILL MEET PURCHASING ENTITY'S REQUIREMENTS, SPECIFICATIONS OR EXPECTATIONS. PURCHASING ENTITY ACKNOWLEDGES THAT ORACLE DOES NOT CONTROL THE TRANSFER OF DATA OVER COMMUNICATIONS FACILITIES, INCLUDING THE INTERNET, AND THAT THE SERVICES MAY BE SUBJECT TO LIMITATIONS, DELAYS, AND OTHER PROBLEMS INHERENT IN THE USE OF SUCH COMMUNICATIONS FACILITIES. ORACLE IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, OR OTHER DAMAGE RESULTING FROM SUCH PROBLEMS. ORACLE IS NOT RESPONSIBLE FOR ANY ISSUES RELATED TO THE PERFORMANCE, OPERATION OR SECURITY OF THE SERVICES THAT ARISE FROM YOUR CONTENT, YOUR APPLICATIONS OR THIRD PARTY CONTENT.

d. FOR ANY BREACH OF THE SERVICES WARRANTY, YOUR EXCLUSIVE REMEDY AND ORACLE'S ENTIRE LIABILITY SHALL BE THE CORRECTION OF THE DEFICIENT SERVICES THAT CAUSED THE BREACH OF WARRANTY, OR, IF ORACLE CANNOT SUBSTANTIALLY CORRECT THE DEFICIENCY IN A COMMERCIALY REASONABLE MANNER, PURCHASING ENTITY MAY END THE DEFICIENT SERVICES AND ORACLE WILL REFUND TO PURCHASING ENTITY THE FEES PAID FOR THE DEFICIENT SERVICES FOR THE PERIOD OF TIME DURING WHICH THE SERVICES WERE DEFICIENT.

e. TO THE EXTENT NOT PROHIBITED BY LAW, THESE WARRANTIES ARE EXCLUSIVE AND THERE ARE NO OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS INCLUDING FOR SOFTWARE, HARDWARE, SYSTEMS, NETWORKS OR ENVIRONMENTS OR FOR MERCHANTABILITY, SATISFACTORY QUALITY AND FITNESS FOR A PARTICULAR PURPOSE.

32. Transition Assistance:

Upon the end of the Services, the Purchasing Entity no longer has rights to access or use the Services, including the associated Oracle Programs and Services Environments; however for a period of up to 60 days after the end of the applicable Services Period, Oracle will make available Your Content and Your Applications then in the Services Environment for the purpose of retrieval by the Purchasing Entity. At the end of such 60 day period, and except as may be required by law, Oracle will delete or otherwise render inaccessible any of Your Content and Your Applications that remain in the Services Environment.

Upon the end of the Services, Oracle may be able to provide Professional Services to assist in transitioning Your Content and Your Applications, dependent upon Oracle Professional Services' capabilities and availability at the time a Purchasing Entity makes a request for such assistance. Any transition services performed by Oracle must be mutually agreed to by the parties in writing in a separate Ordering Document that is executed by both parties. Fees for any transition services will be at Oracle's then-current rates or as mutually agreed to by the parties in writing.

33. Waiver of Breach: Failure of the Lead State Master Agreement Administrator, Participating Entity, Purchasing Entity or Contractor to declare a default or enforce any rights and remedies shall not operate as a waiver under this Master Agreement or any Participating Addendum. Any waiver by the Lead State, Participating State, Participating Entity, or Contractor must be in writing. Waiver by the Lead State Master Agreement Administrator, Participating State Participating Entity, or Contractor of any default, right or remedy under this Master Agreement or Participating Addendum, or breach of any terms or requirements shall not be construed or operate as a waiver of any subsequent default or breach of such term or requirement, or of any other term or requirement under this Master Agreement, a Participating Addendum, or the Ordering Document.

34. Assignment of Antitrust Rights:

Contractor irrevocably assigns to a Participating Entity who is a state any claim for relief or cause of action which the Contractor now has or which may accrue to the Contractor in the future by reason of any violation of state or federal antitrust laws (15 U.S.C. § 1-15 or a Participating Entity's state antitrust provisions), as now in effect and as may be amended from time to time, in connection with any goods or services provided to the Contractor for the purpose of carrying out the Contractor's obligations under this Master Agreement or Participating Addendum, including, at a Participating Entity's option, the right to control any such litigation on such claim for relief or cause of action.

35. Debarment: The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

36. Performance and Payment Time Frames that Exceed Contract Duration:

Provided all Services have been purchased through an Oracle Ordering Document, all maintenance or other agreements for services entered into during the duration of an Order and whose performance and payment time frames extend beyond the duration of this Master Agreement shall remain in effect for performance and payment purposes (limited to the time frame and services established per each written agreement). No new leases, maintenance or other agreements for Services may be executed after the Master Agreement has expired. All Services which require payment must be paid in accordance with the invoice even after the expiration of the Master Agreement.

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. Reserved.

38. No Guarantee of Service Volumes: The Contractor acknowledges and agrees that the Lead State and NASPO ValuePoint makes no representation, warranty or condition as to the nature, timing, quality, quantity or volume of business for the Services or any other products and services that the Contractor may realize from this Master Agreement, or the compensation that may be earned by the Contractor by offering the Services. The Contractor acknowledges and agrees that it has conducted its own due diligence prior to entering into this Master Agreement as to all the foregoing matters.

39. NASPO ValuePoint eMarket Center: In July 2011, NASPO ValuePoint entered into a multi-year agreement with SciQuest, Inc. whereby SciQuest will provide certain electronic catalog hosting and management services to enable eligible NASPO ValuePoint's customers to access a central online website to view and/or shop the goods and services available from existing NASPO ValuePoint Cooperative Contracts. The central online website is referred to as the NASPO ValuePoint eMarket Center.

The Contractor will have visibility in the eMarket Center through Ordering Instructions. These Ordering Instructions are available at no cost to the Contractor and provided customers information regarding the Contractors website and ordering information.

At a minimum, the Contractor agrees to the following timeline: NASPO ValuePoint eMarket Center Site Admin shall provide a written request to the Contractor to begin Ordering Instruction process. The Contractor shall have thirty (30) days from receipt of written request to work with NASPO ValuePoint to provide any unique information and ordering instructions that the Contractor would like the customer to have.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by

Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement. Oracle reserves the right to negotiate such terms and to decline such Orders.

41. Government Support: Reserved.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at <http://www.naspo.org/WNCPO/Calculator.aspx>. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (i) state; (ii) entity/customer type, e.g. local government, higher education, K12, non-profit; (iii) Purchasing Entity name; (iv) Purchasing Entity bill-to and ship-to locations; (v) Purchasing Entity and Contractor Purchase Order identifier/number(s); (vi) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (vii) Purchase Order date; and (viii) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment F.

c. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the

conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. Entire Agreement: The Master Agreement, the information which is incorporated into the Master Agreement by written reference (including reference to information contained in a URL or referenced policy), and any written addenda thereto, together with the applicable Order and Participating Addendum, constitute the entire agreement of the parties to the Master Agreement, and supersede all prior or contemporaneous agreements or representations, written or oral, regarding the Services offered under the Master Agreement.

44. Additional Terms and Conditions:

a. Restrictions:

The Purchasing Entity may not and may not cause or permit others to:

- i. remove or modify any program markings or any notice of Oracle's or its licensors' proprietary rights;
- ii. make the programs or materials resulting from the Services (excluding Your Content and Your Applications) available in any manner to any third party for use in the third party's business operations (unless such access is expressly permitted for the specific Services the Purchasing Entity has acquired);
- iii. modify, make derivative works of, disassemble, decompile, reverse engineer, reproduce, distribute, republish or download any part of the Services (the foregoing prohibitions include but are not limited to review of data structures or similar materials produced by programs), or access or use the Services in order to build or support, and/or assist a third party in building or supporting, products or Services competitive to Oracle;
- iv. perform or disclose any benchmark or performance tests of the Services, including the Oracle Programs;
- v. perform or disclose any of the following security testing of the Services Environment or associated infrastructure: network discovery, port and service identification, vulnerability scanning, password cracking, remote access testing, or penetration testing; and
- vi. license, sell, rent, lease, transfer, assign, distribute, host, outsource, permit timesharing or service bureau use, or otherwise commercially exploit or make available the Services, Oracle Programs, Ancillary Software, Services Environments or Oracle materials, to any third party, other than as expressly permitted under the terms of the applicable Order.

b. Service Specifications:

- i. The Services are subject to and governed by Service Specifications applicable to the Purchasing Entity's Order. Service Specifications may define provisioning and management processes applicable to the Services (such as capacity planning), types and quantities of system resources (such as storage allotments), functional and technical aspects of the Oracle Programs, as well as any Services deliverables. The Purchasing Entity acknowledges that use of the Services in a manner not consistent with the Service Specifications may adversely affect Services performance and/or may result in additional fees. If the Services permit the Purchasing Entity to exceed the ordered quantity (e.g., soft limits on counts for Users, sessions, storage, etc.), then the Purchasing Entity is responsible for promptly purchasing such additional quantity to account for the Purchasing Entity's excess usage.
- ii. Oracle may make changes or updates to the Services (such as infrastructure, security, technical configurations, application features, etc.) during the Services Period, including to reflect changes in technology, industry practices, patterns of system use, and availability of Third Party Content. The Service Specifications are subject to change at Oracle's discretion; however, Oracle changes to the Service Specifications will not result in a material reduction in the level of performance, security or availability of the applicable Services provided to the Purchasing Entity for the duration of the Services Period.

c. Use of the Services:

- i. The Purchasing Entity is responsible for identifying and authenticating all Users, for approving access by such Users to the Services, for controlling against unauthorized access by Users, and for maintaining the confidentiality of usernames, passwords and account information. By federating or otherwise associating the Purchasing Entity's and the Purchasing Entity's Users' usernames, passwords and accounts with Oracle, the Purchasing Entity accept responsibility for the confidentiality and timely and proper termination of user records in the Purchasing Entity's local (intranet) identity infrastructure or on the Purchasing Entity's local computers. Oracle is not responsible for any harm caused by the Purchasing Entity's Users, including individuals who were not authorized to have access to the Services but who were able to gain access because usernames, passwords or accounts were not terminated on a timely basis in the Purchasing Entity's local identity management infrastructure or the Purchasing Entity's local computers. The Purchasing Entity is responsible for all activities that occur under the Purchasing Entity's and the Purchasing Entity's Users' usernames, passwords or accounts or as a result of the Purchasing Entity's or the Purchasing Entity's Users' access to the Services, and agree to notify Oracle immediately of any unauthorized use. The Purchasing Entity agrees to make every reasonable effort to prevent unauthorized third parties from accessing the Services.
- ii. The Purchasing Entity shall not use or permit use of the Services, including by uploading, emailing, posting, publishing or otherwise transmitting any material, including Your Content, Your Applications and Third Party Content, for any purpose that may (1) menace or harass any person or cause damage or injury to any person or property, (2)

involve the publication of any material that is false, defamatory, harassing or obscene, (3) violate privacy rights or promote bigotry, racism, hatred or harm, (4) constitute unsolicited bulk e-mail, "junk mail", "spam" or chain letters; (5) constitute an infringement of intellectual property or other proprietary rights, or (6) otherwise violate applicable laws, ordinances or regulations. In addition to any other rights afforded to Oracle under this Master Agreement, Oracle reserves the right, but has no obligation, to take remedial action if any material violates the restrictions in the foregoing sentence (the "Acceptable Use Policy"), including the removal or disablement of access to such material. Oracle shall have no liability to the Purchasing Entity in the event that Oracle takes such action. The Purchasing Entity shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness and ownership of all of Your Content and Your Applications. To the extent not prohibited by applicable law, the Purchasing Entity agrees to defend and indemnify Oracle against any claim arising out of a violation of the Purchasing Entity's obligations under this section.

iii. The Purchasing Entity is required to accept all patches, bug fixes, updates, maintenance and service packs (collectively, "Patches") necessary for the proper function and security of the Services, including for the Oracle Programs, as such Patches are generally released by Oracle as described in the Service Specifications. Oracle is not responsible for performance or security issues encountered with the Cloud Services that result from the Purchasing Entity's failure to accept the application of Patches that are necessary for the proper function and security of the Services. Except for emergency or security related maintenance activities, Oracle will coordinate with the Purchasing Entity the scheduling of application of Patches, where possible, based on Oracle's next available standard maintenance window.

d. Trial Use and Pilot Cloud Services:

i. For certain Cloud Services, Oracle may make available "trials" and "conference room pilots" for non-production evaluation purposes. Cloud trials and conference room pilots must be ordered under a separate agreement.

ii. Oracle may make available "production pilots" for certain Cloud Services under this Master Agreement. Production pilots ordered by the Purchasing Entity is described in the Service Specifications applicable to the Purchasing Entity's Order, and are provided solely for the Purchasing Entity to evaluate and test Cloud Services for the Purchasing Entity's internal business purposes. The Purchasing Entity may be required to order certain Professional Services as a prerequisite to an Order for a production pilot.

e. Services Period; End of Services:

i. Services provided under this Master Agreement shall be provided for the Services Period defined in the Purchasing Entity's Order, unless earlier suspended or terminated in accordance with this Master Agreement or the Order. Even though the Purchasing Entity order Cloud Services that are designated in the Service Specifications or the Purchasing Entity's Order as Auto Renew, such services will NOT automatically renew. In order to renew, the Purchasing Entity must provide Oracle with written notice no later than thirty (30) days prior to the end of the applicable Services Period of the Purchasing Entity's intent to renew and the Purchasing Entity must execute a contract modification

evidencing such renewal. The preceding sentence shall not apply if Oracle provides the Purchasing Entity with written notice no later than ninety (90) days prior to the end of the applicable Services Period of its intention not to renew such Cloud Services.

ii. Oracle may temporarily suspend the Purchasing Entity's password, account, and access to or use of the Services if the Purchasing Entity or the Purchasing Entity's Users violate any provision within the 'Rights Granted', 'Ownership and Restrictions', 'Fees and Taxes', 'Use of the Services', or 'Export' sections of this Master Agreement, or if in Oracle's reasonable judgment, the Services or any component thereof are about to suffer a significant threat to security or functionality. Oracle will provide advance notice to the Purchasing Entity of any such suspension in Oracle's reasonable discretion based on the nature of the circumstances giving rise to the suspension. Oracle will use reasonable efforts to re-establish the affected Services promptly after Oracle determines, in its reasonable discretion, that the situation giving rise to the suspension has been cured; however, during any suspension period, Oracle will make available to the Purchasing Entity Your Content and Your Applications as existing in the Services Environment on the date of suspension. Oracle may terminate the Services under an Order if any of the foregoing causes of suspension is not cured within 30 days after Oracle's initial notice thereof. Any suspension or termination by Oracle under this paragraph shall not excuse the Purchasing Entity from the Purchasing Entity's obligation to make payment(s) under this Master Agreement.

iii. If the Purchasing Entity has used an Oracle Financing Division contract to pay for the fees due under an Order and the Purchasing Entity is in default under that contract, the Purchasing Entity may not use the Services that are subject to such contract.

iv. Provisions that survive termination or expiration of this Master Agreement are those relating to limitation of liability, indemnification, payment and others which by their nature are intended to survive.

f. Limitation of Liability:

a. CONTRACTOR'S AGGREGATE LIABILITY FOR ALL DAMAGES ARISING OUT OF OR RELATED TO THIS MASTER AGREEMENT OR A PURCHASING ENTITY'S ORDER, WHETHER IN CONTRACT OR TORT, OR OTHERWISE, SHALL IN NO EVENT EXCEED THE GREATER OF (i) TWO (2) TIMES THE TOTAL AMOUNTS ACTUALLY PAID TO ORACLE IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO SUCH LIABILITY LESS ANY REFUNDS OR CREDITS RECEIVED BY THE PURCHASING ENTITY FROM CONTRACTOR UNDER SUCH ORDER OR (ii) ONE MILLION DOLLARS (U.S.\$1,000,000).

b. NOTWITHSTANDING THE ABOVE, NEITHER THE CONTRACTOR NOR THE PURCHASING ENTITY SHALL BE LIABLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, PUNITIVE OR SPECIAL DAMAGES OF ANY KIND ARISING DIRECTLY OR INDIRECTLY OUT OF THIS MASTER AGREEMENT OR A PURCHASING ENTITY'S ORDER, INCLUDING, WITHOUT LIMITATION, DAMAGES

RESULTING FROM LOSS OF USE OR LOSS OF PROFIT OR REVENUE (EXCLUDING FEES UNDER THIS MASTER AGREEMENT), DATA, OR DATA USE BY THE PURCHASING ENTITY, THE CONTRACTOR, OR BY OTHERS.

c. Contractor's obligation to indemnify for (i) infringement claims or damages under Sections 13(a)-(d) or (ii) claim(s) of bodily injury and tangible personal property damage under Section 13(e) shall apply without regard to whether the damages under such claim(s) (y) are classified as direct, indirect, or otherwise, or (z) exceed the limits on liability under this Section 44(f) (Additional Terms and Conditions: Limitation of Liability).

g. Third Party Web Sites, Content, Products and Services:

i. The Services may enable the Purchasing Entity to link to, transmit Your Content to, or otherwise access, other Web sites, platforms, content, products, services, and information of third parties. Oracle does not control and is not responsible for such Web sites or platforms or any such content, products, services and information accessible from or provided through the Services, and the Purchasing Entity bear all risks associated with access to and use of such Web sites and third party content, products, services and information.

ii. Any Third Party Content made accessible by Oracle is provided on an "as-is" and "as available" basis without any warranty of any kind. Third Party Content may be indecent, offensive, inaccurate, infringing or otherwise objectionable or unlawful, and the Purchasing Entity acknowledge that Oracle is not responsible for and under no obligation to control, monitor or correct Third Party Content; however, Oracle reserves the right to take remedial action if any such content violates applicable restrictions under Section 6.2 of this Master Agreement, including the removal of, or disablement of access to, such content. Oracle disclaims all liabilities arising from or related to Third Party Content.

iii. The Purchasing Entity acknowledge that: (1) the nature, type, quality and availability of Third Party Content may change at any time during the Services Period, and (2) features of the Services that interoperate with third parties such as Facebook™, YouTube™ and Twitter™, etc. (each, a "Third Party Service"), depend on the continuing availability of such third parties' respective application programming interfaces (APIs) for use with the Services. Oracle may update, change or modify the Services under this Master Agreement as a result of a change in, or unavailability of, such Third Party Content, Third Party Services or APIs. If any third party ceases to make its Third Party Content or APIs available on reasonable terms for the Services, as determined by Oracle in its sole discretion, Oracle may cease providing access to the affected Third Party Content or Third Party Services without any liability to the Purchasing Entity. Any changes to Third Party Content, Third Party Services or APIs, including their availability or unavailability, during the Services Period does not affect the Purchasing Entity's obligations under this Master Agreement or the applicable Order, and the Purchasing Entity will not be entitled to any refund, credit or other compensation due to any such changes.

iv. Any Third Party Content that the Purchasing Entity store in the Purchasing Entity's Services Environment will count towards any storage or other allotments applicable to

the Cloud Services that the Purchasing Entity ordered.

h. Service Analyses:

Oracle may (i) compile statistical and other information related to the performance, operation and use of the Services, and (ii) use data from the Services Environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). Oracle may make Service Analyses publicly available; however, Service Analyses will not incorporate Your Content or Confidential Information in a form that could serve to identify the Purchasing Entity or any individual, and Service Analyses do not constitute Personal Data. Oracle retains all intellectual property rights in Service Analyses.

i. Export:

i. Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Services. the Purchasing Entity agree that such export laws govern the Purchasing Entity's use of the Services (including technical data) and any Services deliverables provided under this Master Agreement, and the Purchasing Entity agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). the Purchasing Entity agree that no data, information, software programs and/or materials resulting from Services (or direct product thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology.

ii. the Purchasing Entity acknowledge that the Cloud Services are designed with capabilities for the Purchasing Entity and the Purchasing Entity's Users to access the Services Environment without regard to geographic location and to transfer or otherwise move Your Content and Your Applications between the Services Environment and other locations such as User workstations. The Purchasing Entity is solely responsible for the authorization and management of User accounts, as well as export control and geographic transfer of Your Content and Your Applications.

j. Notice:

i. Any notice required under this Master Agreement shall be provided to the other party in writing. If the Purchasing Entity has a dispute with Oracle or if the Purchasing Entity wish to provide a notice under the Indemnification Section of this Master Agreement, or if the Purchasing Entity become subject to insolvency or other similar legal proceedings, the Purchasing Entity will promptly send written notice to: Oracle America, Inc., 500 Oracle Parkway, Redwood Shores, CA 94065. Attention: General Counsel, Legal Department.

ii. To request a termination of Services in accordance with this Master Agreement, the Purchasing Entity must submit a service request to Oracle at the address specified in the Purchasing Entity's Order or the Service Specifications.

iii. Oracle may give notices applicable to Oracle's Cloud Services customer base by means of a general notice on the Oracle portal for the Cloud Services, and notices specific to the Purchasing Entity by electronic mail to the Purchasing Entity's e-mail address on record in Oracle's account information or by written communication sent by first class mail or pre-paid post to the Purchasing Entity's address on record in Oracle's account information.

k. Miscellaneous:

i. If any term of this Master Agreement is found to be invalid or unenforceable, the remaining provisions will remain effective and such term shall be replaced with another term consistent with the purpose and intent of this Master Agreement.

ii. Oracle Programs and Services are not designed for or specifically intended for use in nuclear facilities or other hazardous applications. The Purchasing Entity agrees that it is the Purchasing Entity's responsibility to ensure safe use of Oracle Programs and Services in such applications.

iii. The Purchasing Entity shall obtain at the Purchasing Entity's sole expense any rights and consents from third parties necessary for Your Content, Your Applications, and Third Party Content, as well as other vendor's products provided by the Purchasing Entity that the Purchasing Entity use with the Services, including such rights and consents as necessary for Oracle to perform the Services under this Master Agreement.

iv. The Purchasing Entity remains solely responsible for the Purchasing Entity's regulatory compliance in connection with the Purchasing Entity's use of the Services. The Purchasing Entity is responsible for making Oracle aware of any technical requirements that result from the Purchasing Entity's regulatory obligations prior to entering into an Order governed by this Master Agreement. Oracle will cooperate with the Purchasing Entity's efforts to determine whether use of the standard Oracle Services offering is consistent with those requirements. Additional fees may apply to any additional work performed by Oracle or changes to the Services.

v. The purchase of Cloud Services, Professional Services, or other service offerings, programs or products are all separate offers and separate from any other Order. The Purchasing Entity understands that the Purchasing Entity may purchase Cloud Services, Professional Services, or other service offerings, programs or products independently of any other Order. The Purchasing Entity's obligation to pay under any Order is not contingent on performance of any other service offerings or delivery of programs or products.

Exhibit 1 to the Master Agreement:

Software-as-a-Service

1. Data Ownership and Rights Granted: The control and ownership of Data remains with the Purchasing Entity, and as between Purchasing Entity and Oracle, Purchasing Entity will at all times remain the data controller for the purposes of the Master Agreement, the applicable Participating Addendum, any orders of Cloud Services placed under the Master Agreement and any Participating Addendum, and the Data Processing Agreement. See also *Controller of Data* section of the Data Processing Agreement.

For the duration of the Services Period and subject to the Purchasing Entity's payment obligations, and except as otherwise set forth in the Master Agreement or the Purchasing Entity's Order, the Purchasing Entity has the non-exclusive, non-assignable, worldwide limited right to access and use the Services that the Purchasing Entity ordered, including anything developed by Oracle and delivered to the Purchasing Entity as part of the Services, solely for the Purchasing Entity's internal business operations and subject to the terms of the Master Agreement and the Order, including the Service Specifications. The Purchasing Entity may allow its Users to use the Services for this purpose and the Purchasing Entity is responsible for its Users' compliance with the Master Agreement and the Order.

The Purchasing Entity does not acquire under this Master Agreement any right or license to use the Services, including the Oracle Programs and Services Environment, in excess of the scope and/or duration of the Services stated in the Order. Upon the end of the Services ordered, the Purchasing Entity's right to access and use the Services will terminate.

To enable Oracle to provide the Purchasing Entity and its Users with the Services, the Purchasing Entity grants Oracle the right to use, process and transmit, in accordance with this Master Agreement and the Order, Your Content and Your Applications for the duration of the Services Period plus any additional post-termination period during which Oracle provides the Purchasing Entity with access to retrieve an export file of Your Content and Your Applications. If Your Applications include third party programs, the Purchasing Entity acknowledges that Oracle may allow providers of those third party programs to access the Services Environment, including Your Content and Your Applications, as required for the interoperation of such third party programs with the Services. Oracle will not be responsible for any use, disclosure, modification or deletion of Your Content or Your Applications resulting from any such access by third party program providers or for the interoperability of such third party programs with the Services.

Except as otherwise expressly set forth in the Purchasing Entity's Order for certain Cloud Services offerings (e.g., a private cloud hosted at the Purchasing Entity's facility, if available under this Master Agreement), the Purchasing Entity acknowledges that Oracle has no delivery obligation for Oracle Programs and will not ship copies of such programs to the Purchasing Entity as part of the Services.

As part of certain Cloud Services offerings, Oracle may provide the Purchasing Entity with access to Third Party Content. The type and scope of any Third Party Content is defined in the Purchasing Entity's Order or applicable Service Specifications. The third party owner, author or provider of such Third Party

Content retains all ownership and intellectual property rights in and to that content, and the Purchasing Entity's rights to use such Third Party Content are subject to, and governed by, the terms applicable to such content as specified by such third party owner, author or provider, unless otherwise specified in the Purchasing Entity's Order.

The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

2. Data Protection:

In performing the Services, Oracle will comply with the Oracle Services Privacy Policy, which is available at <http://www.oracle.com/html/Services-privacy-policy.html> and incorporated herein by reference. The Oracle Services Privacy Policy is subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of protection provided for the Purchasing Entity's Personal Data provided as part of Your Content during the Services Period of the Purchasing Entity's Order.

Oracle's Data Processing Agreement for Oracle Cloud Services (the "Data Processing Agreement"), which is available at <http://www.oracle.com/dataprocessingagreement> and incorporated herein by reference, describes the parties' respective roles for the processing and control of Personal Data that the Purchasing Entity provides to Oracle as part of the Cloud Services. Oracle will act as a data processor, and will act on the Purchasing Entity's instruction concerning the treatment of the Purchasing Entity's Personal Data residing in the Services Environment, as specified in the Master Agreement, the Data Processing Agreement and the applicable Order. The Purchasing Entity agree to provide any notices and obtain any consents related to the Purchasing Entity's use of the Services and Oracle's provision of the Services, including those related to the collection, use, processing, transfer and disclosure of Personal Data.

The Service Specifications applicable to the Purchasing Entity's Order define the administrative, physical, technical and other safeguards applied to Your Content residing in the Services Environment, and describe other aspects of system management applicable to the Services. The Purchasing Entity is responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising from Your Content and Your Applications, including any viruses, Trojan horses, worms or other programming routines contained in Your Content or Your Applications that could limit or harm the functionality of a computer or that could damage, intercept or expropriate data. The Purchasing Entity may disclose or transfer, or instruct Oracle to disclose or transfer in writing, Your Content or Your Applications to a third party, and upon such disclosure or transfer Oracle is no longer responsible for the security or confidentiality of such content and applications outside of Oracle.

The Purchasing Entity may not provide Oracle access to health, payment card or similarly sensitive personal information that imposes specific data security obligations for the processing of such data

unless specified in the Purchasing Entity's Order. If available, the Purchasing Entity may purchase services from Oracle (e.g., Oracle Payment Card Industry Compliance Services, Oracle HIPAA Security Services, Oracle Federal Security Services, etc.) designed to address particular data protection requirements applicable to the Purchasing Entity's business or Your Content.

3. Data Location:

The Purchasing Entity's Order will specify the Data Center Region in which the Purchasing Entity's Services Environment will reside. As described in the Service Specifications and to the extent applicable to the Cloud Services that the Purchasing Entity has ordered, Oracle will provide production, test, and backup environments in the Data Center Region stated in the Purchasing Entity's Order. Oracle and its affiliates may perform certain aspects of Cloud Services, such as service administration and support, as well as other Services (including Professional Services and disaster recovery), from locations and/or through use of subcontractors, worldwide.

4. Incident Management and Data Breach Notification and Responsibilities: Reserved. See *Incident Management and Breach Notification* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

5. Personal Data Breach Responsibilities: Reserved. See section 4 (Incident Management and Data Breach Notification and Responsibilities) above.

6. Notification of Legal Requests: Reserved. See *Legally Required Disclosures* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

7. Termination and Suspension of Service: Reserved. See section 32 (Transition Assistance) of the Master Agreement.

8. Background Checks: Oracle, or its agent, has performed a background check on Oracle employees hired on or after January 1, 2003 in the United States. As of the effective date the Ordering Document, the background check is used to attempt to : (i) ascertain an employee's previous employment with up to four (4) employers within the seven (7) years preceding the date of the check; (ii) ascertain an employee's highest degree earned; (iii) assess any public criminal records uncovered for an employee within the seven (7) years preceding the date of the check; and (iv) check for matches on the Office of Foreign Asset Control's Specially Designated Nationals and Foreign Sanctions Evaders Lists. The background check is adjudicated by Oracle. While all criminal records are individually assessed in accordance with applicable laws and agency guidance, generally, significant crimes involving violence, dishonesty, and certain drug-related offenses are considered disqualifiers, except where a diversion program was successfully completed and/or the case was discharged or judicially dismissed. In general, international transfers and individuals with valid United States government issued security clearance are not subject to a background check. Processing and procedural variances may apply to students/interns, university recruiting hires, and to employees of companies acquired by Oracle.

9. Access to Security Logs and Reports: Reserved.

10. Audit Rights: Reserved. See *Audit Rights* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

11. Data Center Audit: Reserved. See section 10 (Audit Rights) above.

12. Change Control and Advance Notice: Reserved. See *Oracle Cloud Change Management and Maintenance* section of Oracle Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

13. Security: Reserved.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Controller of Data: Reserved. See *Controller of Data* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

16. Service Availability Provisions: Reserved. See *Service Availability Provisions* and *Definition of Unplanned Downtime* sections of Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

17. Affiliates and Subprocessors: Reserved. See *Affiliates and Subprocessors* section of Data Processing Agreement which is subject to change from time to time at Oracle's discretion.

18. Right to Remove Individuals: Reserved.

19. Business Continuity and Disaster Recovery: Reserved. See *Oracle Cloud Service Continuity Policy* section of Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

20. Compliance with Accessibility Standards: The extent to which an Oracle product is, at the time of delivery, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of the Architectural and Transportation Barriers Compliance Board standards set out in 36 CFR Part 1194 (known as 'Section 508'), in effect as of the date of the Master Agreement, is indicated by the comments and exceptions (some of which may be significant, if any) noted on the applicable Voluntary Product Accessibility Templates (VPAT) available at www.oracle.com/accessibility for each product, when they are used in accordance with Oracle's associated documents and other written information, and provided that any assistive technologies and any other products used with them properly interoperate with them. In the event that no VPAT is available for a particular Oracle product, please contact the Oracle Accessibility Program Office at accessible_ww@oracle.com. In some cases, the outcome may be that a product is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all. No other terms, conditions, statements or any other such representations regarding or relating to accessibility shall apply to the Oracle products provided under this agreement.

21. Web Services: Reserved.

22. Data Protection: Reserved. See *Scope of Customer-managed Public Cloud Services* section of Oracle Hosting and Delivery Policies which is subject to change from time to time at Oracle's discretion.

23. Subscription Terms: Reserved. See section 1 (Data Ownership and Rights Granted) above and section 26 (Title to Product) of Attachment A.

Exhibit 2 to the Master Agreement:

Platform-as-a-Service

1. Data Ownership and Rights Granted: The control and ownership of Data remains with the Purchasing Entity, and as between Purchasing Entity and Oracle, Purchasing Entity will at all times remain the data controller for the purposes of the Master Agreement, the applicable Participating Addendum, any orders of Cloud Services placed under the Master Agreement and any Participating Addendum, and the Data Processing Agreement. See also *Controller of Data* section of the Data Processing Agreement.

For the duration of the Services Period and subject to the Purchasing Entity's payment obligations, and except as otherwise set forth in the Master Agreement or the Purchasing Entity's Order, the Purchasing Entity has the non-exclusive, non-assignable, worldwide limited right to access and use the Services that the Purchasing Entity ordered, including anything developed by Oracle and delivered to the Purchasing Entity as part of the Services, solely for the Purchasing Entity's internal business operations and subject to the terms of the Master Agreement and the Order, including the Service Specifications. The Purchasing Entity may allow its Users to use the Services for this purpose and the Purchasing Entity is responsible for its Users' compliance with the Master Agreement and the Order.

The Purchasing Entity does not acquire under this Master Agreement any right or license to use the Services, including the Oracle Programs and Services Environment, in excess of the scope and/or duration of the Services stated in the Order. Upon the end of the Services ordered, the Purchasing Entity's right to access and use the Services will terminate.

To enable Oracle to provide the Purchasing Entity and its Users with the Services, the Purchasing Entity grants Oracle the right to use, process and transmit, in accordance with this Master Agreement and the Order, Your Content and Your Applications for the duration of the Services Period plus any additional post-termination period during which Oracle provides the Purchasing Entity with access to retrieve an export file of Your Content and Your Applications. If Your Applications include third party programs, the Purchasing Entity acknowledges that Oracle may allow providers of those third party programs to access the Services Environment, including Your Content and Your Applications, as required for the interoperation of such third party programs with the Services. Oracle will not be responsible for any use, disclosure, modification or deletion of Your Content or Your Applications resulting from any such access by third party program providers or for the interoperability of such third party programs with the Services.

Except as otherwise expressly set forth in the Purchasing Entity's Order for certain Cloud Services offerings (e.g., a private cloud hosted at the Purchasing Entity's facility, if available under this Master Agreement), the Purchasing Entity acknowledges that Oracle has no delivery obligation for Oracle Programs and will not ship copies of such programs to the Purchasing Entity as part of the Services.

As part of certain Cloud Services offerings, Oracle may provide the Purchasing Entity with access to Third Party Content. The type and scope of any Third Party Content is defined in the Purchasing Entity's Order or applicable Service Specifications. The third party owner, author or provider of such Third Party

Content retains all ownership and intellectual property rights in and to that content, and the Purchasing Entity's rights to use such Third Party Content are subject to, and governed by, the terms applicable to such content as specified by such third party owner, author or provider, unless otherwise specified in the Purchasing Entity's Order.

The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

2. Data Protection:

In performing the Services, Oracle will comply with the Oracle Services Privacy Policy, which is available at <http://www.oracle.com/html/Services-privacy-policy.html> and incorporated herein by reference. The Oracle Services Privacy Policy is subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of protection provided for the Purchasing Entity's Personal Data provided as part of Your Content during the Services Period of the Purchasing Entity's Order.

Oracle's Data Processing Agreement for Oracle Cloud Services (the "Data Processing Agreement"), which is available at <http://www.oracle.com/dataprocessingagreement> and incorporated herein by reference, describes the parties' respective roles for the processing and control of Personal Data that the Purchasing Entity provides to Oracle as part of the Cloud Services. Oracle will act as a data processor, and will act on the Purchasing Entity's instruction concerning the treatment of the Purchasing Entity's Personal Data residing in the Services Environment, as specified in the Master Agreement, the Data Processing Agreement and the applicable Order. The Purchasing Entity agree to provide any notices and obtain any consents related to the Purchasing Entity's use of the Services and Oracle's provision of the Services, including those related to the collection, use, processing, transfer and disclosure of Personal Data.

The Service Specifications applicable to the Purchasing Entity's Order define the administrative, physical, technical and other safeguards applied to Your Content residing in the Services Environment, and describe other aspects of system management applicable to the Services. The Purchasing Entity is responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising from Your Content and Your Applications, including any viruses, Trojan horses, worms or other programming routines contained in Your Content or Your Applications that could limit or harm the functionality of a computer or that could damage, intercept or expropriate data. The Purchasing Entity may disclose or transfer, or instruct Oracle to disclose or transfer in writing, Your Content or Your Applications to a third party, and upon such disclosure or transfer Oracle is no longer responsible for the security or confidentiality of such content and applications outside of Oracle.

The Purchasing Entity may not provide Oracle access to health, payment card or similarly sensitive personal information that imposes specific data security obligations for the processing of such data

unless specified in the Purchasing Entity's Order. If available, the Purchasing Entity may purchase services from Oracle (e.g., Oracle Payment Card Industry Compliance Services, Oracle HIPAA Security Services, Oracle Federal Security Services, etc.) designed to address particular data protection requirements applicable to the Purchasing Entity's business or Your Content.

3. Data Location: The Purchasing Entity's Order will specify the Data Center Region in which the Purchasing Entity's Services Environment will reside. As described in the Service Specifications and to the extent applicable to the Cloud Services that the Purchasing Entity has ordered, Oracle will provide production, test, and backup environments in the Data Center Region stated in the Purchasing Entity's Order. Oracle and its affiliates may perform certain aspects of Cloud Services, such as service administration and support, as well as other Services (including Professional Services and disaster recovery), from locations and/or through use of subcontractors, worldwide..

4. Incident Management and Data Breach Notification and Responsibilities: Reserved. See *Incident Management and Breach Notification* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

5. Personal Data Breach Responsibilities: Reserved. See section 4 (Incident Management and Data Breach Notification and Responsibilities) above.

6. Notification of Legal Requests: Reserved. See *Legally Required Disclosures* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

7. Termination and Suspension of Service: Reserved. See section 32 (Transition Assistance) of the Master Agreement.

8. Background Checks: Oracle, or its agent, has performed a background check on Oracle employees hired on or after January 1, 2003 in the United States. As of the effective date the Ordering Document, the background check is used to attempt to : (i) ascertain an employee's previous employment with up to four (4) employers within the seven (7) years preceding the date of the check; (ii) ascertain an employee's highest degree earned; (iii) assess any public criminal records uncovered for an employee within the seven (7) years preceding the date of the check; and (iv) check for matches on the Office of Foreign Asset Control's Specially Designated Nationals and Foreign Sanctions Evaders Lists. The background check is adjudicated by Oracle. While all criminal records are individually assessed in accordance with applicable laws and agency guidance, generally, significant crimes involving violence, dishonesty, and certain drug-related offenses are considered disqualifiers, except where a diversion program was successfully completed and/or the case was discharged or judicially dismissed. In general, international transfers and individuals with valid United States government issued security clearance are not subject to a background check. Processing and procedural variances may apply to students/interns, university recruiting hires, and to employees of companies acquired by Oracle.

9. Access to Security Logs and Reports: Reserved.

10. Audit Rights: Reserved. See *Audit Rights* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

11. Data Center Audit: Reserved. See section 10 (Audit Rights) above.

12. Change Control and Advance Notice: Reserved. See *Oracle Cloud Change Management and Maintenance* section of Oracle Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

13. Security: Reserved.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Controller of Data: Reserved. See *Controller of Data* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

16. Service Availability Provisions: Reserved. See *Service Availability Provisions* and *Definition of Unplanned Downtime* sections of Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

17. Affiliates and Subprocessors: Reserved. See *Affiliates and Subprocessors* section of Data Processing Agreement which is subject to change from time to time at Oracle's discretion.

18. Business Continuity and Disaster Recovery: Reserved. See *Oracle Cloud Service Continuity Policy* section of Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

19. Compliance with Accessibility Standards: The extent to which an Oracle product is, at the time of delivery, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of the Architectural and Transportation Barriers Compliance Board standards set out in 36 CFR Part 1194 (known as 'Section 508'), in effect as of the date of the Master Agreement, is indicated by the comments and exceptions (some of which may be significant, if any) noted on the applicable Voluntary Product Accessibility Templates (VPAT) available at www.oracle.com/accessibility for each product, when they are used in accordance with Oracle's associated documents and other written information, and provided that any assistive technologies and any other products used with them properly interoperate with them. In the event that no VPAT is available for a particular Oracle product, please contact the Oracle Accessibility Program Office at accessible_ww@oracle.com. In some cases, the outcome may be that a product is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all. No other terms, conditions, statements or any other such representations regarding or relating to accessibility shall apply to the Oracle products provided under this agreement.

20. Web Services: Reserved.

21. Data Protection: Reserved. See *Scope of Customer-managed Public Cloud Services* section of Oracle Hosting and Delivery Policies which is subject to change from time to time at Oracle's discretion.

22. Subscription Terms: Reserved. See section 1 (Data Ownership and Rights Granted) above and section 26 (Title to Product) of Attachment A.

Exhibit 3 to the Master Agreement:

Infrastructure-as-a-Service

1. Data Ownership and Rights Granted: The control and ownership of Data remains with the Purchasing Entity, and as between Purchasing Entity and Oracle, Purchasing Entity will at all times remain the data controller for the purposes of the Master Agreement, the applicable Participating Addendum, any orders of Cloud Services placed under the Master Agreement and any Participating Addendum, and the Data Processing Agreement. See also *Controller of Data* section of the Data Processing Agreement.

For the duration of the Services Period and subject to the Purchasing Entity's payment obligations, and except as otherwise set forth in the Master Agreement or the Purchasing Entity's Order, the Purchasing Entity has the non-exclusive, non-assignable, worldwide limited right to access and use the Services that the Purchasing Entity ordered, including anything developed by Oracle and delivered to the Purchasing Entity as part of the Services, solely for the Purchasing Entity's internal business operations and subject to the terms of the Master Agreement and the Order, including the Service Specifications. The Purchasing Entity may allow its Users to use the Services for this purpose and the Purchasing Entity is responsible for its Users' compliance with the Master Agreement and the Order.

The Purchasing Entity does not acquire under this Master Agreement any right or license to use the Services, including the Oracle Programs and Services Environment, in excess of the scope and/or duration of the Services stated in the Order. Upon the end of the Services ordered, the Purchasing Entity's right to access and use the Services will terminate.

To enable Oracle to provide the Purchasing Entity and its Users with the Services, the Purchasing Entity grants Oracle the right to use, process and transmit, in accordance with this Master Agreement and the Order, Your Content and Your Applications for the duration of the Services Period plus any additional post-termination period during which Oracle provides the Purchasing Entity with access to retrieve an export file of Your Content and Your Applications. If Your Applications include third party programs, the Purchasing Entity acknowledges that Oracle may allow providers of those third party programs to access the Services Environment, including Your Content and Your Applications, as required for the interoperation of such third party programs with the Services. Oracle will not be responsible for any use, disclosure, modification or deletion of Your Content or Your Applications resulting from any such access by third party program providers or for the interoperability of such third party programs with the Services.

Except as otherwise expressly set forth in the Purchasing Entity's Order for certain Cloud Services offerings (e.g., a private cloud hosted at the Purchasing Entity's facility, if available under this Master Agreement), the Purchasing Entity acknowledges that Oracle has no delivery obligation for Oracle Programs and will not ship copies of such programs to the Purchasing Entity as part of the Services.

As part of certain Cloud Services offerings, Oracle may provide the Purchasing Entity with access to Third Party Content. The type and scope of any Third Party Content is defined in the Purchasing Entity's Order or applicable Service Specifications. The third party owner, author or provider of such Third Party

Content retains all ownership and intellectual property rights in and to that content, and the Purchasing Entity's rights to use such Third Party Content are subject to, and governed by, the terms applicable to such content as specified by such third party owner, author or provider, unless otherwise specified in the Purchasing Entity's Order.

The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

2. Data Protection: In performing the Services, Oracle will comply with the Oracle Services Privacy Policy, which is available at <http://www.oracle.com/html/Services-privacy-policy.html> and incorporated herein by reference. The Oracle Services Privacy Policy is subject to change at Oracle's discretion; however, Oracle policy changes will not result in a material reduction in the level of protection provided for the Purchasing Entity's Personal Data provided as part of Your Content during the Services Period of the Purchasing Entity's Order.

Oracle's Data Processing Agreement for Oracle Cloud Services (the "Data Processing Agreement"), which is available at <http://www.oracle.com/dataprocessingagreement> and incorporated herein by reference, describes the parties' respective roles for the processing and control of Personal Data that the Purchasing Entity provides to Oracle as part of the Cloud Services. Oracle will act as a data processor, and will act on the Purchasing Entity's instruction concerning the treatment of the Purchasing Entity's Personal Data residing in the Services Environment, as specified in the Master Agreement, the Data Processing Agreement and the applicable Order. The Purchasing Entity agree to provide any notices and obtain any consents related to the Purchasing Entity's use of the Services and Oracle's provision of the Services, including those related to the collection, use, processing, transfer and disclosure of Personal Data.

The Service Specifications applicable to the Purchasing Entity's Order define the administrative, physical, technical and other safeguards applied to Your Content residing in the Services Environment, and describe other aspects of system management applicable to the Services. The Purchasing Entity is responsible for any security vulnerabilities, and the consequences of such vulnerabilities, arising from Your Content and Your Applications, including any viruses, Trojan horses, worms or other programming routines contained in Your Content or Your Applications that could limit or harm the functionality of a computer or that could damage, intercept or expropriate data. The Purchasing Entity may disclose or transfer, or instruct Oracle to disclose or transfer in writing, Your Content or Your Applications to a third party, and upon such disclosure or transfer Oracle is no longer responsible for the security or confidentiality of such content and applications outside of Oracle.

The Purchasing Entity may not provide Oracle access to health, payment card or similarly sensitive personal information that imposes specific data security obligations for the processing of such data unless specified in the Purchasing Entity's Order. If available, the Purchasing Entity may purchase

services from Oracle (e.g., Oracle Payment Card Industry Compliance Services, Oracle HIPAA Security Services, Oracle Federal Security Services, etc.) designed to address particular data protection requirements applicable to the Purchasing Entity's business or Your Content.

3. Data Location: The Purchasing Entity's Order will specify the Data Center Region in which the Purchasing Entity's Services Environment will reside. As described in the Service Specifications and to the extent applicable to the Cloud Services that the Purchasing Entity has ordered, Oracle will provide production, test, and backup environments in the Data Center Region stated in the Purchasing Entity's Order. Oracle and its affiliates may perform certain aspects of Cloud Services, such as service administration and support, as well as other Services (including Professional Services and disaster recovery), from locations and/or through use of subcontractors, worldwide.

4. Incident Management and Data Breach Notification and Responsibilities: Reserved. See *Incident Management and Breach Notification* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

5. Personal Data Breach Responsibilities: Reserved. See section 4 (Incident Management and Data Breach Notification and Responsibilities) above.

6. Notification of Legal Requests: Reserved. See *Legally Required Disclosures* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

7. Termination and Suspension of Service: Reserved. See section 32 (Transition Assistance) of the Master Agreement.

8. Background Checks: Oracle, or its agent, has performed a background check on Oracle employees hired on or after January 1, 2003 in the United States. As of the effective date the Ordering Document, the background check is used to attempt to : (i) ascertain an employee's previous employment with up to four (4) employers within the seven (7) years preceding the date of the check; (ii) ascertain an employee's highest degree earned; (iii) assess any public criminal records uncovered for an employee within the seven (7) years preceding the date of the check; and (iv) check for matches on the Office of Foreign Asset Control's Specially Designated Nationals and Foreign Sanctions Evaders Lists. The background check is adjudicated by Oracle. While all criminal records are individually assessed in accordance with applicable laws and agency guidance, generally, significant crimes involving violence, dishonesty, and certain drug-related offenses are considered disqualifiers, except where a diversion program was successfully completed and/or the case was discharged or judicially dismissed. In general, international transfers and individuals with valid United States government issued security clearance are not subject to a background check. Processing and procedural variances may apply to students/interns, university recruiting hires, and to employees of companies acquired by Oracle.

9. Access to Security Logs and Reports: Reserved.

10. Audit Rights: Reserved. See *Audit Rights* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

11. Data Center Audit: Reserved. See section 10 (Audit Rights) above.

12. Change Control and Advance Notice: Reserved. See *Oracle Cloud Change Management and Maintenance* section of Oracle Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

13. Security: Reserved.

14. Non-disclosure and Separation of Duties: The Contractor shall enforce separation of job duties and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. Controller of Data: Reserved. See *Controller of Data* section of Data Processing Agreement, which is subject to change from time to time at Oracle's discretion.

16. Service Availability Provisions: Reserved. See *Service Availability Provisions* and *Definition of Unplanned Downtime* sections of Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

17. Affiliates and Subprocessors: Reserved. See *Affiliates and Subprocessors* section of Data Processing Agreement which is subject to change from time to time at Oracle's discretion.

18. Business Continuity and Disaster Recovery: Reserved. See *Oracle Cloud Service Continuity Policy* section of Hosting and Delivery Policies, which is subject to change from time to time at Oracle's discretion.

19. Subscription Terms: Reserved. See section 1 (Data Ownership and Rights Granted) above and section 26 (Title to Product) of Attachment A.

ADDENDUM 1



Data Processing Agreement for Oracle Cloud Services

Version November 3, 2015

1. Scope and order of precedence

This agreement (the "Data Processing Agreement") applies to Oracle's Processing of Personal Data provided to Oracle by Customer as part of Oracle's provision of Cloud Services ("Cloud Services"), as further specified in (i) the applicable Oracle master agreement and (ii) the Oracle Cloud Ordering Document between Customer and Oracle, and all documents, addenda, schedules and exhibits incorporated therein (collectively the "Agreement") by and between the Customer entity and Oracle subsidiary listed in the order for Cloud Services.

This Data Processing Agreement is subject to the terms of the Agreement and is incorporated into the Agreement. Except as expressly stated otherwise, in the event of any conflict between the terms of the Agreement and the terms of this Data Processing Agreement, the relevant terms of this Data Processing Agreement shall take precedence. This Data Processing Agreement shall be effective for the Services Period of any Oracle Cloud order placed under the Agreement.

2. Definitions

"Customer" or "you" means the Customer that has executed the order for Cloud Services.

"Oracle" or "Processor" means the Oracle subsidiary listed in the order for Cloud Services.

"Oracle Affiliates" mean the subsidiaries of Oracle Corporation that may assist in the performance of the Cloud Services.

"Model Clauses" means the standard contractual clauses annexed to the EU Commission Decision 2010/87/EU of 5 February 2010 for the Transfer of Personal Data to Processors established in Third Countries under the Directive (defined below).

"Personal Data" means any information relating to an identified or identifiable natural person that Customer or its end users provide to Oracle as part of the Cloud Services; an identified or identifiable natural person (a "data subject") is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

"Process" or "Processing" means any operation or set of operations which is performed by Oracle as part of the Cloud Services upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Subprocessor" means a third party subcontractor engaged by Oracle which, as part of the subcontractor's role of delivering the Cloud Services, will Process Personal Data of the Customer.

"The Directive" means Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995, as amended, on the protection of individuals with regard to the Processing of Personal Data and on the free movement of such data.

Other terms have the definitions provided for them in the Agreement or as otherwise specified below.



3. Categories of Personal Data and purpose of the Personal Data Processing

In order to execute the Agreement, and in particular to perform the Cloud Services on behalf of Customer, Customer authorizes and requests that Oracle Process the following Personal Data:

Categories of Personal Data: Personal Data may include, among other information, personal contact information such as name, home address, home telephone or mobile number, fax number, email address, and passwords; information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, social security details and business contact details; financial details; and goods and services provided.

Categories of Data Subjects: Data subjects may include Customer's representatives and end users, such as employees, job applicants, contractors, collaborators, partners, and customers of the Customer. Data subjects also may include individuals attempting to communicate or transfer Personal Data to users of the Cloud Services.

Oracle will Process Personal Data solely for the provision of the Cloud Services, and will not otherwise (i) Process or use Personal Data for purposes other than those set forth in the Agreement or as instructed by Customer, or (ii) disclose such Personal Data to third parties other than Oracle Affiliates or Subprocessors for the aforementioned purposes or as required by law.

4. Customer's Instructions

During the Services Period of any order for Cloud Services, Customer may provide instructions to Oracle in addition to those specified in the Agreement with regard to processing of Personal Data. Oracle will comply with all such instructions without additional charge to the extent necessary for Oracle to comply with laws applicable to Oracle as a data processor in the performance of the Cloud Services; the parties will negotiate in good faith with respect to any other change in the Cloud Services and/or fees resulting from such instructions.

5. Controller of Data

The control of Personal Data remains with Customer, and as between Customer and Oracle, Customer will at all times remain the data controller for the purposes of the Cloud Services, the Agreement, and this Data Processing Agreement. Customer is responsible for compliance with its obligations as data controller under data protection laws, in particular for justification of any transmission of Personal Data to Oracle (including providing any required notices and obtaining any required consents), and for its decisions and actions concerning the Processing and use of the data.

6. Rights of Data Subject

Oracle will grant Customer electronic access to Customer's Cloud Services environment that holds Personal Data to permit Customer to delete, release, correct or block access to specific Personal Data or, if that is not practicable and to the extent permitted by applicable law, follow Customer's detailed written instructions to delete, release, correct or block access to Personal Data held in Customer's Cloud Services environment. Customer agrees to pay Oracle's reasonable fees associated with the performance of any such deletion, release, correction or blocking of access to Personal Data. Oracle will pass on to the Customer any requests of an individual data subject to delete, release, correct or block Personal Data Processed under the Agreement.

7. Cross Border and Onward Data Transfer

Oracle treats all Personal Data in a manner consistent with the requirements of the Agreement and this Data Processing Agreement in all locations globally. Oracle's information policies, standards and governance practices are managed on a global basis.



To the extent Personal Data originating from the EEA or Switzerland is transferred to Oracle, Oracle Affiliates or Subprocessors located in countries outside the EEA or Switzerland that have not received a binding adequacy decision by the European Commission pursuant to Articles 25(6) and 31(2) of the Directive or by a competent national data protection authority, such transfers are managed as follows.

Transfers from Customer to Oracle or Oracle Affiliates are made subject to the terms of this Data Processing Agreement and (i) the Model Clauses, with Customer acting as the "data exporter" and Oracle and/or the Oracle Affiliate(s) acting as the "data importer(s)" (as those terms are defined in the Model Clauses); or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the applicable requirements of Articles 25 and 26 of the Directive. The terms of this Data Processing Agreement shall be read in conjunction with the Model Clauses or other appropriate transfer mechanism referred to in the prior sentence.

For transfers from Oracle to Oracle Affiliates, Oracle shall ensure that such transfers are subject to (i) the terms of the Oracle intra-company agreement entered into between Oracle Corporation and the Oracle Affiliates, which requires all transfers of Personal Data to be made in compliance with the Model Clauses and with all applicable Oracle security and data privacy policies and standards; or (ii) other appropriate transfer mechanisms that provide an adequate level of protection in compliance with the applicable requirements of Articles 25 and 26 of the Directive.

For transfers from Oracle or Oracle Affiliates to Subprocessors, Oracle requires the Subprocessor to execute Model Clauses incorporating security and other data privacy requirements consistent with those of this Data Processing Agreement.

8. Affiliates and Subprocessors

Some or all of Oracle's obligations under the Agreement may be performed by Oracle Affiliates. Oracle and the Oracle Affiliates have entered into the intra-company agreement specified above, under which the Oracle Affiliates Processing Personal Data adopt safeguards consistent with those of Oracle. Oracle is responsible for its compliance and the Oracle Affiliates' compliance with this requirement.

Oracle also may engage Subprocessors to assist in the provision of the Cloud Services. Oracle maintains a list of Subprocessors that may Process the Personal Data of Oracle's Cloud Service customers and will provide a copy of that list to Customer upon request.

All Subprocessors are required to abide by substantially the same obligations as Oracle under this Data Processing Agreement as applicable to their performance of the Cloud Services. Customer may request that Oracle audit the Subprocessor or provide confirmation that such an audit has occurred (or, where available, obtain or assist customer in obtaining a third-party audit report concerning Subprocessor's operations) to ensure compliance with such obligations. Customer also will be entitled, upon written request, to receive copies of the relevant terms of Oracle's agreement with Subprocessors that may Process Personal Data, unless the agreement contains confidential information, in which case Oracle may provide a redacted version of the agreement.

Oracle remains responsible at all times for compliance with the terms of the Agreement and this Data Processing Agreement by Oracle Affiliates and Subprocessors.

Customer consents to Oracle's use of Oracle Affiliates and Subprocessors in the performance of the Cloud Services in accordance with the terms of Sections 7 and 8 above.

9. Technical and Organizational Measures

When Processing Personal Data on behalf of Customer in connection with the Cloud Services, Oracle has implemented and will maintain appropriate technical and organizational security measures for the Processing of such data, including the measures specified in this Section to the extent applicable to the



Oracle's Processing of Personal Data. These measures are intended to protect Personal Data against accidental or unauthorized loss, destruction, alteration, disclosure or access, and against all other unlawful forms of processing. Additional information concerning such measures, including the specific security measures and practices for the particular Cloud Services ordered by Customer, may be specified in the Agreement.

9.1 Physical Access Control. Oracle employs measures designed to prevent unauthorized persons from gaining access to data processing systems in which Personal Data is processed, such as the use of security personnel, secured buildings and data center premises.

9.2 System Access Control. The following may, among other controls, be applied depending upon the particular Cloud Services ordered: authentication via passwords and/or two-factor authentication, documented authorization processes, documented change management processes, and logging of access on several levels. For Cloud Services hosted @Oracle: (i) log-ins to Cloud Services Environments by Oracle employees and Subprocessors are logged; (ii) logical access to the data centers is restricted and protected by firewall/VLAN; and (iii) intrusion detection systems, centralized logging and alerting, and firewalls are used.

9.3 Data Access Control. Personal Data is accessible and manageable only by properly authorized staff, direct database query access is restricted, and application access rights are established and enforced. In addition to the access control rules set forth in Sections 9.1 – 9.3 above, Oracle implements an access policy under which Customer controls access to its Cloud Services environment and to Personal Data and other data by its authorized personnel.

9.4 Transmission Control. Except as otherwise specified for the Cloud Services (including within the ordering document or the applicable service specifications), transfers of data outside the Cloud Service environment are encrypted. Some Cloud Services, such as social media services, may be configurable to permit access to sites that require unencrypted communications. The content of communications (including sender and recipient addresses) sent through some email or messaging services may not be encrypted. Customer is solely responsible for the results of its decision to use unencrypted communications or transmissions.

9.5 Input Control. The Personal Data source is under the control of the Customer, and Personal Data integration into the system, is managed by secured file transfer (i.e., via web services or entered into the application) from the Customer. Note that some Cloud Services permit Customers to use unencrypted file transfer protocols. In such cases, Customer is solely responsible for its decision to use such unencrypted field transfer protocols.

9.6 Data Backup. For Cloud Services hosted @Oracle: back-ups are taken on a regular basis; back-ups are secured using a combination of technical and physical controls, depending on the particular Cloud Service.

9.7 Data Segregation. Personal Data from different Oracle customers' environments is logically segregated on Oracle's systems.

10. Audit Rights

Customer may audit Oracle's compliance with the terms of the Agreement and this Data Processing Agreement up to once per year. Customer may perform more frequent audits of the Cloud Service computer systems that Process Personal Data to the extent required by laws applicable to Customer. If a third party is to conduct the audit, the third party must be mutually agreed to by Customer and Oracle and must execute a written confidentiality agreement acceptable to Oracle before conducting the audit.

To request an audit, Customer must submit a detailed audit plan at least two weeks in advance of the proposed audit date to Oracle Corporation's Global Information Security organization ("GIS") describing the proposed scope, duration, and start date of the audit. Oracle will review the audit plan and provide Customer with any concerns or questions (for example, any request for information that could



compromise Oracle security, privacy, employment or other relevant policies). Oracle will work cooperatively with Customer to agree on a final audit plan. If the requested audit scope is addressed in a SSAE 16/ISAE 3402 Type 2, ISO, NIST, PCI DSS, HIPAA or similar audit report performed by a qualified third party auditor within the prior twelve months and Oracle confirms there are no known material changes in the controls audited, Customer agrees to accept those findings in lieu of requesting an audit of the controls covered by the report.

The audit must be conducted during regular business hours at the applicable facility, subject to Oracle policies, and may not unreasonably interfere with Oracle business activities.

Customer will provide GIS any audit reports generated in connection with any audit under this section, unless prohibited by law. Customer may use the audit reports only for the purposes of meeting its regulatory audit requirements and/or confirming compliance with the requirements of the Agreement and this Data Processing Agreement. The audit reports are Confidential Information of the parties under the terms of the Agreement.

Any audits are at the Customer's expense. Any request for Oracle to provide assistance with an audit is considered a separate service if such audit assistance requires the use of resources different from or in addition to those required for the provision of the Cloud Services. Oracle will seek the Customer's written approval and agreement to pay any related fees before performing such audit assistance.

11. Incident Management and Breach Notification

Oracle evaluates and responds to incidents that create suspicion of unauthorized access to or handling of Personal Data ("Incident"). GIS is informed of such Incidents and, depending on the nature of the activity, defines escalation paths and response teams to address those Incidents. GIS will work with Customer, with internal Oracle lines of business, with the appropriate technical teams and, where necessary, with outside law enforcement to respond to the Incident. The goal of the Incident response will be to restore the confidentiality, integrity, and availability of the Cloud Services environment, and to establish root causes and remediation steps.

Oracle operations staff is instructed on responding to Incidents where handling of Personal Data may have been unauthorized, including prompt and reasonable reporting to GIS and to Oracle Corporation's legal department, escalation procedures, and chain of custody practices to secure relevant evidence.

For purposes of this section, "Security Breach" means the misappropriation of Personal Data located on Oracle systems or the Cloud Services environment that compromises the security, confidentiality or integrity of such information. Oracle will inform Customer within 72 hours if Oracle determines that Personal Data has been subject to a Security Breach (including by an Oracle employee) or any other circumstance in which Customer is required to provide a notification under applicable law, unless otherwise required by law.

Oracle will promptly investigate the Security Breach and take reasonable measures to identify its root cause(s) and prevent a recurrence. As information is collected or otherwise becomes available, unless prohibited by law, Oracle will provide Customer with a description of the Security Breach, the type of data that was the subject of the breach, and other information Customer may reasonably request concerning the affected persons. The parties agree to coordinate in good faith on developing the content of any related public statements or any required notices for the affected persons and/or the relevant data protection authorities.

12. Return and Deletion of Personal Data upon End of Cloud Services or at Customer's Request ("Data Portability")

Following termination of the Cloud Services, Oracle will return or otherwise make available for retrieval Customer's Personal Data then available in the Customer's Cloud Services environment. Following

return of the data, or as otherwise specified in the Agreement, Oracle will promptly delete or otherwise render inaccessible all copies of Personal Data from the production Cloud Services environment, except as may be required by law. Oracle's data return and deletion practices are described in more detail in the Agreement.

13. Legally Required Disclosures

Except as otherwise required by law, Oracle will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other governmental authority ("Demand") that it receives and which relates to the Personal Data Oracle is Processing on Customer's behalf. At Customer's request, Oracle will provide Customer with reasonable information in its possession that may be responsive to the Demand and any assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that Oracle has no responsibility to interact directly with the entity making the Demand.

14. Service Analyses

Oracle may (i) compile statistical and other information related to the performance, operation and use of the Cloud Services, and (ii) use data from the Cloud Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as "Service Analyses"). Oracle may make Service Analyses publicly available; however, Service Analyses will not incorporate Customer's Content or Confidential Information in a form that could identify or serve to identify Customer or any data subject, and Service Analyses do not constitute Personal Data. Oracle retains all intellectual property rights in Service Analyses.

ADDENDUM 2

ORACLE CLOUD

Oracle Cloud Hosting and Delivery Policies

DECEMBER 2016

VERSION 2.2



ORACLE®

Table of Contents

1	Oracle Cloud Security Policy	1
1.1	Oracle Information Security Practices - General	1
1.2	User Encryption for External Connections	2
1.3	Physical Security Safeguards	2
1.4	Oracle Software Security Assurance	2
1.5	Customer Security Related Obligations	2
2	Oracle Cloud Service Continuity Policy	3
2.1	Oracle Cloud Services High Availability Strategy	3
2.2	Oracle Cloud Services Backup Strategy	3
3	Oracle Cloud Service Level Objective Policy	3
3.1	Hours of Operation	3
3.2	Service Availability	3
3.2.1	Measurement of Availability	3
3.2.2	Reporting of Availability	4
3.3	Definition of Unplanned Downtime	4
3.4	Monitoring	4
3.4.1	Monitored Components	5
3.4.2	Customer Monitoring & Testing Tools	5
4	Oracle Cloud Change Management Policy	5
4.1	Oracle Cloud Change Management and Maintenance	5
4.1.1	Emergency Maintenance	6
4.1.2	Major Maintenance Changes	6
4.1.3	Data Center Migrations	6
4.2	Software Versioning	6
4.2.1	Software Upgrades and Updates	6
4.2.2	End of Life	6

5	Oracle Cloud Support Policy	7
5.1	Oracle Cloud Support Terms	7
5.1.1	Support fees	7
5.1.2	Support period	7
5.1.3	Technical contacts	7
5.1.4	Oracle Cloud Support	7
5.2	Oracle Cloud Customer Support Systems	7
5.2.1	Cloud Customer Support Portal	7
5.2.2	Live Telephone Support	8
5.3	Severity Definitions	8
5.4	Change to Service Request Severity Level	8
5.4.1	Initial Severity Level	8
5.4.2	Downgrade of Service Request Levels	9
5.4.3	Upgrade of Service Request Levels	9
5.4.4	Adherence to Severity Levels definitions	9
5.5	Service Request Escalation	9
6	Oracle Cloud Suspension and Termination Policy	9
6.1	Termination of Cloud Services	9
6.2	Termination of Pilot Environments	10
6.3	Suspension Due to Violation	10

Overview

These Oracle Cloud Hosting and Delivery Policies (the "Delivery Policies") describe the Oracle Cloud Services ordered by You. These Delivery Policies may reference other Oracle 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. Capitalized terms that are not otherwise defined in this document shall have the meaning ascribed to them in the Oracle agreement, ordering document or policy.

Your ordering document or Oracle's Service Specifications (such as Cloud Service Pillar documentation or Service Descriptions) may include additional details or exceptions related to specific Oracle Cloud Services. The Cloud Service Pillar documentation, the Service Descriptions and the Program Documentation for Oracle Cloud Services are available at <http://www.oracle.com/contracts>.

Oracle Cloud Services are provided under the terms of the Oracle agreement, ordering document, and Service Specifications applicable to such services. Oracle's delivery of the Services is conditioned on Your 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 Cloud Services provided during the Services Period of Your order.

Oracle Cloud Services are deployed at data centers or third-party infrastructure service providers retained by Oracle, with the exception of Oracle Remote Cloud Services. Oracle Remote Cloud Services are Public Cloud Services that are deployed at Your data center or a third-party data center retained by You. Customers may purchase these services standalone or they may be deployed as the underlying platform for other Oracle Cloud Services. For Oracle Remote Cloud Services, Oracle will deliver to Your data center certain hardware components, including gateway equipment, needed by Oracle to operate these services. You are responsible for providing adequate space, power, and cooling to deploy the Oracle hardware including the gateway, and for ensuring adequate network connectivity for Oracle Cloud Operations to access the Services. Oracle is solely responsible for maintenance of the Oracle hardware components including gateway equipment.

These Delivery Policies do not apply to Oracle BigMachines Express, Oracle ETAWorkforce, or such other Oracle Cloud offerings as specified by Oracle in Your ordering document or the applicable Service Description.

1 Oracle Cloud Security Policy

1.1 Oracle Information Security Practices - General

Oracle has adopted security controls and practices for Oracle Cloud Services that are designed to protect the confidentiality, integrity, and availability of customer data that is hosted by Oracle in the Services. Oracle continually works to strengthen and improve those security controls and practices.

Oracle Cloud Services operates under practices which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected.

Oracle Cloud information security practices establish and govern areas of security applicable to Oracle Cloud Services and to Your use of such Services. Oracle personnel (including employees, contractors, and temporary employees) are subject to the Oracle information security practices and any additional policies that govern their employment or the Services they provide to Oracle.



Rather than focusing on individual components, Oracle Cloud takes a holistic approach to information security, implementing a multilayered defense security strategy where network, operating system, database, and software security practices and procedures complement one another with strong internal controls, governance, and oversight.

1.2 User Encryption for External Connections

Your access to Oracle Cloud Services is through a secure communication protocol provided by Oracle. If access is through a TLS enabled connection, that connection is negotiated for at least 128 bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. The list of certified browsers for each version of Cloud Services will be made available via a portal accessible to You or in the corresponding Service Description. In some cases, a third party site that You wish to integrate with the Cloud Service may not accept an encrypted connection. For Cloud Services where HTTP connections with the third party site are permitted by Oracle, Oracle will enable such HTTP connections in addition to the HTTPS connection.

1.3 Physical Security Safeguards

Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and Oracle controlled co-locations/datacenters currently include for example:

- » Physical access requires authorization and is monitored.
- » All employees and visitors must visibly wear official identification while onsite.
- » Visitors must sign a visitor's register and be escorted and/or observed while onsite.
- » Possession of keys/access cards and the ability to access the locations is monitored. Staff leaving Oracle employment must return keys/cards.

Additional physical security safeguards are in place for Oracle controlled Cloud data centers, which currently include safeguards such as:

- » Premises are monitored by CCTV.
- » Entrances are protected by physical barriers designed to prevent unauthorized entry by vehicles.
- » Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management.

This section does not apply to Oracle Remote Cloud Services. You must provide secured computing facilities for the hosting and operation of the Service related hardware, including the gateway hardware required for Oracle to access the Services.

1.4 Oracle Software Security Assurance

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its products and services, including the Oracle Cloud Services. The OSSA program is described at <http://www.oracle.com/us/support/assurance/overview/index.html>.

1.5 Customer Security Related Obligations

You are responsible for:

- » Implementing Your own comprehensive system of security and operational policies, standards and procedures, according to Your risk-based assessments and business requirements.
- » Ensuring that end-user devices meet web browser requirements and minimum network bandwidth requirements for access to the Services.

- » Managing client device security controls, so that antivirus and malware checks are performed on data or files before importing or uploading data into the Services.
- » Maintaining Customer-managed accounts according to Your policies and security best practices.
- » Additionally, for Oracle Remote Cloud Services, You are responsible for providing adequate network security (e.g., intrusion detection systems, access controls, and firewalls) to prevent unauthorized access to your Oracle Cloud Service from your networks.

2 Oracle Cloud Service Continuity Policy

2.1 Oracle Cloud Services High Availability Strategy

Oracle deploys the Oracle Cloud Services on resilient computing infrastructure designed to maintain service availability and continuity in the case of an incident affecting the services. Data centers retained by Oracle to host Oracle Cloud Services have component and power redundancy with backup generators in place, and Oracle may incorporate redundancy in one or more layers including network infrastructure, program servers, database servers, and/or storage.

2.2 Oracle Cloud Services Backup Strategy

Oracle periodically makes backups of Your production data in the Oracle Cloud Services for Oracle's sole use to minimize data loss in the event of an incident. Backups are stored at the primary site used to provide the Oracle Cloud Services, and may also be stored at an alternate location for retention purposes. A backup is typically retained online or offline for a period of at least 60 days after the date that the backup is made. Oracle typically does not update, insert, delete or restore Your data on Your behalf. However, on an exception basis and subject to written approval and additional fees, Oracle may assist You to restore data which You may have lost as a result of Your own actions.

3 Oracle Cloud Service Level Objective Policy

3.1 Hours of Operation

The Cloud Services are designed to be available 24 hours a day, 7 days a week, 365 days a year, except during maintenance periods, technology upgrades and as otherwise set forth in the agreement, the ordering document and this *Oracle Cloud Service Level Objective Policy*.

3.2 Service Availability

Commencing at Oracle's activation of Your production service, Oracle works to meet the Target Service Availability Level, or Target Uptime, of 99.5% in accordance with the terms set forth in the Cloud Service Pillar documentation for the applicable Cloud Service (or such other Target System Availability Level or Target Uptime specified by Oracle for the Cloud Service in such documentation).

The foregoing is contingent on Your adherence to Oracle's recommended minimum technical configuration requirements for accessing and using the Services from Your network infrastructure and Your user work stations as set forth in the Cloud Services Program Documentation.

3.2.1 Measurement of Availability

Following the end of each calendar month of the Services Period, Oracle measures the System Availability Level or System Uptime over the immediately preceding month by dividing the difference between the total number of

minutes in the monthly measurement period and any Unplanned Downtime by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure.

3.2.2 Reporting of Availability

Oracle will provide You with access to a Customer notifications portal. This portal will provide metrics on the System Availability Level for Cloud Services purchased under the ordering document. For those Cloud Services for which such metrics are not available via the Customer notifications portal, Oracle will provide metrics on the System Availability Level upon receipt of a Service Request submitted by You to Oracle requesting the metrics.

3.3 Definition of Unplanned Downtime

“Unplanned Downtime” means any time during which the Services are not Available, but does not include any time during which the Services or any Services component are not Available due to:

- » A failure or degradation of performance or malfunction resulting from scripts, data, applications, equipment, infrastructure, software, performance testing or monitoring agents directed or provided or performed by You;
- » Outages caused by scheduled and announced maintenance, or outages initiated by Oracle at Your request or direction or initiated by You for maintenance, activation of configurations, backups or other purposes that require the Services to be temporarily taken offline;
- » Unavailability of management, auxiliary or administration services, including administration tools, reporting services, utilities, third party software components, or other services supporting core transaction processing, not within the sole control of Oracle;
- » Outages resulting from Your equipment, third party equipment or software components not within the sole control of Oracle;
- » For Oracle Remote Cloud Services, downtime or other unavailability, including due to maintenance, of Your data center;
- » For Oracle Remote Cloud Services, downtime or other unavailability occurring outside the on-site hours defined under Your order for Oracle’s Cloud Operations personnel at Your data center;
- » Events resulting from an interruption or shut down of the Services due to circumstances reasonably believed by Oracle to be a significant threat to the normal operation of the Services, the operating infrastructure, the facility from which the Services are provided, access to, or the integrity of Your Content (e.g., a hacker or malware attack);
- » Outages due to system administration, commands, or file transfers performed by Your users or representatives;
- » Outages due to denial of service attacks, natural disasters, changes resulting from government, political, or other regulatory actions or court orders, strikes or labor disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and Oracle’s other vendors), or other force majeure events or circumstances outside of Oracle’s control;
- » Inability to access the Services or outages caused by Your conduct, including Your negligence or breach of Your contractual obligations;
- » Your lack of availability or unreasonable delay in responding to incidents that require Your participation for source identification and/or resolution, including meeting Your responsibilities for any Services; or
- » Outages caused by failures or fluctuations in electrical, connectivity, network or telecommunications equipment or lines due to Your conduct or circumstances outside of Oracle’s control.

Oracle Cloud Services are “not available” at any time during which a problem with the service prevents Your connectivity to the service as applicable in the corresponding pillar documentation

3.4 Monitoring

Oracle uses a variety of software tools to monitor the availability and performance of the Oracle Cloud production service as applicable and the operation of infrastructure and network components. Oracle does not monitor, or

address deviations experienced by any non-Oracle managed components used by You in the Services, such as non-Oracle applications.

3.4.1 Monitored Components

Oracle monitors the hardware that supports the Oracle Cloud Services, and currently generates alerts for monitored network components, such as CPU, memory, storage, database, and other components. Oracle's Operations staff monitors alerts associated with deviations to Oracle defined thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

3.4.2 Customer Monitoring & Testing Tools

Due to potential adverse impact on service performance, security and availability, You may not, as to any program or feature of, or service component within, the Services, (a) use Your own testing tools (including automated user interfaces and web service calls to any Oracle Cloud Service) or perform network or vulnerability scans or penetration tests to directly or indirectly seek to measure security, or (b) use Your own monitoring tools (including automated user interfaces and web service calls to any Oracle Cloud Service) to directly or indirectly seek to measure availability or performance.

You may not use nor authorize the use of data scraping tools or technologies to collect data available through any Oracle user interface or via web service calls without the express written permission of Oracle. Oracle reserves the right to require Your proposed data scraping tools to be validated and tested by Oracle prior to use in production and to be subsequently validated and tested annually. Oracle may require that a written statement of work be executed to perform such testing and validation work subject to additional fees.

You may not make workload changes beyond the amount permitted under the entitlements provided under Your order.

Oracle reserves the right to remove or disable access to any tools or technologies that violate the restrictions in this section, without any liability to You.

4 Oracle Cloud Change Management Policy

4.1 Oracle Cloud Change Management and Maintenance

Oracle Cloud Operations performs changes to cloud hardware infrastructure, operating software, product software, and supporting application software that is provided by Oracle as part of the Services, to maintain operational stability, availability, security, performance, and currency of the Oracle Cloud. Oracle follows formal change management procedures to review, test, and approve changes prior to application in the production service.

Changes made through change management procedures include system and service maintenance activities, upgrades and updates, and customer specific changes. Oracle Cloud change management procedures are designed to minimize service interruption during the implementation of changes.

Oracle reserves specific maintenance periods for changes that may require the Services to be unavailable during the maintenance period. Oracle works to ensure that change management procedures are conducted during scheduled maintenance windows, while taking into consideration low traffic periods and geographical requirements.

Oracle will provide prior notice of modifications to the standard maintenance period schedule. For Customer-specific changes and upgrades, where feasible, Oracle will coordinate the maintenance periods with You.

For changes that are expected to cause service interruption, Oracle will work to provide prior notice of the anticipated impact. The durations of the maintenance periods for planned maintenance are not included in the



calculation of Unplanned Downtime minutes in the monthly measurement period for System Availability Level (see the *Oracle Cloud Service Level Objective Policy*). Oracle uses commercially reasonable efforts to minimize the use of these reserved maintenance periods and to minimize the duration of maintenance events that cause service interruptions.

4.1.1 Emergency Maintenance

Oracle may be required to execute emergency maintenance in order to protect the security, performance, availability, or stability of the Services. Emergency maintenance may include program patching and/or core system maintenance as required. Oracle works to minimize the use of emergency maintenance, and to the extent reasonable under the circumstances as determined by Oracle, will work to provide 24 hours prior notice for any emergency maintenance requiring a service interruption.

4.1.2 Major Maintenance Changes

To help ensure continuous stability, availability, security and performance of the Cloud Services, Oracle reserves the right to perform major changes to its hardware infrastructure, operating software, applications software and supporting application software under its control, typically no more than twice per calendar year. Each such major change event is considered scheduled maintenance and may cause the Cloud Services to be unavailable. Each such event is targeted to occur at the same time as the scheduled maintenance period. Oracle will work to provide no less than 60 days prior notice of a major change event.

4.1.3 Data Center Migrations

Oracle may migrate Your Services deployed in datacenters retained by Oracle between production data centers in the same data center region as deemed necessary by Oracle or in the case of disaster recovery. For data center migrations for purposes other than disaster recovery, Oracle will provide a minimum of 30 days notice to You.

4.2 Software Versioning

4.2.1 Software Upgrades and Updates

Oracle requires all Cloud Services customers to keep the software versions of the Services current with the software versions that Oracle designates as generally available (GA) for such Services. Software updates or upgrades will follow the release of every GA release and are required for the Services in order to maintain version currency. Oracle's obligations under these Delivery Policies, including the *Cloud Service Continuity Policy*, *Cloud Service Levels Objective Policy*, and the *Cloud Support Policy*, are dependent on You maintaining GA version currency. Oracle is not responsible for performance, functionality, availability or security issues experienced with Services that may result from running earlier versions.

4.2.2 End of Life

Oracle will not support older versions beyond the End of Life Policy described as follows. Oracle will host and support only the designated GA version of a Service. All other versions of the service are considered as "end of life" (EOL). Oracle does not provide Services for EOL versions. You are required to complete the Services upgrade to the latest version before the EOL of a given version. You acknowledge that failure to complete the upgrade prior to the EOL of a Service version may result in an upgrade automatically performed by Oracle or a suspension of the Services. In certain circumstances where a Service version reaches EOL and Oracle does not make available an upgraded version, Oracle may designate, and require You to transition to, a successor cloud service.

5 Oracle Cloud Support Policy

The support described in this *Oracle Cloud Support Policy* applies only for Oracle Cloud Services and is provided by Oracle as part of such Services under Your order. Oracle may make available, and You may order for additional fees, additional support service offerings made available by Oracle for the Services.

5.1 Oracle Cloud Support Terms

5.1.1 Support fees

The fees paid by You for the Oracle Cloud Services under Your order include the support described in this Oracle Cloud Support Policy. Additional fees are applicable for additional Oracle support services offerings purchased by You.

5.1.2 Support period

Oracle Cloud support becomes available upon the service start date and ends upon the expiration or termination of the Services (the "support period"). Oracle is not obligated to provide the support described in this Oracle Cloud Support Policy beyond the end of the support period.

5.1.3 Technical contacts

Your technical contacts are the sole liaisons between You and Oracle for Oracle Cloud support services. Such technical contacts must have, at minimum, initial basic service training and, as needed, supplemental training appropriate for specific role or implementation phase, specialized service/product usage, and migration. Your technical contacts must be knowledgeable about the Services in order to help resolve system issues and to assist Oracle in analyzing and resolving service requests. When submitting a service request, Your technical contact should have a baseline understanding of the problem being encountered and an ability to reproduce the problem in order to assist Oracle in diagnosing and triaging the problem. To avoid interruptions in support services, You must notify Oracle whenever technical contact responsibilities are transferred to another individual.

5.1.4 Oracle Cloud Support

Support Services for Oracle Cloud consists of:

- » Diagnosis of problems or issues with the Oracle Cloud Services.
- » Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that they perform in all material respects as described in the associated Program Documentation.
- » Support during Change Management activities described in the *Oracle Cloud Change Management Policy*.
- » Assistance with technical service requests 24 hours per day, 7 days a week.
- » 24 x 7 access to a Cloud Customer Support Portal designated by Oracle (e.g., My Oracle Support) and Live Telephone Support to log service requests.
- » Access to community forums.
- » Non-technical Customer service assistance during normal Oracle business hours (8:00 to 17:00) local time.

5.2 Oracle Cloud Customer Support Systems

5.2.1 Cloud Customer Support Portal

Oracle provides customer support for the Cloud Service acquired by You through the Cloud Customer Support Portal designated for that Cloud Service. Access to the applicable Cloud Customer Support Portal is governed by the Terms of Use posted on the designated support web site, which are subject to change. A copy of these terms is available upon request. Access to the Cloud Customer Support Portal is limited to Your designated technical



contacts and other authorized users of the Cloud Services. Where applicable, the Oracle Cloud Customer Support Portal provides support details to Your designated technical contacts to enable use of Oracle Cloud support. All service notifications and alerts relevant to Your Cloud Service are posted on this portal.

5.2.2 Live Telephone Support

Your technical contacts may access live telephone support via the phone numbers and contact information found on Oracle's support web site at <http://www.oracle.com/support/contact.html>.

5.3 Severity Definitions

Service requests for Oracle Cloud Services may be submitted by Your designated technical contacts via the Oracle Cloud Customer Support Portal noted above. The severity level of a service request submitted by You is selected by both You and Oracle, and must be based on the following severity definitions:

Severity 1

Your production use of the Oracle Cloud Services is stopped or so severely impacted that You cannot reasonably continue work. You experience a complete loss of service. The impacted operation is mission critical to the business and the situation is an emergency. A Severity 1 service request has one or more of the following characteristics:

- » Data corrupted
- » A critical documented function is not available
- » Service hangs indefinitely, causing unacceptable or indefinite delays for resources or response
- » Service crashes, and crashes repeatedly after restart attempts

Oracle will use reasonable efforts to respond to Severity 1 service requests within fifteen (15) minutes. Oracle will work 24x7 until the Severity 1 service request is resolved, a reasonable work-around is put in place, or as long as useful progress can be made. You must provide Oracle with a technical contact during this 24x7 period to assist with data gathering, testing, and applying fixes. You are required to propose this severity classification with great care, so that valid Severity 1 situations obtain the necessary resource allocation from Oracle.

Severity 2

You experience a severe loss of service. Important features of the Oracle Cloud Services are unavailable with no acceptable workaround; however, operations can continue in a restricted fashion.

Severity 3

You experience a minor loss of service. The impact is an inconvenience, which may require a workaround to restore functionality.

Severity 4

You request information, enhancement, or documentation clarification regarding the Oracle Cloud Services, but there is no impact on the operation of such service. You experience no loss of service.

5.4 Change to Service Request Severity Level

5.4.1 Initial Severity Level

At the time Oracle accepts a service request, Oracle will record an initial severity level of the service request based on the above severity definitions. Oracle's initial focus, upon acceptance of a service request, will be to resolve the issues underlying the service request. The severity level of a service request may be adjusted as described below.

5.4.2 Downgrade of Service Request Levels

If, during the service request process, the issue no longer warrants the severity level currently assigned based on its current impact on the production operation of the applicable Oracle Cloud Service, then the severity level will be downgraded to the severity level that most appropriately reflects its current impact.

5.4.3 Upgrade of Service Request Levels

If, during the service request process, the issue warrants the assignment of a higher severity level than that currently assigned based on the current impact on the production operation of the applicable Oracle Cloud Service, then the severity level will be upgraded to the severity level that most appropriately reflects its current impact.

5.4.4 Adherence to Severity Levels definitions

You shall ensure that the assignment and adjustment of any severity level designation is accurate based on the current impact on the production operation of the applicable Oracle Cloud Service. You acknowledge that Oracle is not responsible for any failure to meet performance standards caused by Your misuse or mis-assignment of severity level designations.

5.5 Service Request Escalation

For service requests that are escalated, the Oracle support analyst will engage the Oracle service request escalation manager who will be responsible for managing the escalation. The Oracle service request escalation manager will work with You to develop an action plan and allocate the appropriate Oracle resources. If the issue underlying the service request continues to remain unresolved, You may contact the Oracle service request escalation manager to review the service request and request that it be escalated to the next level within Oracle as required. To facilitate the resolution of an escalated service request, You are required to provide contacts within Your organization that are at the same level as that within Oracle to which the service request has been escalated.

6 Oracle Cloud Suspension and Termination Policy

6.1 Termination of Cloud Services

After termination or expiration of the Services under Your order, or at Your request, Oracle will delete or otherwise render inaccessible the production Services, including Your Content residing therein, in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the service environment.

For a period of no less than 60 days after the termination or expiration of the Services, Oracle will make available Your production data via secured protocols, or keep the service system accessible, for the purpose of data retrieval by You. During this period, the service system should not be used for production activities. Oracle has no obligation to retain Your Content after this 60 day period.

If You need assistance from Oracle to obtain access to or copies of Your Content, You must create a service request in the Cloud Customer Support Portal applicable to the service (e.g., My Oracle Support).

Data retrieval and any related assistance by Oracle is not applicable for Services that do not store Your Content. You are responsible for ensuring that if those Services are dependent on separate Cloud Services, such as Storage Cloud Service or Database Cloud Services, for the storage of data, those separate Cloud Services must have a valid duration through the end of the terminating Service to enable data retrieval.



For Oracle Remote Cloud Services, You must make available for retrieval by Oracle any Service related hardware components, including the gateway, provided by Oracle in good working order and the same condition as at the start of the Services subject to reasonable wear and tear for appropriate use.

6.2 Termination of Pilot Environments

This *Oracle Cloud Suspension and Termination Policy* applies to production pilots of Oracle Cloud Services. Production pilots are not available for all Oracle Cloud Services.

6.3 Suspension Due to Violation

If Oracle detects a violation of, or is contacted about a violation of, Services related terms and conditions or acceptable use policy, Oracle will assign an investigating agent. The investigating agent may take actions including but not limited to suspension of user accounts, suspension of administrator accounts, or suspension of access to the Services until the issues are resolved.



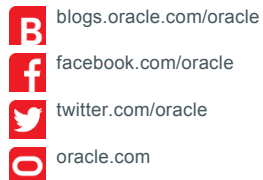
Oracle Corporation, World Headquarters

500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries

Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US



Integrated Cloud Applications & Platform Services

Copyright © 2016, Oracle and/or its affiliates. All rights reserved.



Oracle is committed to developing practices and products that help protect the environment.

Attachment B

Oracle Cloud Services – Overview

Oracle Cloud is the industry's broadest and most integrated public cloud. It offers best-in-class services across software as a service ("SaaS"), platform as a service ("PaaS"), and infrastructure as a service ("IaaS"), and even lets you put Oracle Cloud in your own data center. Oracle Cloud helps organizations drive innovation and business transformation by increasing business agility, lowering costs, and reducing IT complexity. More detailed information is available at <http://cloud.oracle.com> and <http://oracle.com/cloud>.

Oracle's SaaS offerings under the Master Agreement include Oracle's RightNow, Taleo Cloud, Primavera Cloud, Social Relationship Management, Fusion Cloud, Financial Services Cloud and related services.

Oracle's PaaS and IaaS offerings under the Master Agreement include Oracle's current non-metered PAAS and IAAS Cloud and related services.

Oracle may offer under the Master Agreement additional SaaS, PaaS, and IaaS solutions that are generally available and offered to Oracle customers in the normal course of business.

Attachment C – Cost Schedule

Cloud Solutions By Category. Specify **Discount Percent %** Offered for products in each category. Highest discount will apply for products referenced in detail listings for multiple categories. Provide a detailed product offering for each category.¹

Software as a Service **Discount %** **9.77**

Infrastructure as a Service **Discount %** **9.77**

Platform as a Services **Discount %** **9.77**

Value Added Services **Discount %** **N/A**

Note – These discount apply to net new cloud services.

Additional Value Added Services:

Maintenance Services

Onsite Hourly Rate \$	<u>N/A</u>
Remote Hourly Rate \$	<u>N/A</u>

Professional Services

☐	Deployment Services	Onsite Hourly Rate \$	<u>N/A</u>
		Remote Hourly Rate \$	<u>N/A</u>

☐	Consulting/Advisory Services	Onsite Hourly Rate \$	<u>N/A</u>
		Remote Hourly Rate \$	<u>N/A</u>

☐	Architectural Design Services	Onsite Hourly Rate \$	<u>N/A</u>
		Remote Hourly Rate \$	<u>N/A</u>

☐	Statement of Work Services	Onsite Hourly Rate \$	<u>N/A</u>
		Remote Hourly Rate \$	<u>N/A</u>

Partner Services	Onsite Hourly Rate \$	<u>N/A</u>
	Remote Hourly Rate \$	<u>N/A</u>

Training Deployment Services	Onsite Hourly Rate \$	<u>N/A</u>
	Online Hourly Rate \$	<u>N/A</u>

¹ Oracle's SaaS offerings under the Master Agreement include Oracle's RightNow, Taleo Cloud, Primavera Cloud, Social Relationship Management, Fusion Cloud, Financial Services Cloud, and related services. Oracle's PaaS and IaaS offerings under the Master Agreement include Oracle's current non-metered PaaS and IaaS Cloud and related services. Oracle may offer under the Master Agreement additional SaaS, PaaS, and IaaS solutions that are generally available and offered to Oracle customers in the normal course of business.

Attachment D

Oracle America, Inc. Response to

The State of Utah

for a

**ValuePoint Master Agreement
for Cloud Solutions**

Utah Solicitation Number CH16012

TECHNICAL PROPOSAL

March 10, 2016





Oracle America, Inc.

1910 Oracle Way
Reston, VA 20190Phone: 703.478.9000
Fax: 703.318.6340

March 10, 2016

Mr. Christopher Hughes
State of Utah Division of Purchasing
3150 State Office Building, Capitol Hill
Salt Lake City, Utah 84114-1061

Dear Mr. Hughes:

Thank you for the opportunity to respond to the State of Utah (the State) Request for Proposal (RFP), Solicitation Number CH16012, NASPO ValuePoint Master Agreement for Cloud Solutions.

My position and signature below meet your requirements that an authorized signatory with the ability to bind the vendor sign the response to the RFP.

The following paragraphs respond to the mandatory requirements for this cover letter as defined in Section 5.2.1 through 5.2.6 of the Request for Proposal:

1. By submitting this offer, Oracle understands and acknowledges that it may be required to negotiate additional terms and conditions including additional administrative fees with Participating Entities when executing Participating Addendums. It is further assumed that a final Master Agreement will be based on a set of mutually agreed upon specifications, terms and conditions based on the Oracle response as negotiated by the State of Utah and Oracle.
2. The following Oracle America, Inc. staff members were responsible for writing the proposal:
 - Sales Lead: Glenda Sakati, Director, Government Resell Programs. Glenda will be Oracle's primary point of contact for this response. Please contact her at 703.795.2189, or via e-mail at glenda.sakati@oracle.com.
 - Contracts Lead: Helen Velardi, RFx Deal Manager
 - Software as a Service (SaaS) Subject Matter Expert: Beth Veatch, Senior Sales Consultant
 - Platform as a Service (PaaS) Subject Matter Expert: Brian Keehn, Principal Cloud Sales Engineer
3. To the best of my knowledge and belief as of the date of this submission, Oracle is not presently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.
4. Oracle acknowledges that a 0.25% NASPO ValuePoint Administrative Fee will apply to total sales for the Master Agreement(s) awarded from the RFP. In addition, we acknowledge that there may be Participating Entity Administrative fee that apply if negotiated in a Participating Addendum.
5. The service models covered in Oracle's response include SaaS and PaaS with responses based on two primary focus subcategories for evaluation purposes.



6. Oracle is capable of storing and securing data in the Moderate Risk Data category defined in Attachments D and H of the RFP. With regard to data risk categories, Oracle refers the Lead State to the applicable Cloud Security Policy in the applicable cloud hosting and delivery policy provided in Section 9 of this response.

Oracle is proud of its dynamic cloud services and looks forward to your favorable evaluation of this response to provide cloud services to the NASPO ValuePoint members.

Sincerely,


Mark C. Johnson (Mar 9, 2016)

Mark C. Johnson
Senior Vice President, Public Sector Software

Response Guidelines

Corporate Entity

This Response is being made by Oracle America, Inc., a wholly owned subsidiary of Oracle Corporation. All responses reflect information concerning Oracle Corporation (hereinafter referred to as Oracle) except where otherwise indicated as being information of Oracle America, Inc. (hereinafter Oracle America, Inc.).

Definitions

Throughout this Response, the term *solution* refers to and is interchangeable with approach or system. Solution is not intended to commit Oracle to solving problems, but is meant to express that Oracle's approach to cloud services has been well thought out and is the result of the use of Oracle's products, methods, and experience.

Throughout this Response, the term partner refers to an ally or collaborator. Partner is not intended to bind Oracle to any third party.

Oracle's Response Terms

GENERAL TERMS AND CONDITIONS OF ORACLE'S PROPOSAL

Oracle America, Inc. ("Oracle") is in receipt of Solicitation CH16012 (RFP) dated December 21, 2015 (the "Request") issued by the State of Utah, Division of Purchasing ("State") for NASPO ValuePoint Cloud Solutions. Oracle is pleased to have the opportunity to submit this proposal in response to the Request (the "Response"). The general terms applicable to the Response are as follows:

1. The Response is based upon information that the State has provided to Oracle and is intended for the State's evaluation purposes. In accordance with the answer to question number 476 of the Q&A process, Oracle does not plan to incorporate the Request or the Response into the contract that may result. However, Oracle looks forward to negotiating a mutually acceptable agreement with the Lead State and, in accordance with the answer to question number 506, is considering attaching the Response as an information exhibit to the final agreement for historical information purposes only. Except as provided in the proposal signature page, the Response does not provide any representations or warranties on behalf of Oracle prior to contract signing and Oracle does not intend to create or imply warranties of fitness for a particular purpose, merchantability, performance, product, or product/platform or service availability, or any other representation or warranty. The Response is not intended to be a legally binding contract with Oracle. In the event of any inconsistencies between the text in the Response and this document, the text of this document best describes Oracle's position and shall take precedence.
2. Oracle has, as part of the Response, submitted the Exception Form as permitted by the Request. The comments, responses and provisions provided in the "Alternate Language References" column of the Exceptions Form are for informational and discussion purposes with a view toward negotiating a mutually agreed upon Master Agreement. All terms and conditions, including, without limitation, the exceptions provided in the Exceptions Form, are contingent on the finalization of a mutually acceptable Master Agreement. Additionally, Oracle expects that any inapplicable definitions and related provisions will not be included in any final Master Agreement.
3. The Response is valid until 90 days from the Due Date of March 10, 2016, unless otherwise mutually agreed, in writing, by the parties.
4. Except as otherwise may be negotiated and mutually agreed by the parties based on the Exceptions Form, the services described in the Response are subject to the attached Cloud Services Agreement (which includes the Data Processing Agreement and other referenced documentation), as well as one or more ordering documents (template available upon request) which incorporate the applicable cloud hosting and delivery policies, among other references ("Cloud Terms").
5. If you elect to award a contract to Oracle for the services specified in the Response, the parties will endeavor to execute the contract within thirty (30) days after notification of award, or within such other reasonable time period as may be agreed to by the parties. The negotiated contract shall consist of mutually acceptable provisions of the NASPO ValuePoint Master Agreement Terms and Conditions and the Cloud Terms, as may be further amended by the parties following notification of award to Oracle (the "Master Agreement"). Upon agreement on a Participating Addendum with a Participating State or Entity, orders would be placed using the Oracle ordering documents (sample available upon request), which specify the products or services acquired and the fees due Oracle for such acquired products or services (the "ordering document(s)"). All fees payable to Oracle are due within 30 days from the invoice date.
6. The information contained in this Response marked "confidential," redacted from the redacted copy of the technical proposal, and identified in the Business Confidentiality Claim document, is considered by Oracle to be proprietary and confidential to Oracle. The information contained in this Response may be used solely in connection with the evaluation of the Response. To the extent that a claim is made under applicable law to disclose confidential information contained in this Response, Oracle reserves the right to defend its confidential information against such claim. Subject to applicable law, the State agrees (a) to keep the information contained in this Response in strict confidence and not to disclose it to any third party without Oracle's prior written consent and (b) the State's internal disclosure of the information contained in this Response shall be only to those employees, contractors or agents having a need to know such information in connection with the evaluation of the Response and only insofar as such persons are bound by a nondisclosure agreement consistent with the foregoing. The State does not acquire any intellectual property rights in Oracle's property under the Response and the State agrees to comply with all applicable export control laws and regulations to ensure that no confidential information is used or exported in violation of

Oracle General Terms State of UT NASPO.03102016.hv

ORACLE

**THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS**

RFP #: CH16012

such laws and regulations. The State may make a reasonable number of copies of this Response for the State's internal distribution for use solely in connection with the evaluation of the Response; otherwise, subject to applicable law, the State may not reproduce or transmit any part of this Response in any form or by any means without the express written consent of Oracle. By reading the Response, the State has agreed to be bound by the foregoing terms.

Oracle General Terms State of UT NASPO.03102016.hv

ORACLE®

**THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS**

RFP #: CH16012

ORACLE®

USE OR DISCLOSURE OF DATA CONTAINED ON THIS SHEET IS SUBJECT TO THE RESTRICTIONS IN THE LAST PARAGRAPH OF THE GENERAL
TERMS AND CONDITIONS OF ORACLE'S PROPOSAL INCLUDED IN THIS RESPONSE.

Table of Contents

Response Guidelines i

1. RFP Signature Page..... 1

2. Executive Summary 3

3. Mandatory Minimums..... 4

 Cover Letter (RFP #5.2) 4

 Acknowledgement of Amendments (RFP #5.3) 5

 General Requirements (RFP #5.5) 5

 Recertification of Mandatory Minimums and Technical Specifications (RFP #5.7)..... 7

4. Business Profile (RFP #5)..... 8

 Business Profile (RFP #6.1)..... 8

 Scope of Experience (RFP #6.2)..... 9

 Financials (RFP #6.3) 15

 General Information (RFP #6.4) 15

 Billing and Pricing Practices (RFP #6.5)..... 16

 Scope and Variety of Cloud Solutions (RFP #6.6) 17

 Best Practices (RFP #6.7) 19

5. Organization Profile 22

 Organization and Staffing (RFP #7) 22

 Contract Manager (RFP #7.1)..... 22

6. Technical Response..... 24

 6A. Description of Proposed Solutions..... 24

The Oracle SaaS Solutions – The Oracle Service Cloud Platform..... 24

 6B. Technical Requirements Compliance (RFP #8)..... 42

Technical Requirements (RFP #8.1)..... 42

Subcontractors (RFP #8.2)..... 52

Working with Purchasing Entities (RFP #8.3) 54

Customer Service (RFP #8.4) 58

Security of Information (RFP #8.5) 60

Privacy and Security (RFP #8.6) 64

Migration and Redeployment Plan (RFP #8.7) 75

Service or Data Recovery (RFP #8.8) 76

Data Protection (RFP #8.9)..... 80

Service Level Agreements (RFP #8.10) 81

Data Disposal (RFP #8.11) 81

Performance Measures and Reporting (RFP #8.12) 81

Cloud Security Alliance (RFP #8.13) 84

Service Provisioning (RFP #8.14) 84

Back Up and Disaster Plan (RFP #8.15)..... 85

Solution Administration (RFP #8.16) 86

Hosting and Provisioning (RFP #8.17) 90

Trial and Testing Periods (Pre- and Post-Purchase) (RFP #8.18) 93

Integration and Customization (RFP #8.19)..... 97

Marketing Plan (RFP #8.20) 99

Related Value-Added Services to Cloud Solutions (RFP #8.21) 100
Supporting Infrastructure (RFP #8.22) 100
Alignment of Cloud Computing Reference Architecture (RFP #8.23)..... 101
7. Confidential, Protected or Proprietary Information 102
Attachment 3 – The Consensus Assessments Initiative Questionnaire (CAIQ) (RFP Exhibit B.1) 105
Attachment 4 – Compliance with Cloud Controls Matrix (CCM) (RFP Exhibit B.2) 106
Attachment 10. Résumé of Oracle’s Proposed Contracts Manager 107
8. Exceptions and/or Additions to the Standard Terms and Conditions 108
9. Attachments..... 109
1. Acknowledgement of Amendments (RFP #5.3)..... 110
2. Identification of Service Models (RFP Attachment H) 111
3. The Consensus Assessments Initiative Questionnaire (CAIQ) (RFP Exhibit B.1)..... 112
4. Compliance with Cloud Controls Matrix (CCM) (RFP Exhibit B.2) 112
5. Oracle Annual Report FYE May 31, 2015 113
6. Oracle Annual Report FYE May 31, 2014 113
7. Oracle Cloud SLAs 114
 7.1. *Hosting and Delivery Policies for PaaS..... 114*
 7.2. *Hosting and Delivery Policies for SaaS..... 114*
 7.3. *Data Processing Agreement for Oracle Cloud Services..... 114*
 7.4. *Oracle Cloud Services Agreement..... 114*
8. Oracle Exceptions and/or Additions to Standard Terms and Conditions 115
9. Oracle’s Services Privacy Policy 116
10. Résumé of Oracle’s Proposed Contracts Manager 117

List of Figures

Figure 1: Oracle Cloud Solution for Recycling and Economic Development Initiative of South Africa... 10

Figure 2: Oracle Cloud Solution for the U.S. Air Force 11

Figure 3: Oracle Cloud Solution for HM Land Registry, United Kingdom 11

Figure 4: Oracle Cloud Solution for the City of Cartagena, Spain 12

Figure 5: Oracle Cloud Solution for the Boston Globe..... 12

Figure 6: Oracle Cloud Solution for Walmart 13

Figure 7: Oracle Cloud Solution for Orbitz 13

Figure 8: Oracle Cloud Solution for Cox Communications..... 14

Figure 9: Oracle Cloud Solution for Kohl’s Department Stores..... 14

Figure 10: Proposed Oracle Cloud Service Models..... 18

Figure 11: Oracle Cloud Deployment Models 19

Figure 12: The Oracle Service Cloud Platform 25

Figure 13: Oracle’s Solution: Flexible and Performance Proven Application Platform..... 26

Figure 14: Oracle Partners Enhance the Oracle Cloud Solution..... 28

Figure 15: Oracle’s Industry-leading Security Compliance..... 29

Figure 16: Superior Control of the Oracle Cloud Environment..... 29

Figure 17: Oracle’s Solution: Global Scale Platform 30

Figure 18: Statistics-based Customer Data 31

Figure 19: Database as a Service Monitoring Tool..... 38

Figure 20: Database Schema Service Cloud Portal and APEX 40

Figure 21: Overview of Oracle Cloud Solution..... 44

Figure 22: Database as a Service Monitoring Tool..... 49

Figure 23: Database Schema Service Cloud Portal and APEX 51

Figure 24: Sample Project Timeline 57

Figure 25: Oracle’s Solution: Audit Log Example 69

Figure 26: Oracle Service Cloud Overall Architecture..... 72

Figure 27: Oracle Service Cloud Product Architecture 72

Figure 28: Workflows: Drag and Drop Simplicity 88

Figure 29: Sample OPA functionality within Oracle’s Solution 90

Figure 30: Oracle Cloud Free Trial Offer 93

Figure 31: Oracle Provides Comprehensive Cloud Support At All Levels 97

Figure 32: The Oracle Service Cloud Footprint..... 99

1. RFP Signature Page

The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.

5.1 (M) SIGNATURE PAGE

Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an ORIGINAL HANDWRITTEN signature executed in INK OR AN ELECTRONIC SIGNATURE, and be returned with the Offeror's proposal.

Oracle Response:

The Oracle Vendor Information form is on the following page.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012



State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable) Oracle America, Inc.		Federal Tax Identification Number 94-2805249		State of Utah Sales Tax ID Number 12265566-002-STC	
Ordering Address 1910 Oracle Way, Reston, VA 20190		City Reston	State VA	Zip Code 20190	
Remittance Address (if different from ordering address)		City	State	Zip Code	
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation		Company Contact Person Glenda Sakati			
Telephone Number (include area code) 703.478.9000		Fax Number (include area code) 703.318.6340			
Company's Internet Web Address www.oracle.com		Email Address glenda.sakati@oracle.com			
Offeror's Authorized Representative's Signature  (Mark C. Johnson, April 9, 2016)					
Type or Print Name Mark C. Johnson					
Position or Title of Authorized Representative Senior Vice President, Public Sector Software					
Date: March 10, 2016					

ORACLE

2. Executive Summary

5.4 (M) EXECUTIVE SUMMARY

Offerors must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.

Oracle Response:

Oracle's business philosophy is based on a close working relationship with our customers to offer solutions that keep pace with changing technology. As a world leader innovating technology this philosophy is the forefront of the Oracle Cloud story. Oracle's cloud services provide options to customers by creating a path from the traditional investments in enterprise information technology perpetual licenses and hardware to a subscription services for same enterprise solutions in the cloud. Another benefit to Oracle cloud service is the portability between the traditional on premise model to cloud then back again as needed. A move to the cloud requires the agility to integrate easily with legacy applications, future applications, and other third-party technologies all which were accounted for in the development of Oracle cloud services. Once in the cloud Oracle's solution offers configuration throughout the system to adapt to changing business needs with configuration without the use of code for ongoing enterprise management. Oracle offers private cloud, public cloud and hybrid cloud solutions to meet modern technology needs.

Oracle understands that a shift to the cloud or any enterprise technology shift can be disruptive and each customer has their unique requirements which is where the Oracle Account team can assist. The Oracle Account team will engage with customers to understand their varying needs and use cases for the cloud environment. The Oracle Account team will work alongside the customer to explore the wide range of options and provide demonstrations, no cost trial environments, and when possible connections to reference clients who has a similar needs that are deployed in one of the Oracle cloud services. The Response where possible provides examples of how a specific cloud platform or product work in conjunction with one another but there is no one solution or specific approach to meeting the modernization goals across the enterprise in the cloud. Oracle has the breadth, depth, and cloud experience to meet the cloud computing needs while working with the customer's current investment in enterprise technology. In summary, due to the breadth and depth of Oracle's Cloud offerings it is impossible to provide a specific PaaS and/or SaaS solution that is collectively right for all customers but our team of trained professionals can provide information to allow for informed decision.

Oracle's cloud solutions offer choice and flexibility with the most comprehensive, modern, and portfolio of cloud services which use the same technology for all of its cloud solutions providing the same standards and the same product no matter what type of deployment is chosen. As part of our Response we have included a comprehensive list of Additions and Exceptions to the RFP to align with the cloud services that we offer.

3. Mandatory Minimums

Provided below is the information requested in section 5 of the Request for Proposal.

This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses to each mandatory minimum requirement. If a mandatory minimum requirement is not applicable to an Offeror's Solution then the Offeror must explain why the mandatory minimum requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

Cover Letter (RFP #5.2)

Provided below is the information requested in section 5.2 of the Request for Proposal.

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

- 5.2.1 A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.**
- 5.2.2 A statement naming the firms and/or staff responsible for writing the proposal.**
- 5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.**
- 5.2.4 A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.**
- 5.2.5 A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.**

5.2.6 A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

Oracle Response:

The Oracle cover letter is presented on the third page of this response. It is signed by Mark C. Johnson, Senior Vice President, Public Sector Software.

Acknowledgement of Amendments (RFP #5.3)

Provided below is the information requested in section 5.3 of the Request for Proposal.

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

Oracle Response:

Oracle's signed acknowledgement form is presented in Attachment 1.

General Requirements (RFP #5.5)

Provided below is the information requested in section 5.5 of the Request for Proposal

5.5.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

Oracle Response:

Oracle agrees and acknowledges that if it is awarded a Master Agreement that it will provide a Usage Report Administrator in the form of a Contracts Manager as described in Section 5 in response to RFP section 7.1.1 who is responsible for quarterly sales reporting as described in the Master Agreement Terms and Conditions and if applicable for any Participating Addendums. Oracle has successfully completed such reporting for various Federal Government, State IT Schedules, and WSCA/NASPO agreements.

5.5.2 Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

Oracle Response:

Oracle confirms and acknowledges that it will cooperate with SciQuest or any successor thereto to upload ordering instructions if awarded a Master Agreement.

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment . *[Footnote: CSA STAR Self-Assessment documents the security controls provided by an Offeror's offerings, thereby helping Purchasing Entities assess the security of an Offeror, if awarded a Master Agreement, they currently use or are considering*

using. / Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

Oracle Response:

Oracle's response to the Consensus Assessments Initiative Questionnaire (CAIQ) from RFP is presented in Section 7 of this response.

Please note that the relevant contract(s) between you and Oracle will determine the scope of services provided and the related legal terms. While we have tried to be as complete as possible, Oracle's response to your question(s) is provided on an AS-IS basis without warranty or obligation to update, is subject to change, and is confidential information under the Claim of Business Confidentiality Form submitted by Oracle in this response and Oracle's General Terms.

Please note that any Yes/No responses and any computed "In Place" indicators, must be read in the context of the supplied comments and qualifications, and, given the diversity and complexity of the services, will not be absolute or applicable in all instances. Oracle has attempted to address the requirements in light of the Lead State's responses to questions 468 and 484 through 488 from the Q&A process. Please note that the explanation and/or supporting documentation may comprise Oracles response and control regardless of the scoring or any Yes/No response. The responses provided in this document apply solely to the services specifically listed and other products or services may have different controls.

5.5.4 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement , which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements. *[Footnote: SLAs can vary depending on the cloud service being procured as well as the individual ordering activity, and the Lead State does not expect to require a single SLA to all cloud solutions being proposed under the RFP. Additionally, by submitting a sample the Lead State does not agree to its terms and you understand that a Purchasing Entity may revise the SLA to conform to the requirements of its laws.]*

Oracle Response:

Oracle's Cloud Service Level Agreements (SLAs) are comprised of multiple parts depending of the cloud services ordered. The documents contained in Attachment 7 are hereafter referred to as Oracle's SLA's and include the Oracle Cloud Enterprise Hosting and Delivery Policies, the Oracle (non-enterprise) Cloud Hosting and Delivery Policies, the Data Processing Agreement, and the Cloud Services Agreement. These documents are living documents updated to provide the most current service levels to customers and can be found at <http://www.oracle.com/us/corporate/contracts/cloud-services/index.html>.

Recertification of Mandatory Minimums and Technical Specifications (RFP #5.7)

Provided below is the information requested in section 5.7 of the Request for Proposal.

Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal

Oracle Response:

Oracle acknowledges that if awarded a contract pursuant to this RFP that annually it will certify to the technical capability discussed in its proposal or thereafter amended into the Master Agreement.

4. Business Profile (RFP #5)

Provided below is the information requested in section 6 of the RFP.

This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.

Business Profile (RFP #6.1)

Provided below is the information requested in section 6.1 of the RFP.

BUSINESS INFORMATION

Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.

Oracle Response:

Oracle America, Inc. is a wholly owned subsidiary of Oracle Corporation (Oracle). Founded in June 1977, Oracle provides products and services that address all aspects of corporate information technology (IT) environments. Since 2004, Oracle has invested more than \$39 billion in research and development. Products offered include database and middleware software, application software, cloud infrastructure software and hardware systems along with support and related services.

Oracle is a leader in the core technologies of cloud IT environments, including database and middleware software as well as enterprise applications, virtualization, clustering, large-scale systems management and related infrastructure. Oracle offers a wide range of services in all primary layers of the cloud. Oracle Cloud offerings are designed to be rapidly deployable to enable customers shorter time to innovation; easily maintainable to reduce integration and testing work; and cost-effective by requiring lower upfront customer investment.

With more than 400,000 customers including 100 of the Fortune 100 in more than 145 countries, Oracle provides a complete technology stack both in the cloud and in the data center. Oracle's industry-leading cloud-based and on premises solutions give customers complete deployment flexibility and unmatched benefits including application integration, advanced security, high availability, scalability, energy efficiency, powerful performance, and low total cost of ownership.

Oracle has over 132,000 employees worldwide, all of whom are dedicated to providing a complete business offering that includes integrated, award-winning support services combined with industry-leading products. Oracle does not report statistics on employee retention. For more information, visit oracle.com.

Oracle Cloud was announced in 2012, and since then Oracle has delivered cloud services and other services under numerous, large-scale government projects at the Federal and State level, including for the US Department of Defense (DoD), the State of Texas. Under NASPO ValuePoint (formerly WSCA-NASPO) agreements, Oracle has also provided products and services to the States of Illinois, Washington, Utah, New Mexico, and Minnesota.

Scope of Experience (RFP #6.2)

Provided below is the information requested in section 6.2 of the RFP.

Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred

Oracle Response:

CLOUD SOLUTIONS FOR THE U.S. DEPARTMENT OF DEFENSE

Oracle DoD Community Cloud

The Oracle DoD Community Cloud provides a U.S. Department of Defense-only community to use Oracle SaaS solutions. Available to the U.S. Air Force, U.S. Army, U.S. Navy, U.S. Marine Corp., U.S. Coast Guard, U.S. Department of Defense Agencies, and NAF Agencies that support the U.S. Department of Defense.

Oracle Service Cloud for DoD

The Oracle Service Cloud is Oracle's premier Software as a Service (SaaS) solution providing the industry's best-in-class customer service platform for U.S. DoD customers. Oracle Service Cloud is deployed onto a robust, secure infrastructure hosting Oracle's patented Service Cloud software applications in an environment accredited to FedRAMP+ DoD Level 4 specifications. The Oracle Service Cloud leverages a fault-tolerant core application framework offering flexible add-on modules providing customers with a customizable, out-of-the-box feature set to support both customer-facing and customer service agent-facing functions. The Oracle Service Cloud is offered as a hosted cloud solution (that is, operated and maintained by Oracle within its secure hosting environment at co-location facilities in the United States) providing customers with a modern, efficient, and secure cloud solution via proven Software as a Service (SaaS) delivery model. Additional information is available at <https://cloud.oracle.com/dod>.

CLOUD SOLUTIONS FOR THE STATE GOVERNMENTS

Texas Department of Information Resources (DIR)

Location: Austin, Texas

Industry: Public sector

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

Employees: 180

Budget: US\$240,735,442 in 2012

Oracle products: Oracle Exadata Database Machine; Oracle Database, Enterprise Edition; Oracle Enterprise Manager; Oracle Active Data Guard; Oracle Real Application Clusters; Oracle Cloud Management Pack for Oracle Database; PeopleSoft Financials; PeopleSoft Human Resources; PeopleSoft Payroll

Twenty-eight agencies have signed up to use Texas DIR’s Oracle Exadata–based cloud services, including the Texas Education Agency, Texas Health and Human Services Commission, the Texas Department of Assistive and Rehabilitative Services, the Texas Department of Family Protective Services, the Texas Department of Insurance, and the Texas Department of Public Safety.

Leaders at Texas DIR decided to use the cloud technologies within the Oracle Exadata and Oracle Exalogic lines to provision a shared “PeopleSoft-as-a-service” environment that the agencies can consume in a simple, straightforward way.

“Our cloud services are agile and priced very attractively. They are also flexible. We have been careful not to lock customers into a rigid cloud model. Customers pay one price. They don’t have to think about standby databases and disaster recovery; that’s all built in.”

- Todd Kimbriel, director, eGovernment, Texas Department of Information Resources (DIR).

OTHER RELATED CLOUD SOLUTIONS

The following figures present an overview of selected government or large organization cloud solutions similar to those proposed for the NASPO master agreement.



FIGURE 1: ORACLE CLOUD SOLUTION FOR RECYCLING AND ECONOMIC DEVELOPMENT INITIATIVE OF SOUTH AFRICA

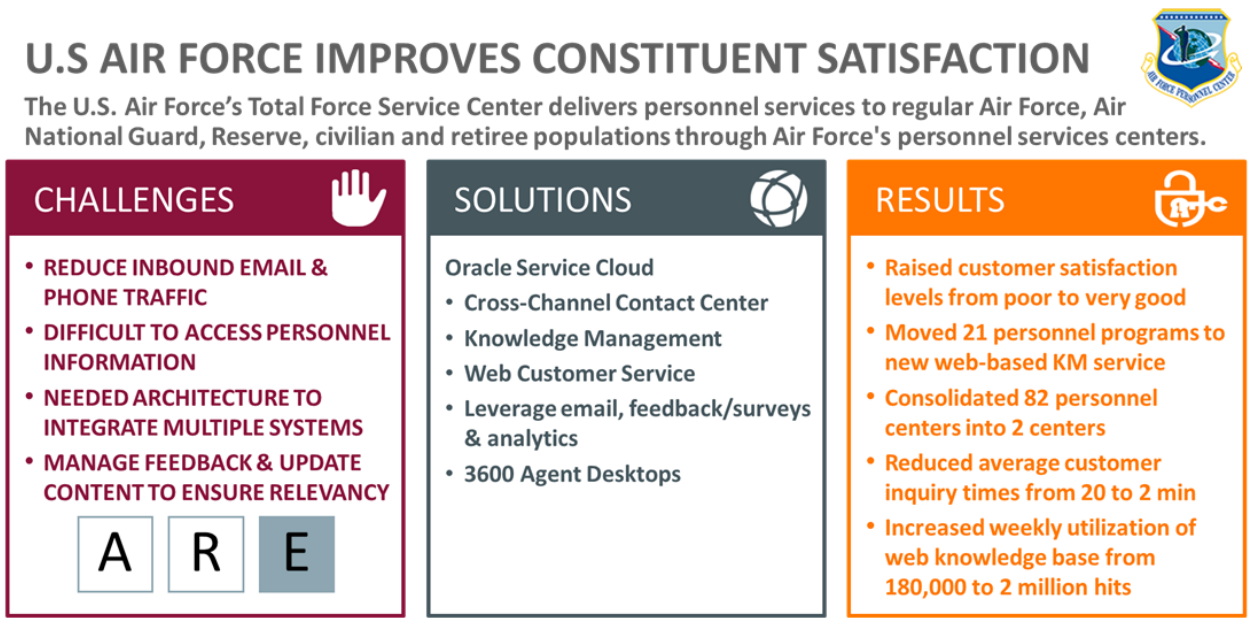


FIGURE 2: ORACLE CLOUD SOLUTION FOR THE U.S. AIR FORCE

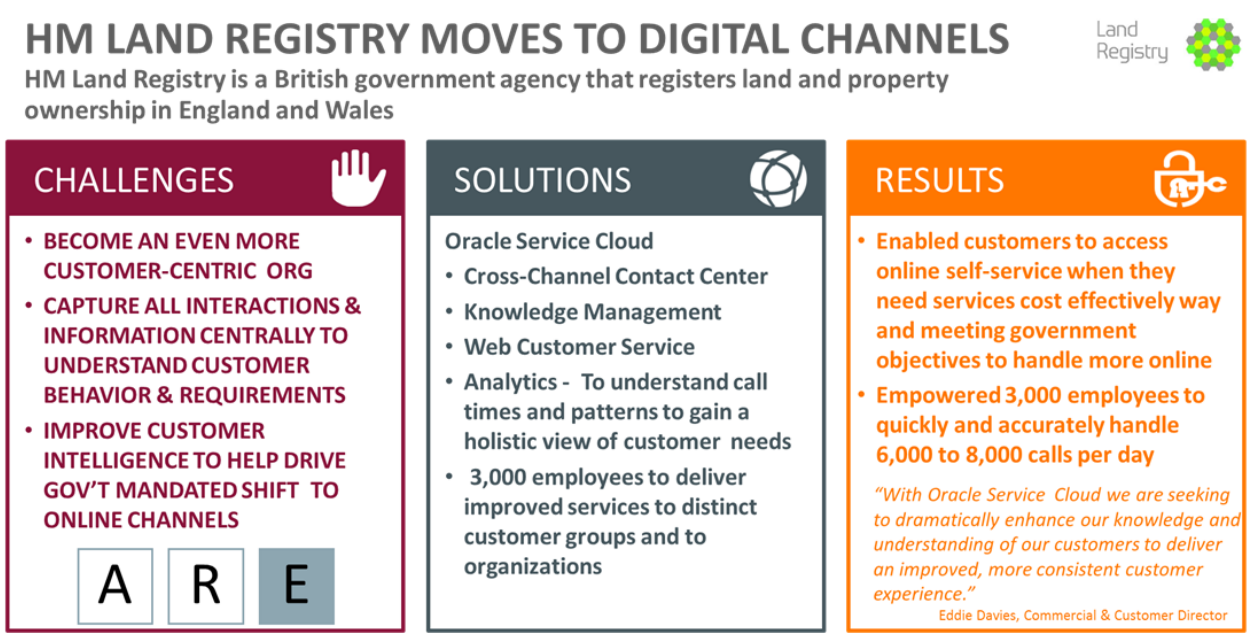


FIGURE 3: ORACLE CLOUD SOLUTION FOR HM LAND REGISTRY, UNITED KINGDOM

CITY OF CARTAGENA CENTRALIZES SOCIAL INTERACTION



Ayuntamiento de Cartagena runs the public admin., social services, sports, police, cultural and youth activities, education, libraries, and communication for the 215K residents of the city of Cartagena, Spain

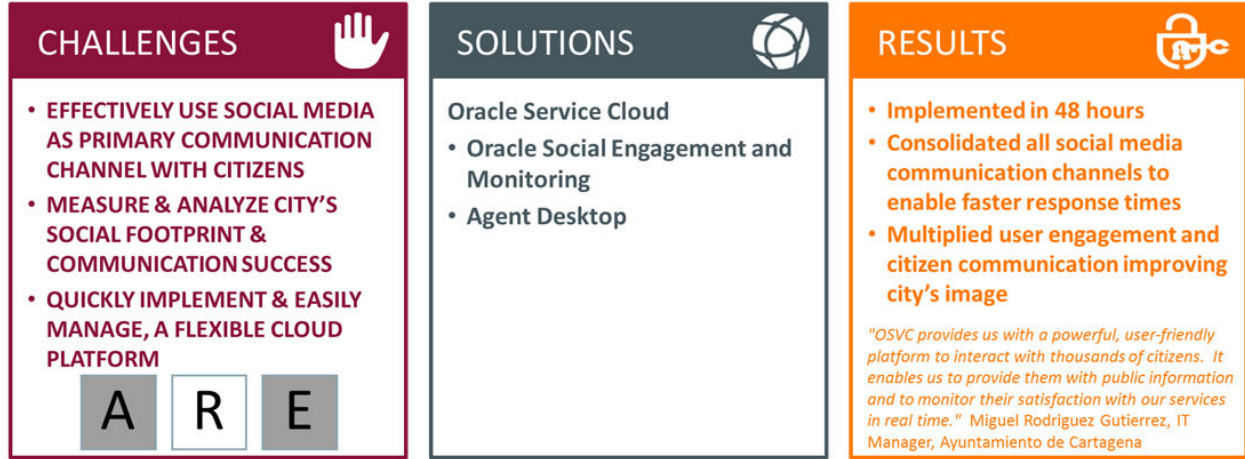


FIGURE 4: ORACLE CLOUD SOLUTION FOR THE CITY OF CARTAGENA, SPAIN

BOSTON GLOBE IMPROVES SERVICE & RETENTION

The Boston Globe

New England's leading newspaper and winner of 21 Pulitzer Prizes with approximately 1.45 million weekly readers and a rapidly growing online subscriber base

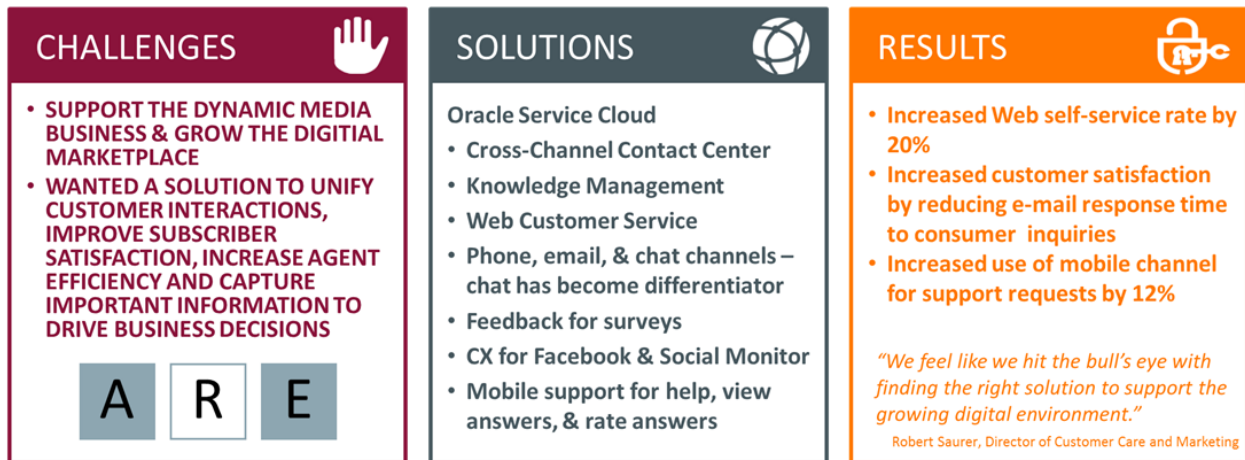


FIGURE 5: ORACLE CLOUD SOLUTION FOR THE BOSTON GLOBE

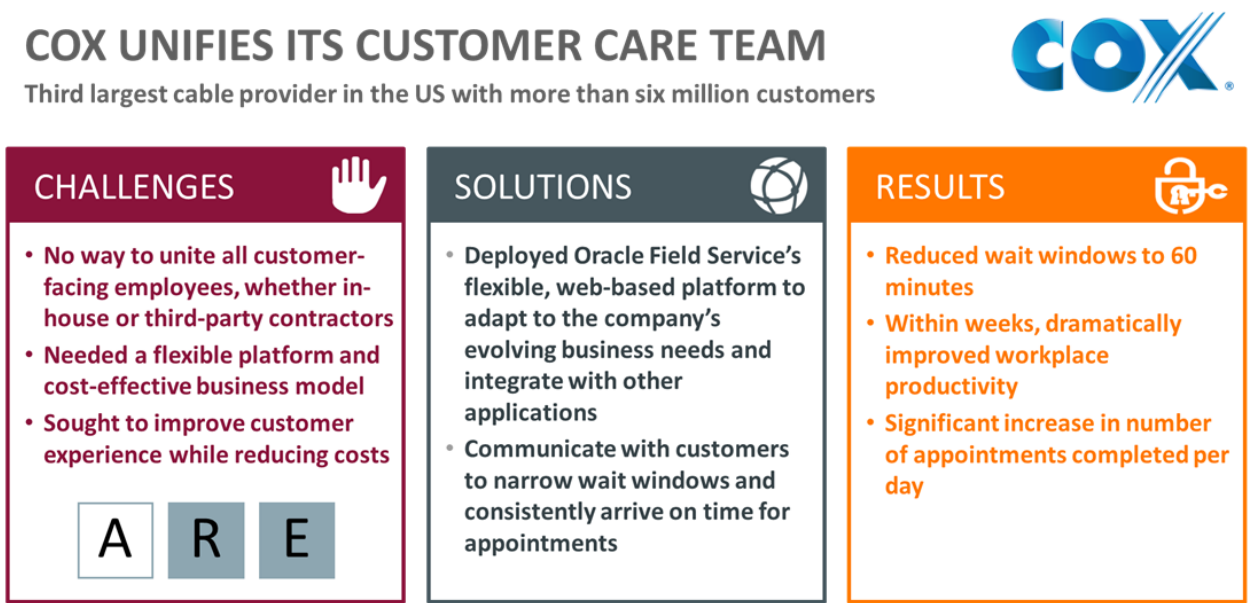


FIGURE 8: ORACLE CLOUD SOLUTION FOR COX COMMUNICATIONS

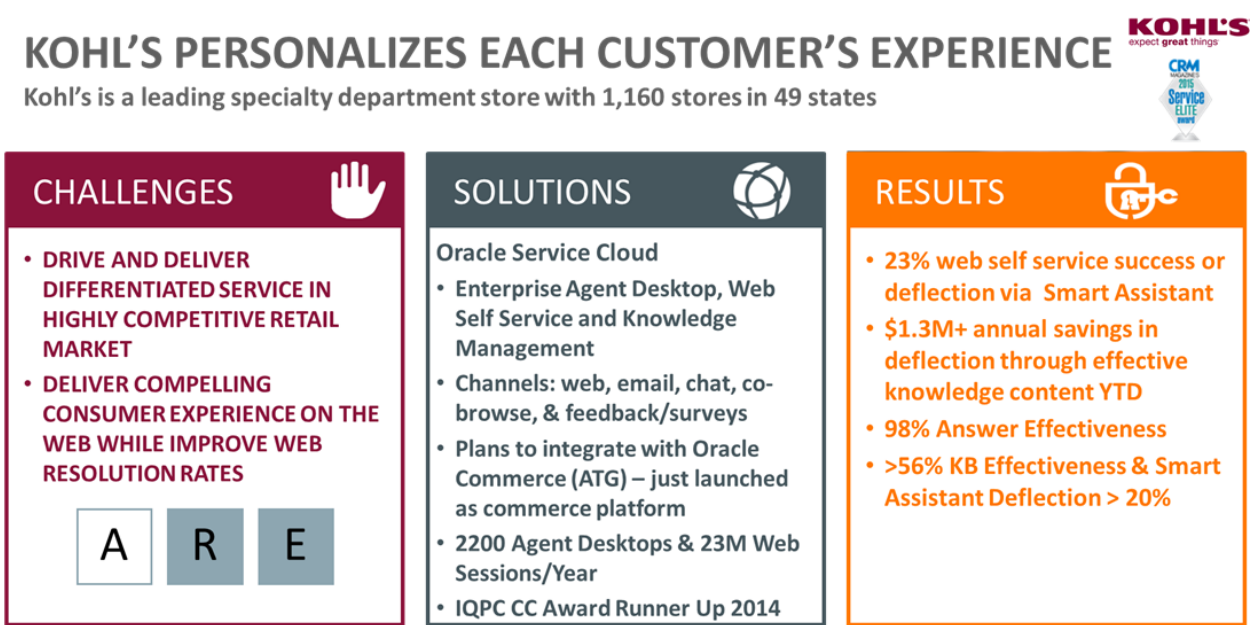


FIGURE 9: ORACLE CLOUD SOLUTION FOR KOHL'S DEPARTMENT STORES

Financials (RFP #6.3)

Provided below is the information requested in section 6.3 of the RFP.

Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

Oracle Response:

Oracle annual reports for fiscal years ending May 31, 2015 and May 31, 2014 are presented in Attachment 6.

The D U N S (D&B) number for Oracle America, Inc. is 01-304-4532. The Oracle Corporation D U N S (D&B) number is 14-470-9193. As of November 19, 2014, the D&B rating for Oracle Corporation was 5A2.

General Information (RFP #6.4)

Provided below is the information requested in section 6.4 of the RFP.

6.4.1 Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace.

Oracle Response:

Oracle's cloud service is portable between the traditional on premise model to cloud then back again as needed. Oracle's cloud services were developed with the agility to integrate easily with legacy applications, future applications, and other third-party technologies. Once in the cloud Oracle's solution offers configuration throughout the system to adapt to changing business needs with configuration without the use of code for ongoing enterprise management. Oracle offers private cloud, public cloud and hybrid cloud solutions to meet modern technology needs.

6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Oracle Response:

Yes, the auditing capabilities and reporting of Oracle's solution are consistent with SSAE 16. Due to confidentiality considerations, Oracle has not included its SSAE16 report(s) as part of this proposal. In the event that Oracle is shortlisted for your RFP, or you elect to award a contract to Oracle for the products and/or services specified in this Response, Oracle would be happy to work with you to provide its SSAE 16(s) reports under a separate nondisclosure agreement.

Billing and Pricing Practices (RFP #6.5)

Provided below is the information requested in section 6.5 of the RFP.

DO NOT INCLUDE YOUR PRICING CATALOG, as part of your response to this question.

6.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

Oracle Response:

Purchase orders are required for ordering cloud services and at the point of order a customer can select from a manual or electronic invoicing option. Service fees are due quarterly in arrear of service delivery with net thirty-payment terms. A credit or purchase card (P-Card) may be used as a form of payment against an invoice provided the fees do not exceed \$99,999 USD. Credit card as a form of payment against an invoice <\$2,000 is mandatory.

Pricing is based on an annual subscription for a particular cloud service for a defined metric discounted from commercial list price. Metrics vary by cloud service type as presented in the Cost Proposal section but an example two of common metrics are:

FOR SAAS

Hosted Named User: is defined as an individual authorized to access the hosted service, regardless of whether the individual is actively accessing the hosted service at any given time.

FOR PAAS

Hosted Environment: is the combination of systems and supporting resources to which Oracle grants you access as part of the Oracle Cloud Services ordered by you, that is (i) configured for the Oracle Programs operating on it and for specific uses as part of the Oracle Public Cloud Services, and (ii) used by Oracle to perform the Oracle Cloud Services. The Hosted Environment consists of the Production Environment, and any non-Production Environment(s), as referenced in the applicable Ordering Document and services policies.

6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

Oracle Response:

Each customer has different considerations and requirements that align with their overall technology objectives and budget. The Oracle Account team will perform an assessment with each perspective Participating Entity to gain an understanding of their goals which may include:

- Reducing facilities/real estate cost
- Reducing technical support fees
- Investment in on premise licenses; do they have a value that can be shelved/exchanged to reduce the cost of a cloud solution

6.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.**Oracle Response:**

Please see our discussion of meeting NIST requirements for our solutions, which are detailed in our response to RFP section 8.1.2 below.

Scope and Variety of Cloud Solutions (RFP #6.6)

Provided below is the information requested in section 6.6 of the RFP.

Specify the scope and variety of the Solutions you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services and deployment models that you offer.**Oracle Response:**

Oracle's platform as a service offering has been extremely well-received in the industry. Today, over 250 SaaS providers are using Oracle products and technologies as a foundation for their own offerings. Providers such as salesforce.com, Ariba, and Perot Systems are just a few of the companies using Oracle's platform as a service solution to power their clouds. Similarly, Oracle leverages this very same, customer available, technology to power its own cloud computing offerings including the Oracle Public Cloud and Oracle Cloud Services. Oracle's PaaS offering is based upon a well-integrated collection of products and technologies that provide middleware and application integration functionality as well as data services, but organizations seeking to build cloud computing architectures need business-ready solutions not point products. Oracle understands what it takes to run enterprise-ready cloud computing environments, and that is why Oracle introduced its line of fit-for-purpose engineered systems—complete hardware and software solutions, engineered together and optimized to deliver the best performance, elastic scalability, security, and availability while drastically reducing IT complexity. These engineered systems are designed to speed up time to deployment, reduce support and management costs, and scale in response to the needs of the organization making them ideal foundations for any PaaS architecture.

Organizations realize that a shared services platform, used to create, integrate, and share applications is critical to maximizing the value of a cloud computing architecture. Just as with applications delivered as a service, platform technologies must too offer flexibility, elastic scalability, and self-service access in order to more rapidly respond to workload fluctuation as well as the ever-changing needs of the organization. Oracle has a very comprehensive PaaS offering that includes market-leading, best-in-class products such as the Oracle Database, the Oracle WebLogic Suite, and the Oracle Identity Management Suite—all #1 in their respective categories according to industry analyst reports.

SERVICES OFFERINGS IN THE ORACLE PUBLIC CLOUD

Currently, Oracle offers the following services in the Oracle Public Cloud:

Oracle Database Cloud Service – provides the power and flexibility of the Oracle Database in the cloud with your choice of a dedicated database instance with direct network connections and full administrative control, or a dedicated schema with a full development and deployment platform managed by Oracle.

The Oracle Database has been the standard for enterprise databases for more than two decades. With the Oracle Database Cloud Service, you get the full power of this legendary platform. You can use the same SQL for data interaction that is used for hundreds of thousands of enterprise applications. You can use PL/SQL, the procedural extensions for the Oracle Database. All the optimizations and data structures, which make the Oracle Database so robust, are available in your Oracle Database Cloud Service.

The Oracle Database Cloud Service uses schema isolation to implement multi-tenancy, which allows full transparency while still providing efficient use of database resources. The Oracle Database is, at its core, a multiuser system for sharing data, so the Oracle Database Cloud Service simply uses the capabilities built up for the Oracle Database to share resources among multiple Oracle Database Cloud Service customers

CLOUD SERVICE MODELS

Oracle is proposing to provide the following two cloud computing services models:

- **Software as a Service (SaaS)** – The service provider offers one or more applications over the network to be customized (where possible) and used by its customers.
- **Platform as a Service (PaaS)** – The service provider offers development and deployment platforms over the network to be used by customers building or assembling their own applications using these provided frameworks.

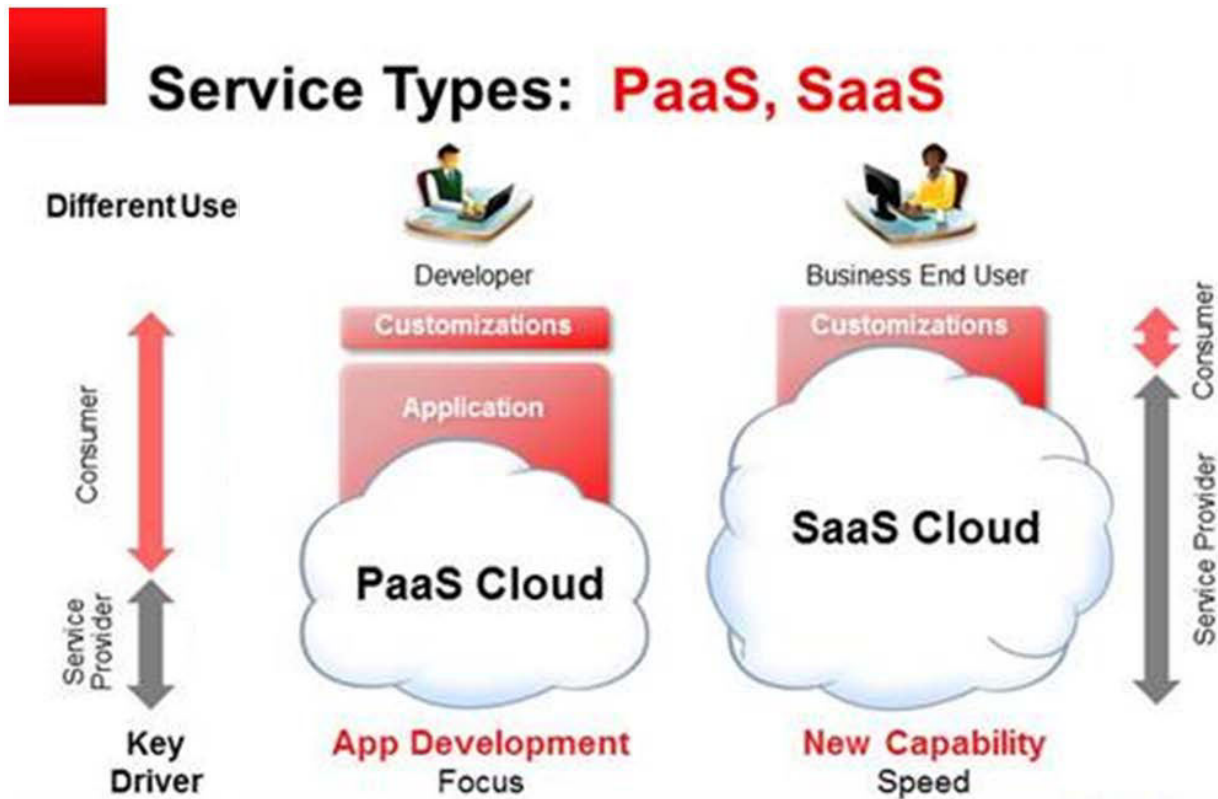


FIGURE 10: PROPOSED ORACLE CLOUD SERVICE MODELS

DEPLOYMENT MODELS

The four cloud computing deployment models include:

- **Public Cloud** – An environment provisioned for open use by the general public.
- **Private Cloud** – An environment provisioned for exclusive use by a single organization comprising multiple (internal) consumers. Sometimes called an enterprise cloud, private clouds can be on premise or off premise, managed internally or managed by a third-party provider.
- **Community Cloud** – An environment provisioned for exclusive use by a specific community of consumers from different organizations that share business or computing goals, needs or concerns.
- **Hybrid Cloud** – An environment comprised of two or more of the above specified cloud computing deployment models in a manner where they are bound together using technology that supports application, service or data portability, migration, and interoperability.

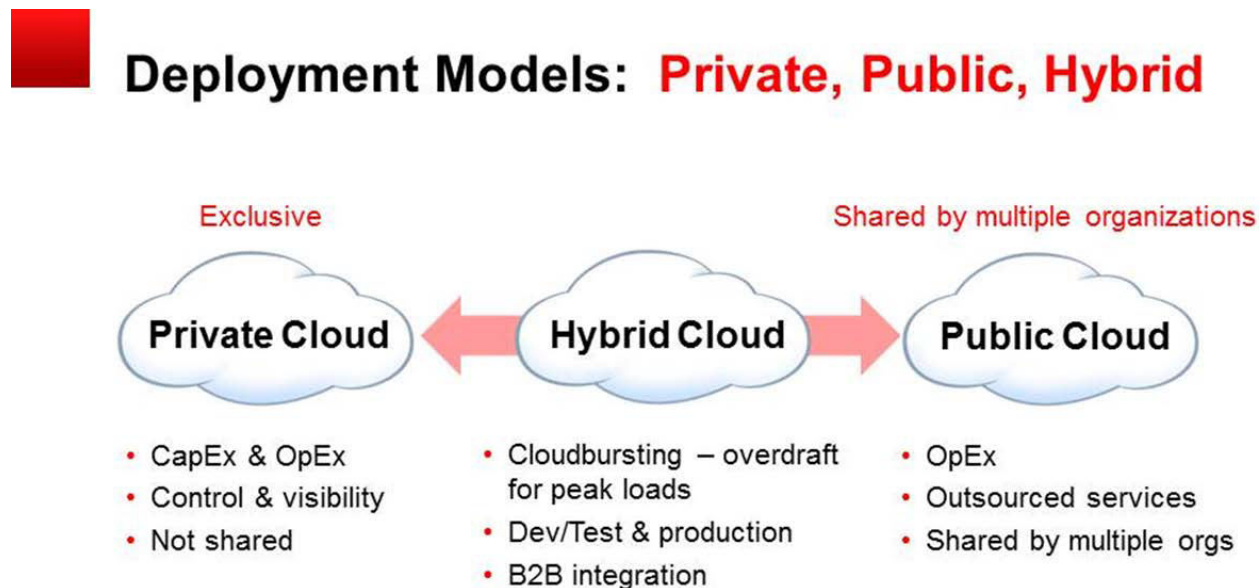


FIGURE 11: ORACLE CLOUD DEPLOYMENT MODELS

Best Practices (RFP #6.7)

Provided below is the information requested in section 6.7 of the RFP.

Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

Oracle Response:

Oracle Cloud services employ a holistic approach to application and data security, with controls enforced at multiple layers—physical, network, application, infrastructure, and personnel security.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

The Oracle Cloud services are aligned with the security framework of International Organization for Standardization (ISO) and International Electro-technical Commission (IEC), specifically ISO/IEC 27002:2005, Code of Practice for Information Security Management and ISO/IEC 27001:2005 standards, but are not ISO 27001 certified.

Customers with a licensing agreement or signed confidentiality disclosure agreement can request a copy of the SOC 1—SSAE 16 and ISAE 3402 reports for Oracle Cloud Services. The controls included in Oracle's self-attestations for SSAE 16 SOC1 and SOC2 reports are aligned with the controls and objectives of the ISO 27001 framework. These reports are steps toward formalizing our ISO 27001 compliance and certification.

Additional details can be found in Section 1.9 of the Oracle Cloud Enterprise Hosting and Delivery Policies document found in Attachment 7.2.

Encryption is offered end-to-end for Oracle Cloud Services. Oracle Cloud Services can provide encryption capabilities for both data in-transit as well as data at rest. Encryption technologies may vary based on cloud services and leverage technologies such as SAN encryption or database encryption.

Oracle has an Incident Response Plan for IT security breaches. Oracle evaluates and responds to incidents that create suspicions of unauthorized access to or handling of customer data whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. When Oracle's Global Information Security (GIS) organization is informed of such incidents and, depending on the nature of the activity, it defines escalation paths and response teams to address those incidents. GIS will work with customer, and the appropriate technical teams, and law enforcement where necessary to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of customer's environment, and to establish root causes and remediation steps. Operations staff has documented procedures for addressing incidents where handling of data may have been unauthorized, including prompt and reasonable reporting, escalation procedures, and chain of custody practices.

In addition, Oracle has an Oracle Cloud Service Exception Report Practice, geared toward fulfilling our customers' Enterprise IT and transparency needs. Service Exception Reports (SER) contains information from root cause analysis performed by Oracle Cloud Operations on specific service outages.

Root Cause Analysis (RCA) is a procedural framework used as part of IT Infrastructure Library Problem Management by Oracle Cloud Operations personnel to:

- Identify and understand the root cause of problems concerning Oracle Cloud services.
- Maintain transparency with service subscribers.
- Implement adequate controls and measures to ensure that the problem does not recur.

SERs are provided to customers only when they formally request them through My Oracle Support (<http://support.oracle.com>). Typically, Oracle provides SERs to affected customers as soon as the root cause analysis is complete. Oracle Cloud customers can request SERs for issues or outages that occurred in the last 30 days.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

SERs can be requested for the following types of outages.

- **Unplanned Outages** – P0 impact lasting more than 15 minutes, outages that prevents us from fulfilling customer SLAs, and third-party system outages.
- **Performance Degradation** – Persistent issues, slow performance for longer than 15 minutes.
- **Other** – Maintenance windows exceeding projected duration, partial service failure events exceeding 15 minutes.

The Oracle Cloud Customer Portal is a one-stop-shop for customer's Oracle Cloud Service lifecycle management needs. The portal is role-based and provides both business and operational details of the Oracle Cloud.

Account owners as well as security contacts can perform various functions on the Oracle Cloud Customer Portal including, but not limited to:

- Monitor health of all services across multiple data centers
- Purchase one or more services across multiple data centers
- Retrieve customer support identifier (CSI), that can be used My Oracle Support Portal to obtain help with issues related to paid services from highly qualified technical staff
- Manage payments, credit cards, and purchase orders
- Monitor service entitlement overages
- Monitor Service Level Agreements (SLAs) and aggregated service as well as business metrics
- Monitor scheduled and unscheduled outages to services
- Delegate service and/or account administration role assignment to other users
- Manage users, roles and policies, and perform bulk operations
- Manage service lockouts
- Retrieve terminated service archives within 60 days after termination

Oracle Cloud Services uses firewalls to control access between the internet and Oracle Cloud by allowing only authorized traffic. Firewalls are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address to identify authorized sources, destinations, and traffic types.

Security vulnerability tests are performed regularly, at least annually. There are multiple levels of ongoing security checks, threat and risk assessments, vulnerability scanning, and penetration testing used to validate system controls, including file integrity where applicable.

5. Organization Profile

This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.

Organization and Staffing (RFP #7)

Provided below is the information requested in section 7 of the RFP.

Contract Manager (RFP #7.1)

Provided below is the information requested in section 7.1 of the RFP.

The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have experience managing contracts for cloud solutions.

7.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

Oracle Response:

Contract Manager: Rachel Kasoff

Email Address: rachel.l.kasoff@oracle.com

Phone Number: +13032729791

Work Hours: 9 a.m. to 5 p.m. (MST)

7.1.2 Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager.

Oracle Response:

Rachel Kasoff is a member of Oracle's Government Sector Contract Administration Group. She manages some of the key customer contracts Oracle, namely the contracts for CT, DE, IL, LA, MD, MN, NM, WA and NASPO. Please see attached resumé in Section 7.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

7.1.3 Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

Oracle Response:

The Contracts Manager shall be responsible to administer all the contract administration requirements of the awarded contract, including reporting, pricing updates, and any other contract communications required by the contract.

6. Technical Response

6A. Description of Proposed Solutions

This section should constitute the Technical response of the proposal and must contain at least the following information:

A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offeror's ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

Oracle Response:

The Oracle SaaS Solutions – The Oracle Service Cloud Platform

In an effort to properly introduce you to the Oracle Service Cloud Platform, we believe that a brief solution overview is an important place to start. To be clear, we are offering Oracle RightNow Enterprise Contact Center Dynamic Agent Desktop Cloud Service and Tier 1, Tier 2, and Tier 3 Web Sessions. This offering includes the following list which is discussed in the sections that follow:

- Oracle RightNow Web Experience
 - Oracle RightNow Customer Portal Cloud Service (Tier 1 and Tier 2 Sessions)
 - Oracle RightNow Chat Cloud Service
 - Oracle RightNow Cobrowse Cloud Service
 - Oracle RightNow Email Management Cloud Service
 - Oracle Policy Automation Web Cloud Service (Tier 3 Sessions)
- Oracle RightNow Contact Center Experience
 - Case Management
 - Core Agent Desktop
 - Incident (Case) and SLA Management
 - Business Rules, Escalations, Routing
 - Interaction Management
 - Oracle RightNow Basic Screen Pop Cloud Service
 - Oracle RightNow Incident Collaboration Cloud Service
 - Oracle RightNow Mobile Agent App Cloud Service
 - Oracle RightNow Asset Management and Product Tracking Cloud Service

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

- Oracle RightNow Engage
 - Oracle RightNow Outreach Cloud Service
 - Oracle RightNow Feedback Cloud Service
 - Oracle RightNow Analytics Cloud Service
- Oracle RightNow Social Experience
 - Oracle RightNow Social Monitor Cloud Service
- Oracle RightNow Platform
 - Oracle RightNow Connect Cloud Service
 - Oracle RightNow Cloud Platform Cloud Service
 - Oracle RightNow Incident Thread Masking Cloud Service
 - Oracle RightNow Standalone Foundation Agent Knowledgebase Cloud Service

We believe this solution and its components fall in line with the performance objectives outlined in your requirements and greatly exceed those expectations with an out-of-the-box, scalable solution. A solution that can support multiple departments while providing an end-to-end approach for web services to your customers. The Oracle Service Cloud Platform will be able to let you field, evaluate, and implement requests via tools like workflow and experience routing all with robust reporting. In essence, you can engage your customers, empower your staff, and adapt through the actionable insights available in the Oracle Service Cloud Platform. Oracle Policy Automation (OPA) will be able to put your policies into easy to understand natural language through familiar interfaces like Excel and Word, not complicated code. It can be applied to intake to assist in the evaluation and determination processes. Such assistance can be presented through our platform's self-service, on the web via any device or to contact center agents handling calls or conducting determination interviews. Lets look a little closer at the solution components in the sections that follow.



FIGURE 12: THE ORACLE SERVICE CLOUD PLATFORM

1. THE ORACLE SERVICE CLOUD PLATFORM

Since the requirements in this request are more around the SaaS platform and its capabilities, we are going to begin with a discussion of the Oracle Service Cloud Platform, and then delve into the solution components that were built upon this Customer Experience platform.

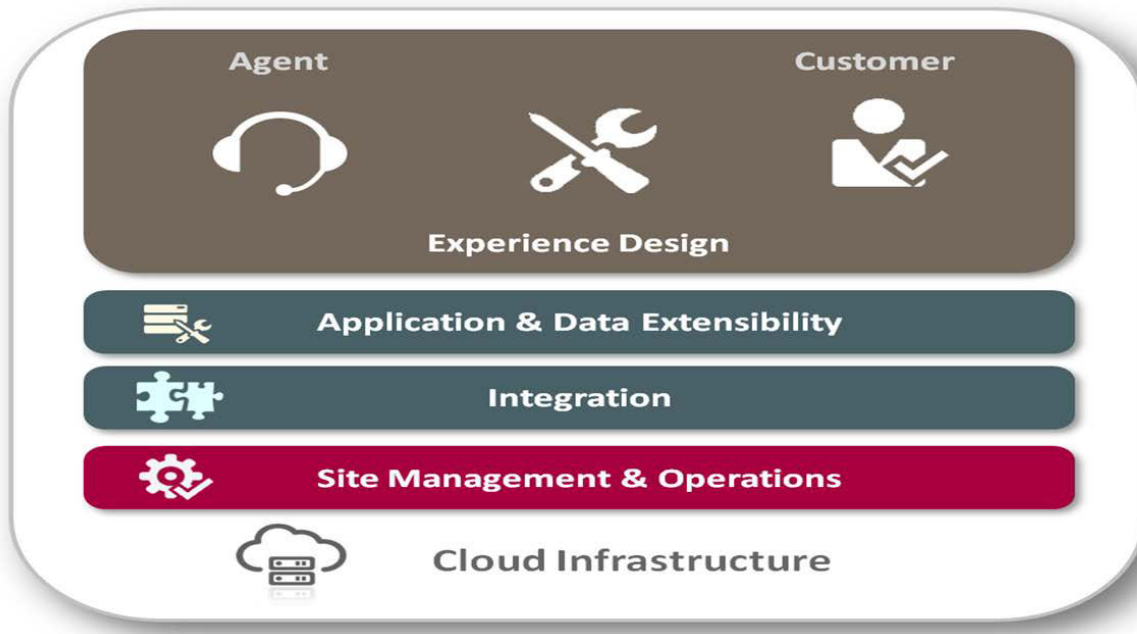


FIGURE 13: ORACLE'S SOLUTION: FLEXIBLE AND PERFORMANCE PROVEN APPLICATION PLATFORM

- Agent and Customer Design
 - Leverage designers built for business users to customize the experience
- Integration and Extensibility
 - Integrate using open standards technology and extend applications to meet business needs
- Cloud Operations and Delivery
 - Monitor, test, and control your site(s) with visibility into the entire implementation
 - Trust mission-critical levels of security, reliability, and data redundancy

1.1. Agent Experience Design for Business Users

- **Experience Designers – Make it Simple**
 - Leverage an array of designers to configure your own custom application
 - Build screens and views simply by dragging and dropping elements
 - Control interaction flow, trigger events, and define access by profile

- **Developer Tools** – Expand and Adapt
 - Leverage add-ins to create new user interface functionality, automate user interface behavior, and integrate behind the firewall
 - Use the JavaScript application programming interface (API) to embed any web application and pass context

1.2 Design Pixel Perfect Customer Experiences – Fast!

- **Web Service Design**
 - Match your existing website branding down to the pixel
 - Leverage widget-based design to mash-up capabilities on any web page
 - Extend and customize widgets using step-by-step wizards
 - Meet Oracle accessibility standards
- **Fast Deployments**
 - Accelerate deployment with 160 pre-built widgets, pages, and templates
 - Implement changes instantly with zero site downtime
 - Deliver for browsers, mobile browsers, and Facebook



1.3 Extensibility

- **Custom Objects**
 - Create an entirely new application or extend the base applications
 - Leverage the array of designers to create rich applications—new objects inherit all platform capabilities
 - Define relationships between objects and create new custom fields
 - Define and extend business logic to new and existing objects
- **Upgrade Safe**
 - Rest assured that your work will always be upgrade safe

1.4 Integration

- **Standards-based APIs**
 - Leverage non-proprietary APIs and integration capabilities (PHP, XML, WSDL, SOAP)
 - Conduct real-time and batch data synchronization via SOAP APIs
 - Integrate via PHP-based APIs to support server-side scripting scenarios and event triggers

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

- SOA Ready
 - Enable SOA tooling via SOAP/WSDL APIs, Oracle SOA Connector, and Oracle Service Bus
 - Leverage built-in single sign-on support
- System Integrator Partners
 - Leverage system integrators to help with everything from the initial implementation to customizations
 - Take advantage of direct switch access and control with telephony integrators
 - Ensure proven, repeatable integrations to Oracle Service Cloud
- ISV Partners
 - Select best of breed ISV partners to extend solution capabilities



FIGURE 14: ORACLE PARTNERS ENHANCE THE ORACLE CLOUD SOLUTION

1.5 Mission-critical Cloud Delivery

- Secure
 - Industry-leading security compliance
 - The only cloud solution operating inside the U.S. Department of Defense
- Reliable
 - Mission-critical reliability
 - Carrier-grade hosting facilities
- Redundant
 - Data redundancy and disaster recovery across multiple geographic locations
 - No single points of failure for continuous availability

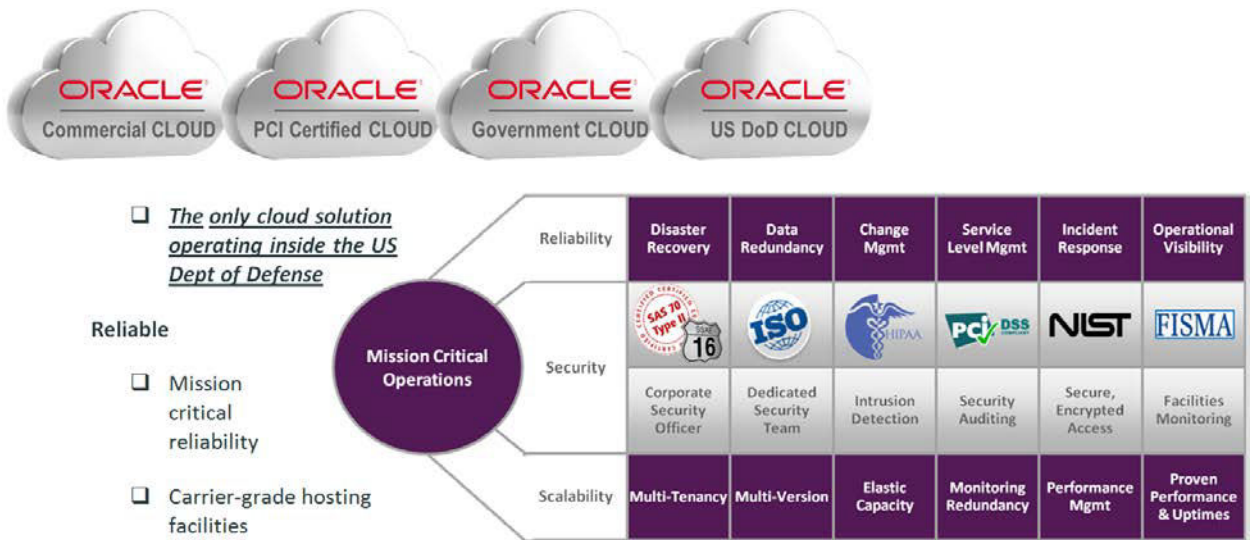


FIGURE 15: ORACLE’S INDUSTRY-LEADING SECURITY COMPLIANCE

1.6 Site Operations Management

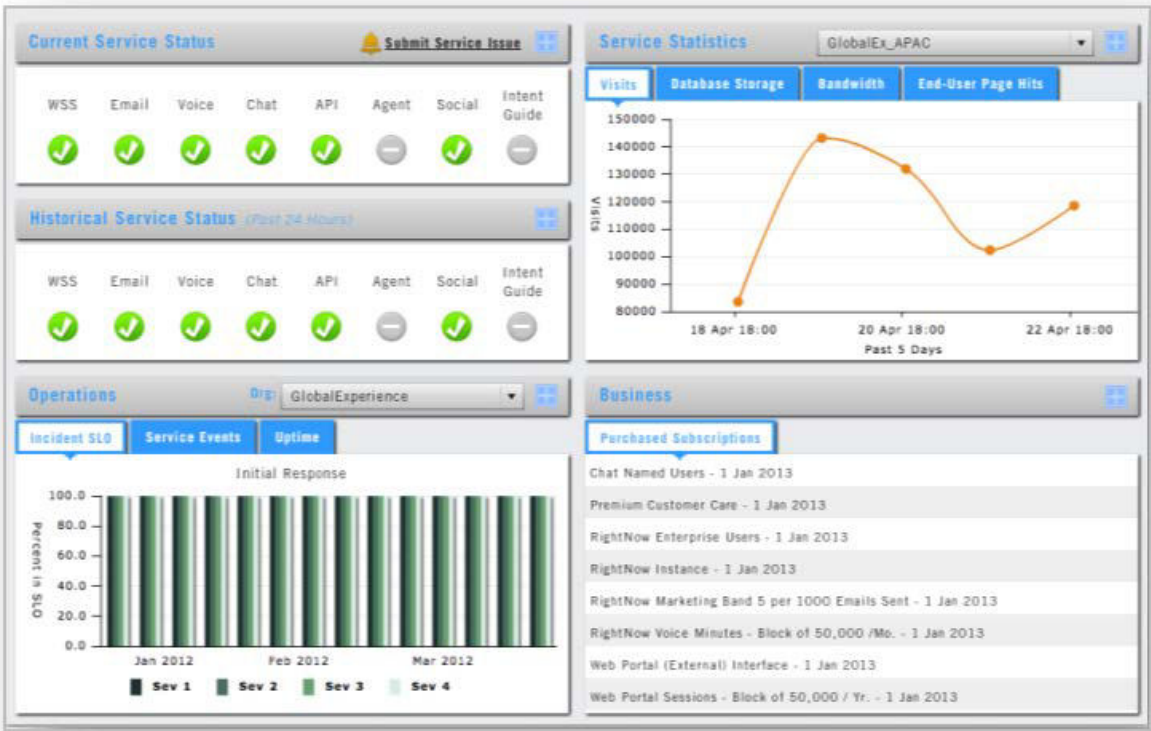


FIGURE 16: SUPERIOR CONTROL OF THE ORACLE CLOUD ENVIRONMENT

- Monitor
 - Monitor system-wide performance as well as individual applications
 - Track application usage
 - Monitor service level targets
 - Track purchases and subscriptions
- Test
 - Create test sites to evaluate changes, integrations and extensions
- Control
 - Schedule upgrades
 - Control application access

1.7. Beyond Enterprise to Global Scale

- Global Presence
 - Major hosting centers worldwide
 - Redundancy and failover handled across geographies
 - Global implementation scale
- Language Support
 - Application localization in 34 languages

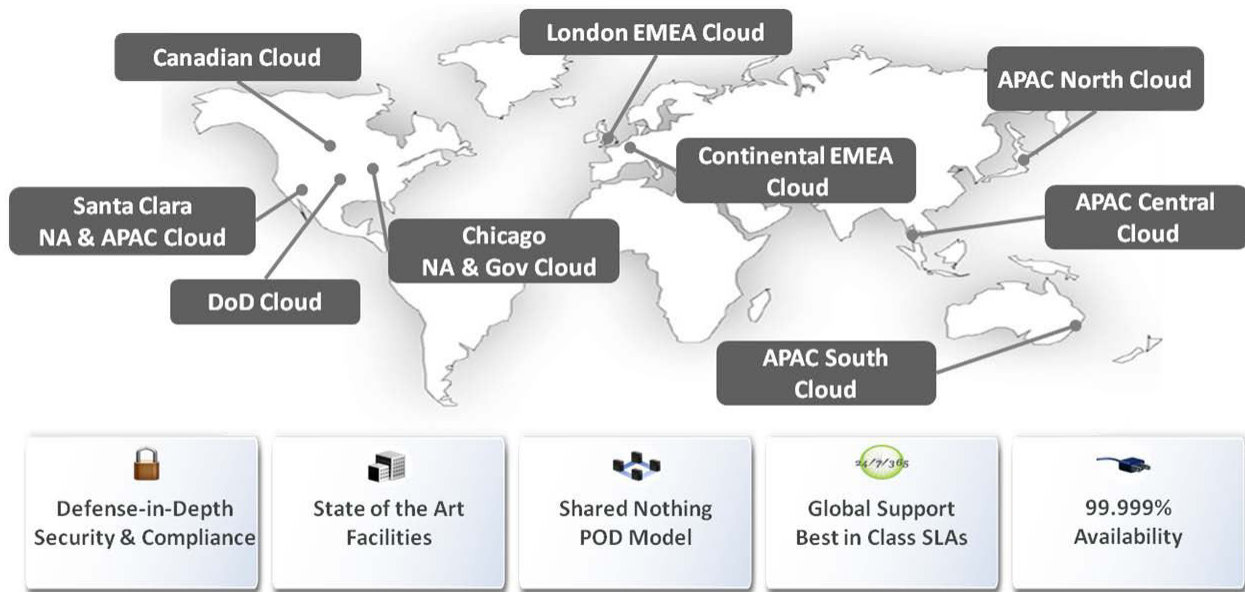


FIGURE 17: ORACLE'S SOLUTION: GLOBAL SCALE PLATFORM

2. MODERN CUSTOMER SERVICE

Today's global economy has been made more accessible by the internet, social media, mobile, and other technologies. This has shifted from the provider to the consumer. Organizations can no longer rely solely

on having a better product or lower price in order to remain competitive. This demand on the Private Sector has split over into the Public Sector. Increasingly, it is the manner in which organizations engage with their existing and potential customers that dictates success or failure in their mission.

"Oracle Service Cloud helps us to deliver superb customer experience and is integral to our vision of presenting a personal, responsive, and a customer-focused brand."

- Helen Ellis, Director, Customer Experience, Photobox

Successfully delivering an omni-channel service capability has been proven by existing Oracle customers to drive significant reduction in the cost of customer service.

First call resolution	15% ↑
Email into contact center	30% ↓
Call volumes	15% ↓
Training costs	50% ↓
Average handle time	25% ↓
Customer satisfaction & Net Promoter Score	25% ↑

FIGURE 18: STATISTICS-BASED CUSTOMER DATA

Oracle's solution offers a full service, cross-channel out-of-the-box solution. Our fully integrated Customer Experience (CX) Suite makes it possible for us to offer a lower cost and lower risk solution, which can be:

- Implemented quickly at low cost
- Configured to your business needs
- Scaled rapidly to meet demand
- Maintained by business users
- Leveraged to achieve quantifiable benefits in as little as a month

Oracle's solution gives you the flexibility and speed to quickly adapt to your customers' changing needs allowing you to beat competitors and to rapidly address new market opportunities. Oracle offers a one-stop solution out-of-the-box, meaning that you do not have to worry about the extra cost and complexity of managing add-on partners and their solutions.

Oracle's solution empowers connected engagements that let organizations:

- Understand needs – Infuse insight into each customer engagement.
- Solve problems – Manage interactions across all channels
- Delight customers – Increase trust through great service
- Drive self-service

3. ORACLE'S SOLUTION: WEB CUSTOMER SERVICE

Oracle's solution provides a rich online customer experience solution, allowing customers to research and resolve issues from multiple devices. It sets a standard for excellent service by allowing your members, non-members, and customers to interact on their own terms while you lower service costs and increase customer loyalty.

FAQ knowledge management enables visitors to find answers online from any web-enabled device. The self-learning knowledgebase improves with every customer interaction and provides deep and valuable insight into every customer and trend. Guided Assistance uses branching logic to guide customers through more complex queries. SmartAssistant suggests knowledgebase answers to queries ahead of submission; providing one last opportunity for self-service resolution.

Live Chat software provides an easy and effective way to provide assistance solving an issue and, perhaps, engage a customer in a research process. Chats can be customer-initiated (reactive) or proactively (proactive) offered, based on criteria defined by your organizations. Oracle's Engagement Engine allows powerful and flexible rules to be created that detect conditions in the user's session and allow invitations for chat (or indeed other services such as Click to Call or Knowledge article display) to be offered based on that context and thereby offer a differentiated service based on both customer needs and the value of that customer to the organization. In the Engagement Engine, 70+ rules types are available to detect a wide variety of conditions in the user's session that can be combined to perform a range of different actions including the offering of live chat. Further, co-browse provides the ability for your customer service staff to share control of the customer's screen during a contact. This way, you are able to achieve a visual connection that allows customers to reach their goals on the phone or via live chat.

Social Self-Service differentiates your brand by increasing your relevance, growing your fan base, and delivering on your brand promise where your customers are.

- Enable customers to browse and find knowledgebase answers without leaving Facebook.
- Communities are the lowest cost service channel. Customers can ask questions, post answers, and then rate and reuse the collective expertise of your community. Further, questions can be escalated into service incidents, accessible on the Agent Desktop; where agents can view community members' profile data and manage follow-up actions.
- Innovation Communities help you reduce research and development costs and discover profitable new ideas and business opportunities. Customers are able to form personal networks, communicate through private messaging, participate in discussions and share community content with the broader social web.
- Smart Engagement provides the ability to focus on customer intent. It is a set of capabilities that includes Guided Assistance, SmartAssistant and Intelligent Routing. The goal of Smart Engagement is to help you reduce inbound escalations by guiding your customers to the best answer via the web.
- Guided Assistance provides step-by-step troubleshooting, based on branching logic. Guides can be created quickly and easily, and updated as required.
- SmartAssistant recommends the best answer based on customer question content submitted via an "Ask a Question" web form. SmartAssistant can reduce inbound escalations by up to 30 percent (based on customer data).
- Intelligent Routing leverages real-time behavior and agent skills to match the right agent with the right customer.

4. ORACLE'S SOLUTION: CROSS-CHANNEL CONTACT CENTER

Oracle's solution offers a unified Agent Desktop, providing the ability to:

- Unify Your Applications
 - Embed the multi-channel media bar
 - Use the add-in framework and API
- Extend the Desktop
 - Extend the data model with object extensibility
 - Enable non-technical business users with experience designers
- Integrate Everything
 - Connect web applications with JavaScript API
 - Integrate the Contact Center out-of-the-box to other applications in the Oracle portfolio

Oracle's solution offers a complete omni-channel case management solution. All channels are blended within the Agent Desktop. If an inquiry is received from someone who does not have a customer record, a new record will be created automatically by the system to speed up the interaction.

The case management capabilities in Oracle's solution deliver quality communications and timely resolution to cases; with personalized responses that leverage centralized knowledge, routing, workflow, and cross-channel communications.

The flexible, multi-channel Agent Workspace offers a unified view of a customer's service experience and interactions across multiple channels. The customer data model captures information unique to your business. The solution provides the ability to manage workspaces for contacts and accounts across service interactions and to define the SLA each customer is eligible to receive and credit incidents against the SLA. Further, intelligent queuing and routing provides the ability to automate updates, responses, escalations and assignments; balance workloads using standard assignment and round-robin queuing.

The mobile desktop application provides agents with native mobile capabilities, away from their desktop. The application provides the ability to manage incidents and tasks, as well as contacts and organizations. Users can also use offline caching in areas where internet connection is not available.

Incident Collaboration makes it possible to collaborate in context of an incident between multiple agents and subject matter experts. Collaboration is available through mobile devices, Outlook and web browsers in order to participate in conversations. Participants are able to post messages, and annotate documents so everyone in the conversation can view them. Additional people can be added to the conversation as required.

Guided Resolution reduces agent training time and ensures consistent troubleshooting and resolution.

- Guided Assistant guides agents through a series of questions and answers to diagnose issues.
- Ensure Consistency with Agent Scripting. Create scripts to guide agents through customer interactions and capture their responses. Agents are efficiently guided through complex business processes. Deliver personalized experiences with scripts that change based on the customer or interaction.

- Contextual Workspaces dynamically change workspaces based on agent role, customer information or any field change.
- Policy Automation ensures policies are met prior to delivering products or services. Design dynamic interviews that change based on customer answers.

Integrated Knowledge Management helps to improve resolution time with more accurate answers available to staff and customers in the single knowledgebase. Visibility to knowledge articles can be restricted by public, private, and group access. Content can be authored and managed in multiple languages.

Social Engagement allows you to monitor social channels, such as Twitter and Facebook, and engage with your customers within the social sphere.

- Social Monitor allows you to monitor Twitter, Facebook, YouTube, and any social site with an RSS feed. The Social Monitor makes it possible to understand trends in activity and sentiment across social networks. Post authors can be matched to existing contacts and a threaded conversation can be added to an existing incident thread.
- Social Communities provide a space where customers can share insights and knowledge. Partner organizations can moderate posts and identify best answers and respond to posted questions. Agents can search for answers across both community and company knowledge.

Customer Engagement allows you to gather feedback from, and proactively communicate with, your customers.

- Easily capture customer feedback with customer surveys and social monitoring.
- Outreach mailings allow you to create proactive, relevant communications based on complete customer history.

5. ORACLE'S SOLUTION: POLICY AUTOMATION

Oracle Policy Automation (OPA) – OPA will enable your organizations to define, deploy, monitor, and analyze complex and rapidly changing policies and procedures, using natural language and familiar software tools such as Microsoft Word and Excel. With this platform, partner staff can leverage highly complex business logic and processes to make critical decisions consistently and accurately.

OPA provides tools that will enable the business to mark up existing policies using tools that are familiar to business users, such as Microsoft Word and Microsoft Excel. Once compiled, this creates an application that can be used either via your self-service website or within your call center. The result is an interview that either a customer or agent can work through to obtain an answer to their query.

Benefits of Oracle Policy Automation – Oracle Policy Automation will enable your organizations to offer a service to its customers with:

- More efficient, effective, and accountable delivery of product and customer services.
- Fairer and more consistent determination of legislation and policy obligations.
- Dynamically generated questionnaires that only ask relevant questions, and delivers personalized interactive advice to citizen and organizations and tracks it.
- Pre-integrated Oracle's solution, including deployment as a natural knowledgebase extension, and can be used to deliver a single set of decision/advice logic across multiple service delivery channels.

- The ability to rapidly deliver innovative, fast-changing products and customer services to your customers in a cost-effective manner.
- Vastly improved agility and flexibility, as the business can adjust the rules in minutes rather than days.
- The ability to significantly reduce the possibility of ‘translation errors’.
- Capability to automate decisions using business rules, moving the operational process much closer to the customer front-end; resulting in greatly improved consistency, accuracy, timeliness, and reduced operational costs.
- Natural language as a way to centrally manage intellectual property and business logic rather than encoded in complex programming code across multiple applications.
- Overall productivity increases, with fewer repeat inquiries and appeals.

6. ORACLE’S SOLUTION: KNOWLEDGE MANAGEMENT

Knowledge Management will provide the ability to capture and deliver knowledge, in order to more effectively resolve your customer issues. Knowledge Management is a core function within Oracle’s solution. It is the primary driver for our Web Self-Service offering and is natively integrated to Contact Center, Chat, Email, and Analytics.

The single knowledgebase is presented across all channels and is available to both customers and staff users, meaning that a single version of the truth is presented to all users. The knowledgebase can be segmented according to user profile; allowing you to maintain appropriate access levels. Knowledge articles can be segmented by public, private, brand, product, and custom groups. It is also possible to customize content via conditional sections within articles.

Content Authoring is managed in the application, via a user-friendly WYSIWYG editor. Rich, compelling knowledge interactions are handled with Rich Media Support. Custom authoring and approval workflow can be designed within the solution. The solution is also easily integrated into the KCS methodology and is KCS verified. Core language dictionaries are available in 33 languages.

Self-Learning Search minimizes knowledge maintenance with self-learning capabilities that dynamically push the best answers to the top. Self-service rates are maximized by delivering the best answers with self-learning and real-time indexing.

SmartAssistant evaluates the language of a customer’s question on Ask a Question queries and suggests possible answers. SmartAssistant can reduce inbound escalations by up to 30 percent (based on customer data).

Guided Assistant offers guided resolution with step-by-step troubleshooting for agent and customers. Guides can be embedded wherever they are most useful on web pages, in email responses or within knowledgebase articles.

Knowledge Analytics allow you to gain insight into how knowledge is being used, understand, which articles have the lowest/highest deflection rate and identify and address gaps in your knowledge. Numerous standard reports are available. It is also possible to create ad-hoc reports from scratch or modify existing pre-built reports.

7. ORACLE'S SOLUTION: FIELD SERVICE

Oracle Field Service Cloud Service transforms customer experiences as well as the effectiveness and productivity of your field service operation. Customers no longer wait without knowing when service will occur and how long a job will take, because Oracle Field Service Cloud Service's patented approach eliminates guesswork and uncertainty. Users can plan, optimize, and manage fieldwork, scheduling and coordinating jobs for mid-to-large workforces in minutes. Then, field teams can communicate with customers and each other to ensure jobs are completed in a timely manner. This holistic field service loop allows you to create efficient daily job schedules, work assignments, and routes while maintaining a real-time view of the field. If something changes, you can make adjustments on the fly and still keep customers informed.

Avoid disappointing customers by :

- Quickly determining how much work can be completed based on available resources, skills, work zones, and work types,
- Eliminating the risk of over- and under-booking,
- Setting limits for the desired amount of work, and making adjustments on the fly to match changing business priorities, and
- Empowering agents to book appointments that match customer preferences.

8. INTEGRATING ORACLE'S SOLUTION ACROSS THE ENTERPRISE

Oracle's solution offers several APIs that permit real-time integration to either point systems or via a web services-enabled Enterprise Service Bus. Oracle's solution is designed to integrate effectively with existing systems and data transfer can be done in a variety of different ways.

On the most basic-level data can be imported and exported to and from Oracle's solution using a simple comma delimited (CSV) file, but both real-time and batch data transfer can be automated using Oracle solution's API.

Oracle's solution supports several methods of integration and accommodates both real-time and batch modes.

From a real-time perspective, Oracle's solution supports a variety of APIs.

- Oracle's solution Connect is a framework of APIs available in both .NET and Java distributed libraries. This enables you to choose the programming model that best aligns with their skills and experience as well as current in-house methodology in order to integrate with Oracle's solution. In addition, third parties may leverage these APIs to develop connectors between Oracle's solution and other enterprise applications. This framework of APIs will continue to be enhanced in future releases to support new APIs as well as new programming models.
- The Oracle's solution desktop console also supports .NET add-ins which may greatly extend the functionality of the solution; for example, Google Map pop-ups to display location addresses of members, cases or transactions

- Oracle's solution also provides the ability to send outbound messages based on events within the Oracle solution environment. External Events provide the ability to create custom programs that can be invoked from within the Business Rules Engine of Oracle's solution. These custom programs are typically used to integrate with third-party applications, but they can also be used to implement unique functionality that extends the capabilities within the environment of the Oracle solution.

Oracle's solution also supports batch integration techniques for periodic importing or exporting of bulk data. These batch utilities are most often used during the initial set-up of Oracle's solution environment to "seed" customer and support data. However, the utilities are also deployed for recurring imports and exports in conjunction with other enterprise applications as a part of master data management initiatives.

In addition, Oracle's solution enables customers to integrate the customer experience within the desktop or over the web. In the contact center, Oracle's solution provides third-party specialist teams with the ability to use standard connectors to all of the major telephony providers, including the Cisco telephony infrastructure that may currently be in use.

9. ORACLE PAAS – ORACLE DATABASE CLOUD SERVICE

Oracle Database Cloud Service provides the power and flexibility of the Oracle Database in the cloud with your choice of a dedicated database instance with full administrative control, or a dedicated schema with a complete development and deployment platform managed by Oracle. Database as a Service provides dedicated virtual machines with fully configured and running Oracle Database instances. Database Schema Service offers dedicated database schemas, RESTful web services for access to data, and a powerful declarative development and deployment environment for custom applications. Oracle Database Cloud Service enables businesses to reap all the benefits of the cloud including subscription-based, self-service access to reliable, scalable, and secure cloud environments.

Features

- Full capabilities of the Oracle Database, including SQL and PL/SQL support
- Dedicated virtual machine with pre-configured database instance or dedicated schema
- General purpose and high-memory compute shapes
- Flexible management options from self-managed to fully managed by Oracle
- Rapid provisioning and easy to use cloud tooling for simpler management
- Integrated Identity Management for user repository and single sign-on (SSO)

Instant Productivity, More Choice, Fewer Compromises

Oracle Database Cloud Service is designed to maximize and accelerate productivity. With the Oracle Database Cloud, businesses can gain instant access to cloud environments ready for application development, deployment, and built on the world's #1 database platform. The Oracle Database Cloud provides self-service tools to make the completion of development and database administration tasks faster and easier. In addition, the Oracle Database Cloud offers flexible database management options ranging from self-managed with full administrative control to fully managed by Oracle. With the Oracle Database Cloud, you get instant productivity, more choice, and fewer compromises.

THE STATE OF UTAH VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

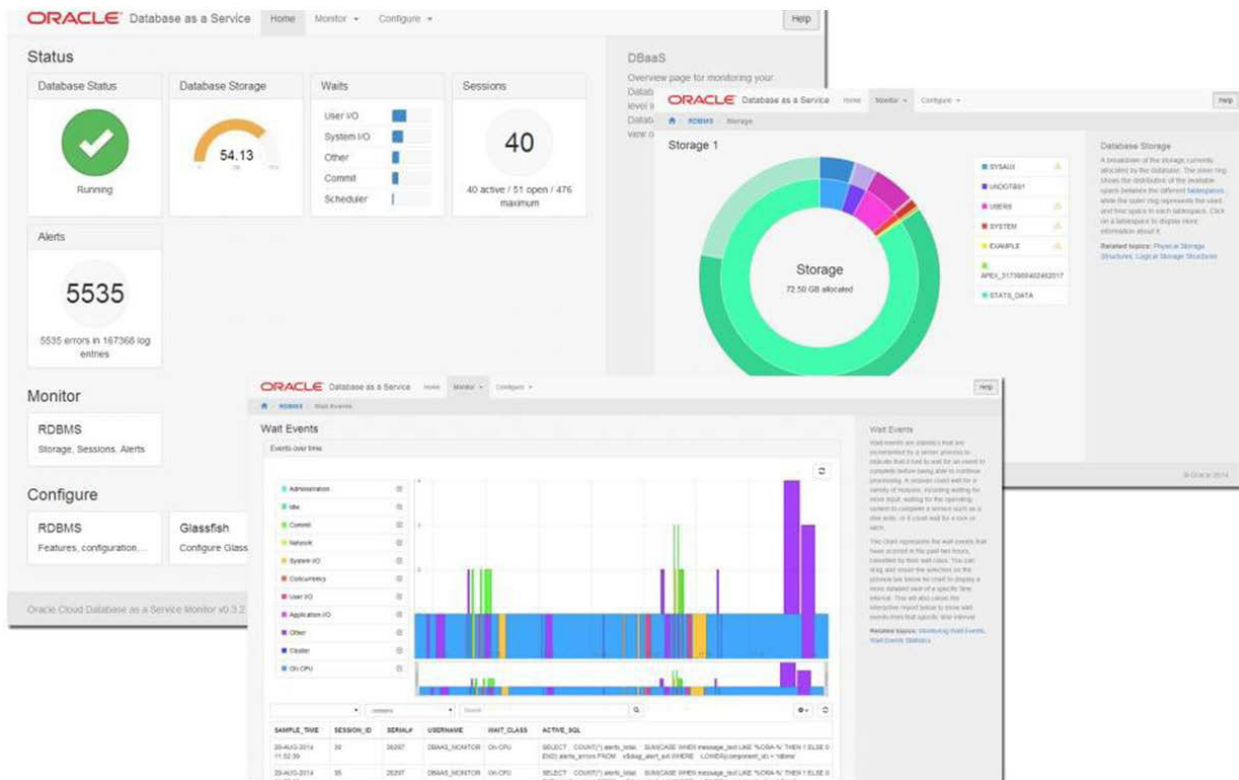


FIGURE 19: DATABASE AS A SERVICE MONITORING TOOL

Oracle Database

- Oracle Database 12c and 11g, including Standard Edition One, Enterprise Edition, Enterprise Edition High Performance, and Enterprise Edition Extreme Performance option bundles

Oracle Application Express

- Declarative, iterative development
- Utilities for browsing database objects and running SQL and scripts
- Tools for team-based development

RESTful Web Services

- Use SQL and PL/SQL for implementation
- Wizard-based definition
- Access to identity and other header information

Identity Management

- Secure applications
- User and role management
- Automatic single sign-on (SSO)

Database as a Service

Database as a Service provides dedicated virtual machines with pre-configured and running Oracle Database 12c or 11g instances. Database as a Service offers general purpose and high-memory compute shapes that provide the full power of the Oracle Database for any type of application, whether deploying production workloads or simply for development and testing. Businesses can also choose between different editions including Standard Edition One, Enterprise Edition (includes no Database Options), Enterprise Edition High Performance (includes most Database Options), or Enterprise Edition Extreme Edition (includes all Database Options).

Database as a Service is ideal for businesses that want a fully featured Oracle Database in the cloud, while retaining full administrative control such as root operating system and SYSDBA access. Database as a Service provides advanced cloud tooling for simpler management of the database including one-click automated backup with point-in-time recovery, one-click patching, and one-click upgrades. Database as a Service also supports a wide range of connectivity and access choices, including a comprehensive set of CLI (command line interfaces) for typical administration tasks and network access via SSH, SQL*Net, JDBC, web, HTTPS, and other drivers. There is also support for development and administrative tools such as Oracle Application Express, SQL Developer, Data Pump, SQL*Plus, and more.

Database as a Service includes a provisioning wizard to quickly and easily create new database instances, advanced cloud tooling to back up and restore database instances and related configuration and system files, utilities to automate database patching, and a local monitoring application that provides a wide set of controls and information about the Oracle Database.

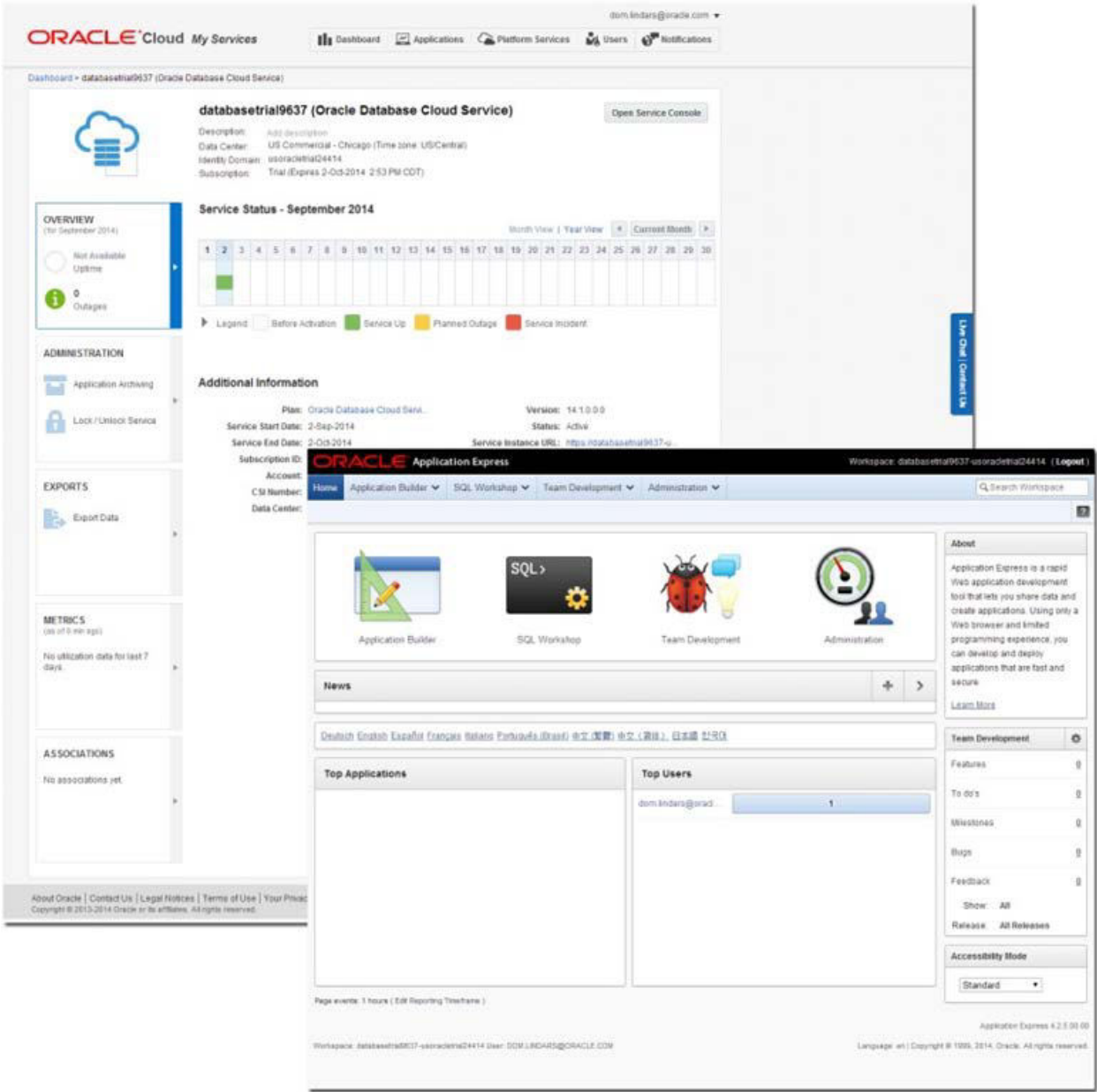


FIGURE 20: DATABASE SCHEMA SERVICE CLOUD PORTAL AND APEX

Database Schema Service

Database Schema Service is designed to maximize and accelerate productivity by providing instant access to dedicated database schemas in cloud environments ready for application development and deployment. With dedicated schemas, each businesses data is completely isolated to ensure data security. Use Oracle Application Express to quickly create robust, scalable business applications, modify them in real-time, and deploy them instantly for access from any web browser or mobile device.

The Database Schema Service includes tools to load data, develop, and run SQL and PL/SQL, browse data and data structures, and facilitate team development. The Schema Service also includes a wizard-driven interface to create RESTful web services that can call any SQL statement or PL/SQL code and return values in JSON format, CSV format, or any format you wish to create. Once created, these web services provide secure access to your data through a unique URI.

The entire development and deployment architecture of the Database Schema Service is contained within the Oracle Database. As a result, applications and RESTful web services can be moved to any other Oracle Database, whether on premise or in other clouds. This portability protects investments deployed in Oracle Cloud and enables businesses to extend the Oracle Database Cloud Service in virtually any way.

Enterprise-grade Cloud for Any Business

As part of the Oracle Cloud, the Oracle Database Cloud Service is deployed on enterprise-grade infrastructure that includes generic x86 Compute resources or Oracle Exadata for extreme performance and availability, triple mirroring of storage for data redundancy, full system backup and restore, datacenters in multiple geographic locations, and industrial strength physical and logical security.

Furthermore, Oracle Cloud is backed by 24/7 multi-lingual Support to ensure customers' needs in various regions are met.

Whether your business needs the flexibility and control of a dedicated database instance or the simplicity of a dedicated database schema that is fully managed by Oracle, the Oracle Database Cloud Service has your needs covered

10. CONCLUSION

Thank you again to your team for issuing this RFP. We welcome the opportunity to meet with you, demonstrate our solution, and discuss our implementation experience relevant to you on this important project. We believe the solution set described in this RFP will provide your team (both technical and non-technical) with the most comprehensive suite of tools to service those in need and while working through evaluations and determinations in the fastest, most convenient and consistent business manner. We are the only solution that provides policy automation functionality through natural language.

There are several differences between Oracle's solution Platform with Policy Automation and other solutions.

- Ability to transform policy documents (legislation, regulation, policy) directly to executable form. This breaks the standard requirements bottleneck, where teams get stuck in "analysis paralysis" trying to take the traditional approach of defining a data model from thousands of pages of policy and then attempting to express policy rules in technical or code formats.
- Ability for policy experts to work directly with rules, using familiar tools (Word, Excel) in natural language.
- Ability to see clearly and at-a-glance that the rules implemented in the system match the policy. This is achieved by retaining the same language and structure as the original policy material throughout the rule lifecycle.
- Ability to simulate future policy changes, to see the impact on the citizen base, and to very rapidly implement changes.

- Ability to process against multiple versions of rules; for example, retaining rules for multiple years, and also multiple versions of customer circumstances; for example, when incomes and family structures change; and to do this without requiring custom code to aggregate the results from each version of the rules and circumstances. The solution needs to be able to process transactions that span multiple versions of both rules and circumstances.
- Ability to write the rules once and deploy them many times, for example, the same rules in standalone web self-service and positioned as an enterprise service that can be called by any application
- The ability to offer service access to case members and citizens alike, on any device, at any time.
- True end to end case management where every system interaction leaves an audit trail.
- Multiple Cloud Deployment opportunities including, Government and DoD Clouds that are FedRAMP JAB and FedRAMP+ certified respectively.

6B. Technical Requirements Compliance (RFP #8)

Provided below is the information requested in section 8 of the RFP.

A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

8 TECHNICAL REQUIREMENTS

If applicable to an Offeror's Solution, an Offeror must provide a point by point responses to each technical requirement demonstrating its technical capabilities. If a technical requirement is not applicable to an Offeror's Solution then the Offeror must explain why the technical requirement is not applicable.

If an Offeror's proposal contains more than one Solution (i.e., SaaS and PaaS) then the Offeror must provide a response for each Solution. However, Offerors do not need to submit a proposal for each Solution.

Technical Requirements (RFP #8.1)

Provided below is the information requested in section 8.1 of the RFP.

8.1.1 Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

Oracle Response:

CLOUD SERVICE MODELS

The two proposed cloud computing services models are the following.

- **Software as a Service (SaaS)** – The service provider offers one or more applications over the network to be customized (where possible) and used by its customers.
- **Platform as a Service (PaaS)** – The service provider offers development and deployment platforms over the network to be used by customers building or assembling their own applications using these provided frameworks.

DEPLOYMENT MODELS

The four cloud computing deployment models include:

- **Public Cloud** – An environment provisioned for open use by the general public.
- **Private Cloud** – An environment provisioned for exclusive use by a single organization comprising multiple (internal) consumers. Sometimes called an enterprise cloud, private clouds can be on premise or off premise, managed internally or managed by a third-party provider.
- **Community Cloud** – An environment provisioned for exclusive use by a specific community of consumers from different organizations that share business or computing goals, needs or concerns.
- **Hybrid Cloud** – An environment comprised of two or more of the above specified cloud computing deployment models in a manner where they are bound together using technology that supports application, service or data portability, migration, and interoperability.

8.1.2 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the following characteristics, as defined in NIST Special Publication 800-145:

8.1.2.1 NIST Characteristic - On-Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.

Oracle Response:

Oracle's Cloud Computing offerings can be easily mapped to the NIST definition for cloud computing, as shown in Figure 21 below. When used together or with interoperable third-party software, these products help satisfy customer requirements for self-service, elasticity, resource pooling, network accessibility, and measured service. These products can be assembled to form private cloud architectures, used in conjunction with Oracle or third-party public cloud services or combined to create hybrid cloud architectures.

Oracle Cloud Offerings – Complete Choice

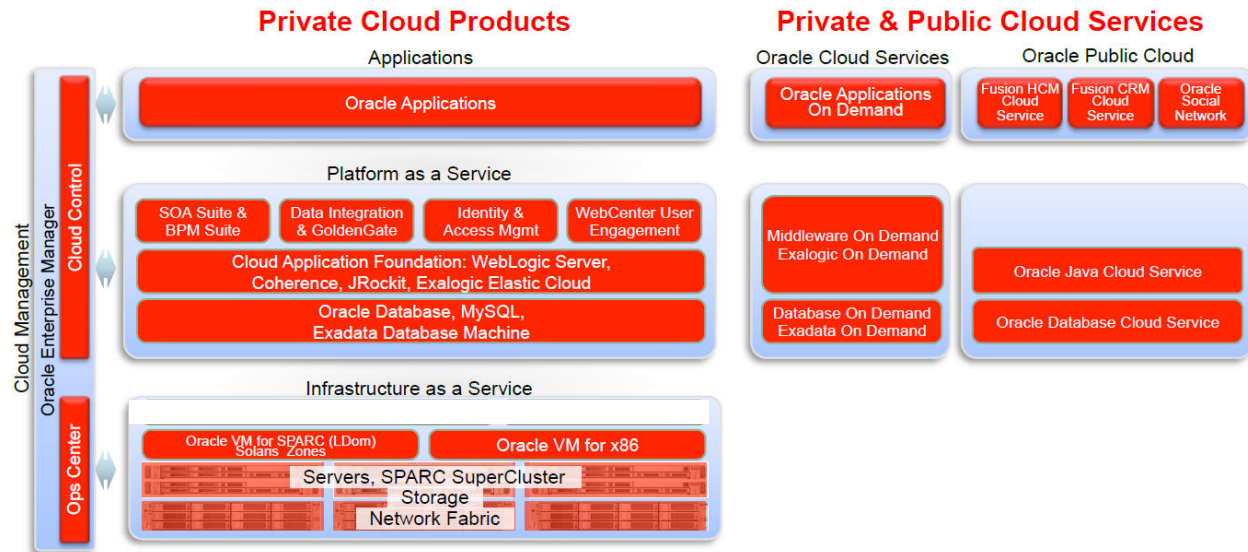


FIGURE 21: OVERVIEW OF ORACLE CLOUD SOLUTION

8.1.2.2 NIST Characteristic - Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.

Oracle Response:

All a user needs to access Oracle Cloud Service is a certified web browser – such as Internet Explorer, Firefox or Safari—and a working internet connection. Any computer system configuration capable of running a certified browser can access Oracle Cloud Services.

In addition, where applicable, Oracle offers a LAN-to-LAN IPSEC based software VPN connection following for the encryption of all data between Oracle’s data center firewalls, where Oracle Cloud Services are hosted, and the customer's firewall. This is an optional service and may be purchased at additional price.

Yes, please refer to section 4 of Attachment 7.2, our Oracle Cloud Enterprise Hosting and Delivery Policies. The most recent copy of this living document is always available <http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

In addition, the Oracle Service Cloud has been FedRAMP JAB Certified. JAB Provisional Authorizations: Cloud systems listed under the FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs.

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30% to 40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), **National Institute of Standards and**

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

8.1.2.3 NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.

Oracle Response:

A virtualized and clustered grid computing architecture is often the basis for PaaS offerings, because grid provides the necessary elastic scalability and resource pooling.

Please refer to section 4 of Attachment 7.2, our Oracle Cloud Enterprise Hosting and Delivery Policies. The most recent copy of this living document is always available
<http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

In addition, the Oracle Service Cloud has been FedRAMP JAB Certified. JAB Provisional Authorizations: Cloud systems listed under the FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs.

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30% to 40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), **National Institute of Standards and Technology (NIST)**, Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

8.1.2.4 NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.

Oracle Response:

A virtualized and clustered grid computing architecture is often the basis for PaaS offerings, because grid provides the necessary elastic scalability and resource pooling.

Please refer to section 4 of Attachment 7.2, our Oracle Cloud Enterprise Hosting and Delivery Policies. The most recent copy of this living document is always available
<http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

In addition, the Oracle Service Cloud has been FedRAMP JAB Certified. JAB Provisional Authorizations: Cloud systems listed under the FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30% to 40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

8.1.2.5 NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.

Oracle Response:

Yes, the proposed solution satisfies this NIST characteristic. Please refer to section 4 of Attachment 7.2, our Oracle Cloud Enterprise Hosting and Delivery Policies. The most recent copy of this living document is always available <http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

In addition, the Oracle Service Cloud has been FedRAMP JAB Certified. JAB Provisional Authorizations: Cloud systems listed under the FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs.

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30 to 40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), **National Institute of Standards and Technology (NIST)**, Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

MEASUREMENT OF AVAILABILITY

Following the end of each calendar month of the services period under an ordering document, Oracle measures the system availability level over the immediately preceding month. Oracle measures the system availability level by dividing the difference between the total number of minutes in the monthly measurement period and any unplanned downtime by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure.

REPORTING OF AVAILABILITY

Oracle will provide customer with access to a Customer Notifications Portal. This portal will provide metrics on the system availability level for Cloud Services purchased under the ordering document. For those Cloud Services for which such metrics are not available via the Customer Notifications Portal, Oracle will provide metrics on the system availability level upon receipt of a service request submitted by customer to Oracle requesting the metrics.

MONITORING

Oracle uses a variety of software tools to monitor (i) the availability and performance of customer's production services environment and (ii) the operation of infrastructure and network components.

MONITORED COMPONENTS

Oracle monitors the service infrastructure, and currently generates alerts for CPU, memory, storage, database, network components, and transactions. Oracle's Operations staff attends to any automated warnings and alerts associated with deviations of the environment from Oracle-defined monitoring thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

8.1.3 Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

Oracle Response:

ORACLE SERVICE CLOUD

Oracle Service Cloud, the customer experience suite, will help you by delivering superior customer experiences across Web, social, and contact center touch points.

Oracle Service Cloud Web Experience seamlessly integrates into an existing Web infrastructure for a fully branded online customer experience. When customers visit a Web site, they should be able to quickly and easily find what they're looking for. The Web experience must be interactive, engaging, and branded to create "stickiness." A great Web experience should also allow a customer to seamlessly transition across Web self-service, agent online, mobile devices, and telephone assistance based on their needs.

Oracle Service Cloud Social Experience taps social networking to promote brands, facilitate community, address customer concerns, and drive trust. Opinions are being formed and decisions being made about you without your involvement - on social networking sites like YouTube, Twitter, and Facebook, and on blogs and in online communities. Agencies need to have a presence on the social Web, must engage with customers through corporate-sponsored communities, and must take advantage of the power of the social Web rather than be at its mercy.

Oracle Service Cloud Contact Center Experience enables end-to-end management of the customer experience by unifying customer data, contextual knowledge, and interaction channels. Your agents are equipped to consistently deliver better customer experiences across channels.

Oracle Service Cloud Engage enables organizations to deliver the voice of the customer across the Web, social, and contact center experiences. Paired with Engage's analytics engine, it delivers deep customer insights and enables proactive, relevant customer communications, which builds loyalty and drives trust.

Underlying Oracle Service Cloud is the Oracle Service Cloud CX Platform. The platform includes Oracle Service Cloud's innovative self-learning knowledge foundation which infuses every customer interaction with relevant and consistent knowledge to provide the basis for a positive customer experience. Oracle Service Cloud Connect provides the integration framework to easily connect Oracle Service Cloud with other systems. The entire Oracle Service Cloud leverages a mission-critical SaaS (Software as a Service) delivery model to guarantee unparalleled up-time, security, and performance.

ORACLE DATABASE CLOUD SERVICE

Oracle Database Cloud Service provides the power and flexibility of the Oracle Database in the cloud with your choice of a dedicated database instance with full administrative control, or a dedicated schema with a complete development and deployment platform managed by Oracle. Database as a Service provides dedicated virtual machines with fully configured and running Oracle Database instances. Database Schema Service offers dedicated database schemas, RESTful web services for access to data, and a powerful declarative development and deployment environment for custom applications. Oracle Database Cloud Service enables businesses to reap all the benefits of the cloud including subscription-based, self-service access to reliable, scalable, and secure cloud environments.

FEATURES

- Full capabilities of the Oracle Database, including SQL and PL/SQL support
- Dedicated virtual machine with pre-configured database instance or dedicated schema
- General purpose and high-memory compute shapes
- Flexible management options from self-managed to fully managed by Oracle
- Rapid provisioning and easy to use cloud tooling for simpler management
- Integrated Identity Management for user repository and single sign-on (SSO)

INSTANT PRODUCTIVITY, MORE CHOICE, FEWER COMPROMISES

Oracle Database Cloud Service is designed to maximize and accelerate productivity. With the Oracle Database Cloud, businesses can gain instant access to cloud environments ready for application development, deployment, and built on the world's #1 database platform. The Oracle Database Cloud provides self-service tools to make the completion of development and database administration tasks faster and easier. In addition, the Oracle Database Cloud offers flexible database management options ranging from self-managed with full administrative control to fully managed by Oracle. With the Oracle Database Cloud, you get instant productivity, more choice, and fewer compromises.

THE STATE OF UTAH VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

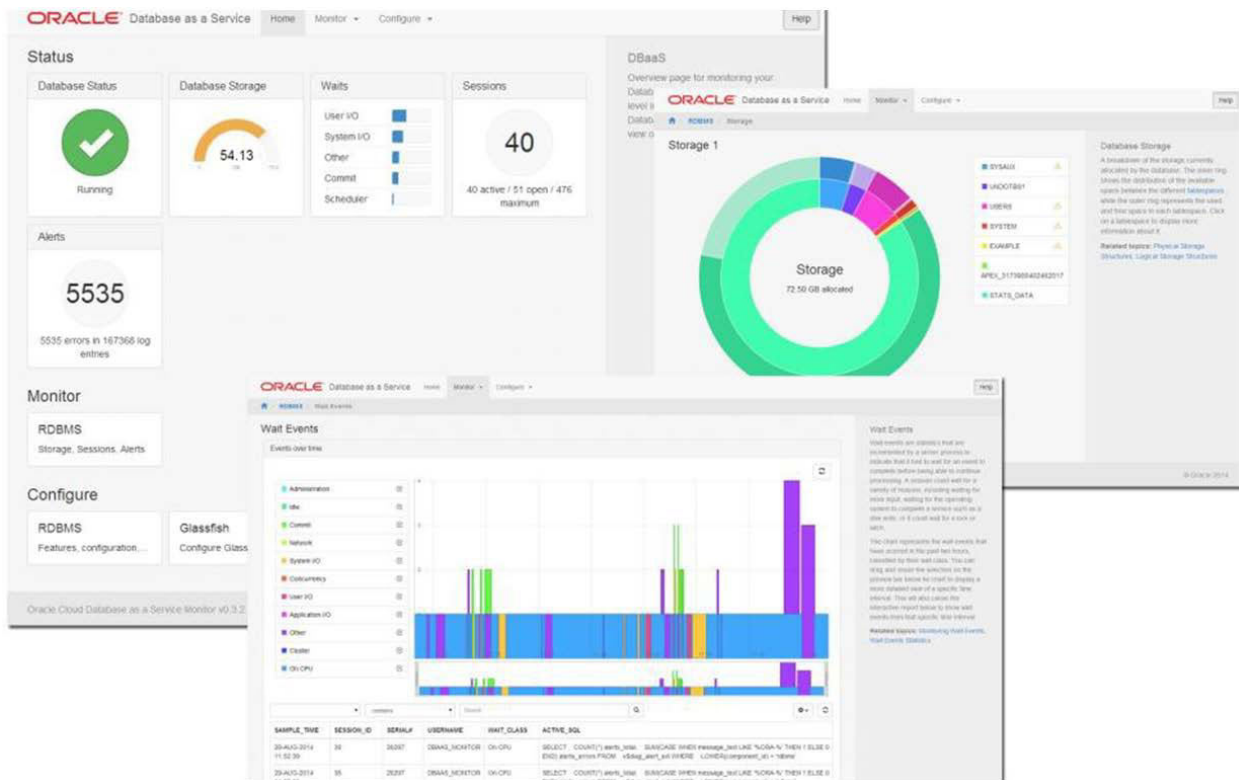


FIGURE 22: DATABASE AS A SERVICE MONITORING TOOL

Oracle Database

- Oracle Database 12c and 11g, including Standard Edition One, Enterprise Edition, Enterprise Edition High Performance, and Enterprise Edition Extreme Performance option bundles

Oracle Application Express

- Declarative, iterative development
- Utilities for browsing database objects and running SQL and scripts
- Tools for team-based development

RESTful Web Services

- Use SQL and PL/SQL for implementation
- Wizard-based definition
- Access to identity and other header information

Identity Management

- Secure applications
- User and role management
- Automatic single sign-on (SSO)

DATABASE AS A SERVICE

Database as a Service provides dedicated virtual machines with pre-configured and running Oracle Database 12c or 11g instances. Database as a Service offers general purpose and high memory compute shapes that provide the full power of the Oracle Database for any type of application, whether deploying production workloads or simply for development and testing. Businesses can also choose between different editions including Standard Edition One, Enterprise Edition (includes no Database Options), Enterprise Edition High Performance (includes most Database Options), or Enterprise Edition Extreme Edition (includes all Database Options).

Database as a Service is ideal for businesses that want a fully featured Oracle Database in the cloud, while retaining full administrative control such as root operating system and SYSDBA access. Database as a Service provides advanced cloud tooling for simpler management of the database including one-click automated backup with point-in-time recovery, one-click patching, and one-click upgrades. Database as a Service also supports a wide range of connectivity and access choices, including a comprehensive set of CLI (command line interfaces) for typical administration tasks and network access via SSH, SQL*Net, JDBC, web, HTTPS, and other drivers. There is also support for development and administrative tools such as Oracle Application Express, SQL Developer, Data Pump, SQL*Plus, and more.

Database as a Service includes a provisioning wizard to quickly and easily create new database instances, advanced cloud tooling to back up and restore database instances and related configuration and system files, utilities to automate database patching, and a local monitoring application that provides a wide set of controls and information about the Oracle Database.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

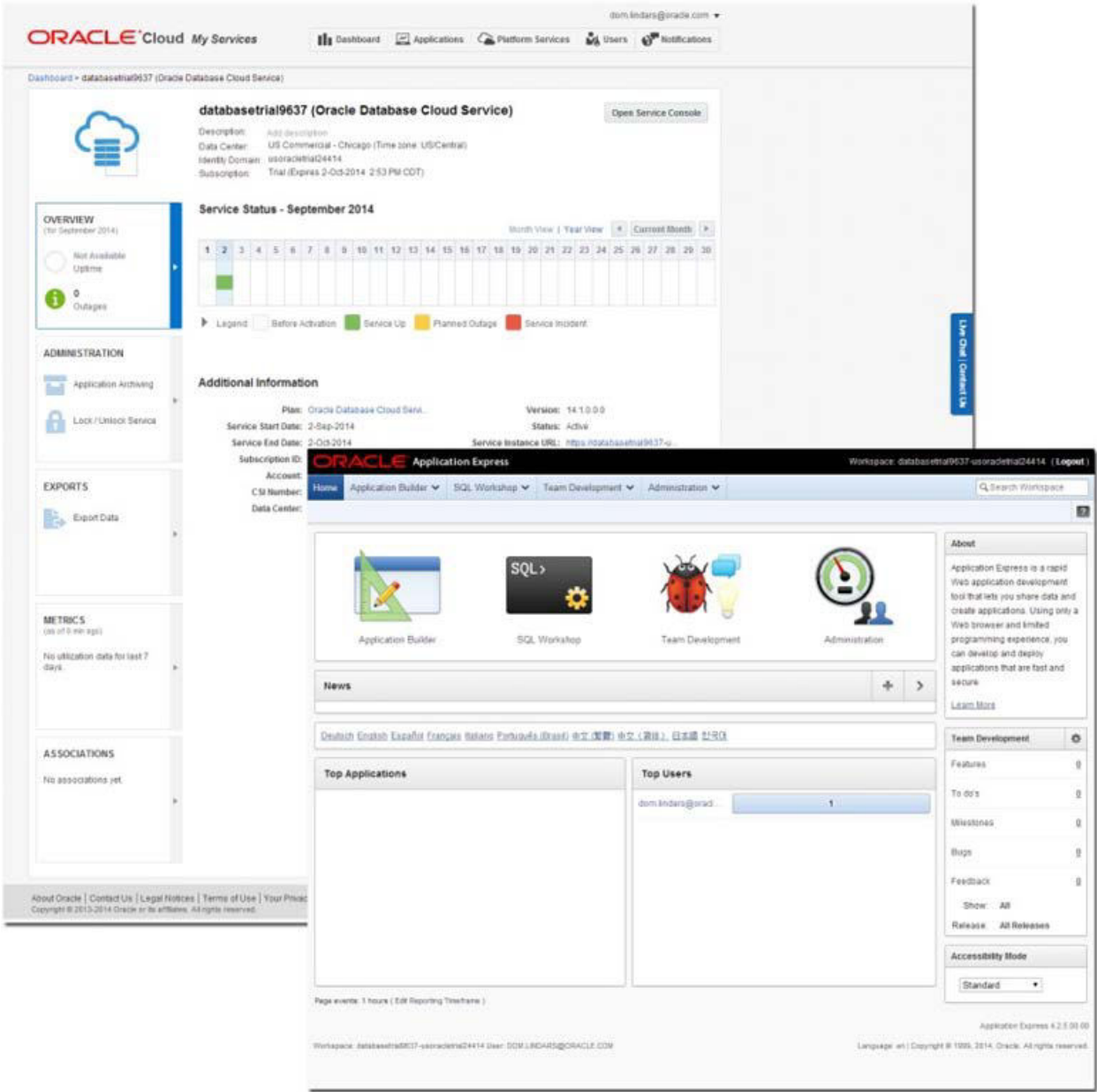


FIGURE 23: DATABASE SCHEMA SERVICE CLOUD PORTAL AND APEX

DATABASE SCHEMA SERVICE

Database Schema Service is designed to maximize and accelerate productivity by providing instant access to dedicated database schemas in cloud environments ready for application development and deployment. With dedicated schemas, each businesses data is completely isolated to ensure data security. Use Oracle Application Express to quickly create robust, scalable business applications, modify them in real-time, and deploy them instantly for access from any web browser or mobile device.

The Database Schema Service includes tools to load data, develop and run SQL and PL/SQL, browse data and data structures, and facilitate team development. The Schema Service also includes a wizard-driven interface to create RESTful web services that can call any SQL statement or PL/SQL code and return values in JSON format, CSV format, or any format you wish to create. Once created, these web services provide secure access to your data through a unique URI.

The entire development and deployment architecture of the Database Schema Service is contained within the Oracle Database. As a result, applications and RESTful web services can be moved to any other Oracle Database, whether on premise or in other clouds. This portability protects investments deployed in Oracle Cloud and enables businesses to extend the Oracle Database Cloud Service in virtually any way.

ENTERPRISE-GRADE CLOUD FOR ANY BUSINESS

As part of the Oracle Cloud, the Oracle Database Cloud Service is deployed on enterprise-grade infrastructure that includes generic x86 Compute resources or Oracle Exadata for extreme performance and availability, triple mirroring of storage for data redundancy, full system backup and restore, datacenters in multiple geographic locations, and industrial strength physical and logical security.

Furthermore, Oracle Cloud is backed by 24/7 multi-lingual Support to ensure customers' needs in various regions are met.

Whether your business needs the flexibility and control of a dedicated database instance or the simplicity of a dedicated database schema that is fully managed by Oracle, the Oracle Database Cloud Service has your needs covered.

8.1.4 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

Oracle Response:

Please see our detailed response on meeting NIST requirements found in our response to RFP section 8.1.2 above.

8.1.5 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

Oracle Response:

Please see our detailed response on meeting NIST requirements found in our response to RFP section 8.1.2 above.

Subcontractors (RFP #8.2)

Provided below is the information requested in section 8.2 of the RFP.

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of subcontractors. Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified subcontractors. Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific subcontractors. Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must

also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. SubcontractorSubcontractors do not need to comply with Section 6.3.

Oracle Response:

The cloud services described in Oracle's response are provided by Oracle. Customers have a choice of selecting their own implementation provider, either using Oracle Consulting Services (OCS) or implementing directly with one of our comprehensive partners described in this section below.

Oracle has built a comprehensive partner community with more than 25,000 partners worldwide. The Oracle Partner Network is a global program that manages Oracle's business relationships with this large, broad-based network of partners, including independent software and hardware vendors, system integrators, and resellers that deliver innovative solutions and services based upon Oracle's product offerings. Oracle customers can find a partner with the knowledge, experience, and commitment to help their business succeed. Oracle can help customers locate, secure, and retain the right partner to develop and implement business solutions for the specific needs of their business. Types of partners include the following:

- Applications Hosting Services
- Education Services Provider
- Hardware Resellers
- Independent Software Supplier
- Independent Software Vendor (ISV)
- Managed Service Provider
- Management Consultancy
- Original Equipment Manufacturer (OEM)
- Service Partners
- Software License Reseller
- Support Services Provider
- System Integrators (SI)
- Value Added Distributor (VAD)
- Value Added Reseller (VAR)

More information including a listing of partners is provided at <http://www.oracle.com/partners/index.html>.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Oracle Response:

Oracle does not anticipate the use of a subcontractor at this point.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Oracle Response:

Not applicable at this time.

Working with Purchasing Entities (RFP #8.3)

Provided below is the information requested in section 8.3 of the RFP.

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- **Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;**
- **Response times;**
- **Processes and timelines;**
- **Methods of communication and assistance; and**
- **Other information vital to understanding the service you provide.**

Oracle Response:

WORKING WITH PURCHASING ENTITIES- GENERAL

The Oracle Account team is comprised of sales professional and engineers who will be the primary interface with customers for needs assessment and scoping the cloud services. The Contracts Manager will handle operational requirements and be engaged with the Participating Entities as described in Oracle's response in Section 5 above to RFP Section 7.

WORKING WITH PURCHASING ENTITIES- DURING A SECURITY INCIDENT

There are detailed steps in monitoring and reporting incidents that are most effectively read in context with one another on the Oracle Cloud Enterprise Hosting and Delivery Policies, specifically sections 1, 2, 3, 4, and 6.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Oracle Response:

The customer is in control of its data in the cloud environment at all times. Oracle has well established policies with regard data handling and communication protocols as described in the

Oracle Cloud Enterprise Hosting and Delivery Policies, specifically sections 1, 2, 3, 4, and 6 for detailed information.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

Oracle Response:

Test sites (a clone of your existing production site) are available for an additional fee. Any information loaded into the test site or any configuration performed on the test site is not transferred back to the production site automatically. However, during an upgrade, an upgrade test site is created (at no

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

additional fee). The upgrade test site can be used for training purposes and some pre-configuration work. Some configuration procedures performed are automatically transferred back to the production site when the production site is upgraded.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are be accessible to people with disabilities, and must comply with Participating entity accessibility policies and the Americans with Disability Act, as applicable.

Oracle Response:

Oracle agrees to review with the Participating Entities their requirements but offers the preceding general information.

The extent to which an Oracle product is, at the time of delivery, capable of providing comparable access to individuals with disabilities consistent with the applicable provisions of the Architectural and Transportation Barriers Compliance Board standards set out in 36 CFR Part 1194 (known as 'Section 508'), in effect as of the date of this Agreement, is indicated by the comments and exceptions (some of which may be significant, if any) noted on the applicable Voluntary Product Accessibility Templates (VPAT) available at www.oracle.com/accessibility for each product, when they are used in accordance with Oracle's associated documents and other written information, and provided that any assistive technologies and any other products used with them properly interoperate with them. In the event that no VPAT is available for a particular Oracle product, please contact the Oracle Accessibility Program Office at accessible_ww@oracle.com. In some cases, the outcome may be that a product is still being evaluated for accessibility, may be scheduled to meet accessibility standards in a future release, or may not be scheduled to meet accessibility standards at all. No other terms, conditions, statements or any other such representations regarding or related to accessibility shall apply to the Oracle products provided under this agreement.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

Oracle Response:

The following web browsers are supported by Customer Portal's standard page set.

TABLE 1: MINIMUM REQUIREMENTS FOR WEB BROWSERS

Browser	Supported Version(s)
Microsoft Internet Explorer	11.0, Edge
Google Chrome	46 or newer
Mozilla Firefox	41 or newer
Apple Safari	9.0

RESTRICTIONS

- Mac/Safari is not supported by the Oracle Knowledge Cloud Service (OKCS) feature of the Service Cloud
- The browser text size must be set to normal.
- Using versions of web browsers that are not listed in this table will result in malfunction.
- Windows/Safari is only supported by the OKCS feature of Service Cloud

ORACLE®

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Oracle Response:

The Oracle Account team is comprised of sales professional and engineers who will be the primary interface with customers for needs assessment and scoping the cloud services. Each customer has different considerations and requirements that align with their overall technology objectives, budget use cases and regulations. The Oracle Account team will perform an assessment with each perspective Participating Entity to gain an understanding of their goals which may include:

- Reducing facilities/real estate cost
- Reducing technical support fees
- Investment in on premise licenses; do they have a value that can be shelved/exchanged to reduce the cost of a cloud solution
- Regulatory requirements

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Oracle Response:

While we anticipate that this project will be implemented by an Oracle solution partner if Oracle's solution is selected, we will provide the Oracle based methodology as a baseline.

Oracle's solution project methodology provides an overarching methodology for implementing any of our solution's products or services, regardless of size or complexity, and activities are tailored to specific project needs. Our goal is to be as thorough as possible, while achieving collaboration, speed, effectiveness, and overachievement.

- **Plan** – We collaborate with you to establish the direction of the project introducing project teams, validating the project scope, outlining the business objectives, developing the project plan/timeline, and establishing measures and baselines for the project.
- **Design** – We collaborate with you to establish the direction of the project introducing project teams, validating the project scope, outlining the business objectives, developing the project plan/timeline and establishing measures and baselines for the project.
- **Configure** – Oracle RightNow Professional Services consultants and/or application engineers work with you to configure, integrate, and/or customize the solution based on the design. In addition to standard configuration activities, other set-up tasks such as data imports, integrations to third-party applications to data share; and customization may be performed to support your requirements.
- **Test** – The test phase is a verification period for all parties to confirm that the system has been set up according to the requirements and design. The Oracle RightNow project team performs a range of system tests before your project team engages in user acceptance testing.

- **Deploy** – During the deploy phase, Oracle works with you to ensure a smooth launch of your solution into production. Marked by a go-live project milestone, your solution is promoted to a production environment, ready for use.
- **Results** – After deploying to production, we measure project success by mapping back to your project goals and objectives. We are committed to a continued partnership with you and will support you as your business needs grow and expand.

Your OCX project manager will work with you to develop a detailed project plan and timeline for your specific implementation.

When implementing our solution, it is vital to set up an active project team to plan for the significant actions to be taken through the project’s execution. This active and complete project team ensures a successful, timely, and budgeted solution implementation. It is not necessary to have one person per team role; however, it is important to have each role filled.

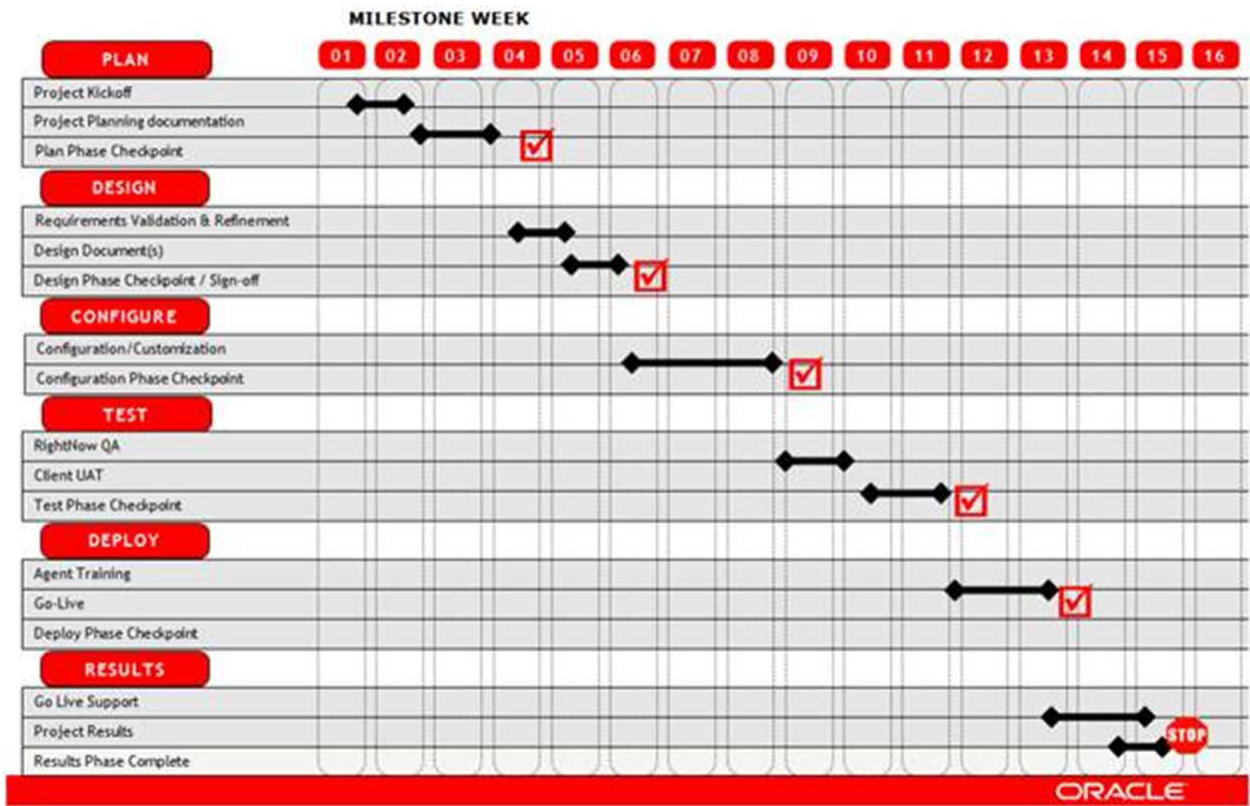


FIGURE 24: SAMPLE PROJECT TIMELINE

The project team is not only needed during the initial implementation but throughout the process to assist in maintaining the knowledgebase moving forward. We recommend regular meetings with the project team to review site statistics and determine improvement that can continue to be made.

- **Project Sponsor** – an executive or director who helps with project team direction and escalates issues when needed.
- **Project Manager** – ensures the product is released quickly and that the team members complete their tasks in conjunction with the project plan.

- **RightNow Administrator** – performs the majority of the configuration on the product for the release.
- **Knowledgebase Engineer** – ensures that the knowledgebase is being maintained and is always up to date. The knowledgebase engineer is normally a full-time position, depending on the size of your knowledgebase.

Customer Service (RFP #8.4)

Provided below is the information requested in section 8.4 of the RFP.

8.4.1 Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include:

- **Quality assurance measures;**
- **Escalation plan for addressing problems and/or complaints; and**
- **Service Level Agreement (SLA).**

Oracle Response:

Oracle has provided its documents that describe our Oracle Cloud Enterprise Hosting and Delivery Policies, (sections 4 and 6 specifically) found in Attachment 7.2.

In addition:

ISO 27002 CERTIFICATE OF CONFORMANCE

Oracle Cloud Services has received the ISO 27002 Certificate of Conformance. ISO/IEC 27002 is an internationally recognized standard that assists organizations with selecting and applying controls to information security.

Information technology, and provides a framework that takes into account legal, regulatory and contractual requirements.

ISO 27001 CERTIFICATION FOR THE INFORMATION SECURITY SYSTEM

Oracle Cloud Services Risk Management's On Demand Security Services team has been granted an ISO 27001 Certification for its staff, technology, and processes. Product information is provided at: <https://www.oracle.com/cloud/managed-cloud.html>.

ISO 14001 CERTIFICATION (ENVIRONMENTAL AND ENERGY)

Oracle's hardware manufacturing facilities maintained their ISO 14001 certifications.

The following Oracle locations are certified to the ISO 14001:2004 standard: Hillsboro, Oregon, Louisville, Colorado and Morrisville, North Carolina. Objectives and targets at Oracle certified locations are designed to ensure environmental protection and increased operational efficiency and include solid waste reduction and enhanced management of air, water, and waste controls. Further information is provided at: <http://www.oracle.com/us/products/applications/green/ehsms-184396.html>.

IS9001 QUALITY MANAGEMENT SYSTEM

Oracle has a dedicated Global Quality Programs team and is IS9001 certified across all product lines throughout all regions.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.

Oracle Response:

b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.

c. Customer Service Representative will respond to inquiries within one business day.

d. You must provide design services for the applicable categories.

e. You must provide Installation Services for the applicable categories.

Oracle Response:

Oracle Support Services for Oracle Cloud consists of:

- Diagnosis of problems or issues with the Oracle Cloud Services
- Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud services so that they perform in all material respects as described in the associated Program Documentation
- Support during Change Management activities described in the Oracle Cloud Change Management Policy
- Assistance with technical Service Requests 24/7
- 24/7 access to a Cloud Customer Support Portal designated by Oracle (for example, My Oracle Support) and Live
- Telephone Support to log Service Requests
- Access to community forums
- Non-technical Customer service assistance during normal Oracle business hours (8:00 to 17:00) local time.

LIVE TELEPHONE SUPPORT

Customer's technical contacts may access live telephone support via the phone numbers and contact information found on Oracle's support web site at <http://www.oracle.com/support/contact.html> or such other address designated by Oracle for the applicable Cloud Services ordered.

RESPONSE TIME

Every attempt is made to return technical support calls as quickly as possible. Oracle will make reasonable efforts to respond to Severity 1 service requests within one hour. (A Severity 1 problem causes complete loss of service). In addition, Premier Support provides 24/7 coverage on Severity 1 issues until the issue is resolved or as long as useful progress can be made.

For further information refer to Technical Support Policies documents available at:
<http://www.oracle.com/us/support/policies/index.html>.

Security of Information (RFP #8.5)

Provided below is the information requested in section 8.5 of the RFP.

- 8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.**
- 8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.**
- 5.6.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.**

Oracle Response:

The following response is excerpted from Attachment 7.2, "Oracle Cloud Enterprise Hosting and Delivery Policies."

1. ORACLE'S CLOUD SECURITY POLICY

1.1 User Encryption for External Connections

Customer access to the system is through the Internet. TLS encryption technology is available for Oracle Cloud Service access. TLS connections are negotiated for at least 128 bit encryption or stronger. The private key used to generate the cipher key is at least 2048 bits. TLS is implemented or configurable for all web-based TLS certified applications deployed at Oracle. It is recommended that the latest available browsers certified for Oracle programs, which are compatible with higher cipher strengths and have improved security, be utilized for connecting to web enabled programs. The list of certified browsers for each version of Oracle programs can be found on the Cloud Customer Support Portal designated by Oracle for the specific service ordered (for example, the My Oracle Support portal). In some cases, a third-party site used with cloud services and not under the control of

Oracle may force a non-encrypted connection. In some cases, a third party site that Customer wishes to integrate with the Cloud Service may not accept an encrypted connection. For Cloud Services where HTTP connections with the third party site are permitted by Oracle, Oracle will enable such HTTP connections in addition to the HTTPS connection.

1.2 Network Access Control

Oracle Cloud operations teams access Customer environments through a segregated network connection, which is dedicated to environment access control and isolated from Oracle's internal corporate network traffic. Authentication, authorization, and accounting are implemented through standard security mechanisms designed to ensure that only approved operations and support engineers have access to the systems.

1.3 Network Bandwidth and Latency

Oracle is not responsible for Customer's network connections or for conditions or problems arising from or related to Customer's network connections (for example, bandwidth issues, excessive latency, network outages), or caused by the internet. Oracle monitors its own networks and will work to address internal issues that may impact availability.

1.4 Anti-Virus Controls

Oracle Cloud employs anti-virus software to scan uploaded files when deemed necessary by Oracle. Virus definitions are updated daily.

1.5 Firewalls

Oracle Cloud Services use firewalls to control access between the internet and Oracle Cloud Services by allowing only authorized traffic. Oracle managed firewalls are deployed in a layered approach to perform packet inspection with security policies configured to filter packets based on protocol, port, source, and destination IP address, as appropriate, in order to identify authorized sources, destinations, and traffic types.

1.6 System Hardening

Oracle employs standardized system hardening practices across Oracle Cloud devices. This includes restricting protocol access, removing or disabling unnecessary software and services, removing unnecessary user accounts, patch management, and logging.

1.7 Physical Security Safeguards

Oracle provides secured computing facilities for both office locations and production cloud infrastructure. Common controls between office locations and co-locations/datacenters currently include, for instance:

- Physical access requires authorization and is monitored.
- Everyone must visibly wear official identification while onsite
- Visitors must sign a visitor's register and be escorted and/or observed when on the premises
- Possession of keys/access cards and the ability to access the locations is monitored. Oracle employment must return keys/cards

Additional physical security safeguards are in place for all Oracle Cloud data centers, which currently include safeguards such as:

- Premises are monitored by CCTV
- Entrances are protected by physical barriers designed to prevent vehicles from unauthorized entry
- Entrances are manned 24 hours a day, 365 days a year by security guards who perform visual identity recognition and visitor escort management

1.8 System Access Control & Password Management

Access to Cloud systems is controlled by restricting access to only authorized personnel. Oracle enforces password policies on infrastructure components and cloud management systems used to operate the Oracle Cloud environment.

System access controls include system authentication, authorization, access approval, provisioning, and revocation for employees and any other Oracle-defined 'users'. Customer is responsible for all end user administration within the program. Oracle does not manage the Customer's End User accounts. Customer may configure the programs and additional built-in security features.

1.9 Review of Access Rights

Network and operating system accounts for Oracle employees are reviewed regularly to ensure appropriate employee access levels. In the event of employee terminations, Oracle takes prompt actions to terminate network, telephony, and physical access for such former employees. Customer is responsible for managing and reviewing access for its own employee accounts.

1.10 Security-Related Maintenance

Oracle performs security related change management and maintenance as defined and described in the Oracle Cloud Change Management Policy. For any security patch bundle that Oracle will deploy for designated Oracle Programs, Oracle will apply and test the security patch bundle on a stage environment of the applicable Cloud Service. Oracle will apply the security patch bundle to the production environment of the Cloud Service after Oracle successfully completes testing on the stage environment.

1.11 Data Management / Protection

During the use of Oracle Cloud services, Oracle Cloud Customers maintain control over and responsibility for their data residing in their environment. Oracle Cloud services provide a variety of configurable information protection services as part of the subscribed service. Customer data is data uploaded or generated for use within the Oracle Cloud Services.

1.11.1 Physical Media in Transit

Designated Oracle personnel handle media and prepare it for transportation according to defined procedures and only as required. Digital media is logged, encrypted, securely transported, and as necessary for backup archiving vaulted by a third-party offsite vendor. Vendors are contractually obligated to comply with Oracle-defined terms for media protection.

1.11.2 Data Disposal

Upon termination of services (as described in the Oracle Cloud Suspension and Termination Policy) or at Customer's request, Oracle will delete environments or data residing therein in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the environments or data.

1.11.3 Security Incident Response

Oracle evaluates and responds to incidents that create suspicions of unauthorized access to or handling of Customer data whether the data is held on Oracle hardware assets or on the personal hardware assets of Oracle employees and contingent workers. When Oracle's Global Information Security (GIS) organization is informed of such incidents, GIS defines escalation paths and response teams to address those incidents, depending on the nature of the activity. GIS will work with Customer, the appropriate technical teams, and law enforcement where necessary to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of the Customer's environment, and to establish root causes and remediation steps. Operations staff has documented procedures for addressing incidents where handling of data may have been unauthorized, including prompt and reasonable reporting, escalation procedures, and chain of custody practices.

If Oracle determines that Customer's data has been misappropriated, Oracle will report such misappropriation to Customer within 72 hours of making such determination, unless prohibited by law.

1.11.4 Data Privacy

Oracle's Data Processing Agreement for Oracle Cloud Services (Data Processing Agreement), and the Oracle Services Privacy Policy, describe Oracle's treatment of data that resides on Oracle systems (including personally identifiable information or "PII") to which Oracle may be provided access in connection with the provision of Cloud Services. The Data Processing Agreement specifically describes Oracle's and Customer's respective roles for the processing and control of personal data that Customer provides to Oracle as part of the Cloud Services. These documents are available at:

- Oracle Services Privacy Policy: <http://www.oracle.com/us/legal/privacy/services-privacy-policy-078833.html>
- Data Processing Agreement for Oracle Cloud Services: <http://www.oracle.com/dataprocessingagreement>

1.12 Regulatory Compliance

Oracle Cloud Services operate under Policies which are aligned with the ISO/IEC 27002 Code of Practice for information security controls, from which a comprehensive set of controls are selected, as described by ISO/IEC 27001.

The Information Security Management System Family of Standards (ISO/IEC 270xx) are published by ISO (the International Organization for Standardization) and the IEC (the International Electrotechnical Commission), and are a comprehensive reference for information security management, data protection and risk management for organizations of all types and sizes.

The internal controls of Oracle Cloud Services are subject to periodic testing by independent third-party audit organizations. Such audits may be based on the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization (SSAE 16), the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization (ISAE 3402), or such other third party auditing standard or procedure applicable to the specific Oracle Cloud Service. Audit reports of Oracle Cloud Services are periodically published by Oracle's third party auditors, although reports may not be available for all services or at all times. Customer may request to receive a copy of the current published audit report available for a particular Oracle Cloud Service.

The audit reports of Oracle Cloud Services, and the information they contain, are Oracle confidential information, and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to Oracle Cloud Services and are provided without any warranty.

Customer remains solely responsible for its regulatory compliance in its use of any Oracle Cloud Service. Customer must make Oracle aware of any technical requirements that result from its regulatory obligations prior to contract signing. Some Oracle Cloud services are audited to PCI DSS or FISMA/NIST standards and additional certifications and attestations to specific regulatory frameworks for the Oracle Cloud Service may be available for additional fees. Customer must not provide Oracle with health, payment card or other sensitive personal information that requires specific regulatory, legal or industry data security obligations for the processing of such data; however, where available for certain Cloud Services, Oracle may offer for purchase by Cloud Customers additional services designed for the processing of regulated data within the services environment. Note that such additional services are not available for all Cloud Services.

Oracle understands that some Customers may have regulatory audit requirements and Oracle will cooperate with Customer as described in the Data Processing Agreement in those cases.

1.13 Oracle Software Security Assurance

Oracle Software Security Assurance (OSSA) is Oracle's methodology for building security into the design, build, testing, and maintenance of its services. The OSSA program is described at <http://www.oracle.com/us/support/assurance/overview/index.html>.

Privacy and Security (RFP #8.6)

Provided below is the information requested in section 8.6 of the RFP.

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

Oracle Response:

IMMEDIATE SECURITY CERTIFICATION (FedRAMP)

Utah should consider a modern citizen experience platform that is already a FedRAMP JAB (Joint Authorization Board) certified SaaS. While operating in our Government Cloud is not required for a Citizen Relationship Management (CRM) deployment, we have included this section to explain the significance of a FedRAMP JAB Certification.

Specifically, it is important to understand that not all FedRAMP certifications are alike. More to the point a FedRAMP JAB certification must be scrutinized by the "Board", comprised of the Chief Information Officers (CIOs) of the U.S. Department of Homeland Security (DHS), U.S. Department of Defense (DOD), and U.S. General Services Administration (GSA). This board is responsible for prioritizing authorizing cloud services that will be widely used across government. To obtain FedRAMP JAB certification, the CIOs of DoD, DHS, and GSA must agree that the Cloud Service Providers (CSPs):

- Strictly meets all controls

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

- Presents an acceptable risk posture for use across the federal government
- Conveys a baseline-level of likely acceptability for government-wide use

It is important to note that the FedRAMP JAB certification puts the onus of maintaining certification on the Cloud Service Providers (CSPs), and not on the city/county/agency obtaining the service. Additional CSP responsibilities are listed below.

- CSPs must use an accredited Third-party Assessor Organization (3PAO)
- FedRAMP PMO manages continuous monitoring activities; agencies review results

Finally, proven benefits of working with a company that has FedRAMP JAB certification include:

- It's the most rigorous, (although slowest) path to authorization.
- JAB authorization offers the LOWEST risk tolerance-level
- HIPAA controls (AT-101) and FISMA NIST 800-53 Moderate Controls are included

When you go to the [fedramp.gov](https://www.fedramp.gov) site, you can see that both our PaaS and SaaS offerings are FedRAMP JAB Certified:

- <https://www.fedramp.gov/marketplace/compliant-systems/>
- [Oracle Corporation – Federal Managed Cloud Services \(PaaS\)](#)
- [Oracle Corporation – Oracle Service Cloud \(SaaS\)](#)

SECURITY AND MISSION CRITICAL CLOUD OPERATIONS

Oracle understands that the confidentiality, integrity, and availability of your information are vital to your business operations. That's where Oracle's solution excels. You must have trust and confidence in your service provider, and Oracle takes this commitment seriously. Security is embedded in Oracle's "DNA" – within the product, the development cycle, and Cloud Operations practices – to ensure your information remains your information.

PHYSICAL SECURITY

Full-time, 24/7 local operations and security staff ensure that only authorized individuals have the ability to access the data center. All data center access doors, including shipping and parking areas, are monitored and video recorded. All data center access is secured by access cards, biometric devices (hand scanners), man-traps, portals, or a combination thereof. Exterior walls, doors, and windows are taken into careful design considering the environment and are generally constructed according to the requirements to protect from natural hazards such as lightening and wind.

Server and network equipment is physically secured within locked cages/suites inside the data center. The listing of employees and cages are updated promptly to ensure access is limited to authorized personnel. Each data center provides centralized security operations and monitoring on a 24/7 basis, including prompt response to actual or suspected physical security incidents. In addition to administering and monitoring access to the data center, the operations and security teams monitor and enforce other security policies and environmental sensors and alarms. All security and environmental systems are supported by redundant power, uninterruptible power supply (UPS) devices, and stand by generators.

LOGICAL SECURITY

Oracle's solution requires management authorization for employee access to any critical applications and systems, and additional approval levels are required for all cloud services access. Access is granted according to a user's role and business need. Logical and physical access is immediately revoked from employees who have resigned or are terminated. Oracle Cloud Service continuously monitors logs, and audits system and network activities, including access or attempted access to customer data. This includes monitoring and auditing of systems for unauthorized or inappropriate access to customer data by Oracle employees.

DATA AVAILABILITY

Oracle's solution is architected with availability, maintainability, scalability, and customer security at the top of the list. Every data center implementation meets or exceeds the following specifications:

- Redundant firewalls
- Redundant F5 load balancers with SSL acceleration
- Redundant web farms
- Multi-processor servers connected by multiple gigabit NICs
- Redundant database disk using real-time replication
- Redundant (failover) database servers
- Tape library for offsite data storage

In addition to the robust computing architecture, each data center supports Oracle's solution via:

- Dedicated substation on utility grid
- Four or more onsite diesel generators
- Independent rack power sources
- Dual entry network connectivity
- 3+ internet backbone providers
- Less than 40 percent peak network utilization
- 99.999 percent availability of power and cooling

ENVIRONMENTAL CONTROLS

All data centers leverage advanced monitoring and reporting systems to monitor environmental controls and alert data center staff to potential or merging issues. Using these systems, the 24/7 staff monitor:

- All power systems, including generators, transfer switches, UPS, diesel generators, and their fuel supplies
- Fire detection and suppression systems, and water sensors, as well as a double interlock pre-action and detection system

All data centers are equipped with independent utility sources originating from independent feeders or substations. The incoming services lines are connected to automatic transfer switches, which also connect to redundant standby diesel generators.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

All mission-critical systems, including all server and network equipment, heating and cooling equipment, and security systems at the data centers are sourced by redundant UPS systems. All data centers have zoned temperature control systems, with multiple HVAC units at each center to verify correct temperature in critical areas. If temperatures vary outside preset limits, an alarm is generated. The HVAC units are powered by utility and generator systems for redundancy.

DISASTER RECOVERY

Regardless of the quality of any system architecture, infrastructure, or robustness of any individual data center, unexpected situations can occur that potentially may impact Oracle's solution operation, and limit ability to deliver service to customers. Oracle has established a recovery strategy and a detailed recovery plan, including recovery procedures for critical infrastructure components, to allow for a quick recovery of Oracle's solution, with minimal disruptions to the customer's operations.

Each production customer's data is replicated in near-real-time to two replication servers within the production data center, as well as to a geographically-remote disaster recovery (DR) facility. This creates multiple redundant copies of all customer data to guard against system, local disruptions, and even entire data center failure

INTRUSION DETECTION AND ANTI-VIRUS

Oracle's solution operates an advanced intrusion detection system (IDS) on the internal and customer facing networks to monitor network traffic for unauthorized or suspicious activity. Traffic monitor correlates threats and provides event aggregation across all systems and networks, and sends events to the SIEM. All log summaries are reviewed daily, with certain alerts or events escalated as appropriate, and may invoke the Incident Response Plan.

All files sent to Oracle Cloud Service, regardless of the method used to transmit, are scanned for known attack signatures. Infected files are flagged and not permitted into the service.

INTERNAL AND THIRD-PARTY TESTING AND ASSESSMENTS

New product features are tested prior to code completion to identify features that do not work properly. Security testing is integrated into feature testing and regression testing. Additional security testing is provided in the form of source code scans of modified or added code, and internal audits of the products. Every Oracle Service release is subjected to a third-party application vulnerability assessment prior to release.

REGULATORY COMPLIANCE

Oracle's solution is designed and certified to meet many of the compliance requirements of the most demanding environments. The security landscape continues to evolve, and you can rely on Oracle's solution to stay ahead of threats. Note that some compliance offerings are unique to Oracle's solution, and not all regulatory frameworks listed below are applicable to all available environments of Oracle's solution.

- PCI DSS Service Provider Level 1 (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- Family Education Rights and Privacy Act
- GLBA (Gramm-Leach-Bliley Act)

ORACLE

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

- NIST 800-53 Moderate Control (National Institute of Standards and Technology 800-53)
- FISMA (Federal Information Security Management Act)
- U.K. Data Protection Act 1998, and all other E.U. National Legislation
- E.U. Data Privacy Directive 95/46/EC
- DIACAP (DoD Information Assurance Certification and Accreditation Process)
- FIPS 140-2 (Federal Information Processing Standard)
- SSAE 16 (Statement on Standards for Attestation Engagements 16)
- E.U. – U.S. Safe Harbor Registration SOC 1/SOC 2 (Service Organization Controls)

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

Oracle Response:

Yes, please see response 8.6.1 above.

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

Oracle Response:

Yes, please see response 8.6.1 above.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

Oracle Response:

Yes, please see response 8.6.1 above.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls.

Oracle Response:

Yes, please see response 8.6.1 above.

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

Oracle Response:

Yes, please see response 8.6.1 above. In addition, When looking at a record in Oracle's solution, the audit log lists a series of actions that have affected that record, including when the record was created, events that occurred related to the record (such as editing or changing the status of an incident), and by whom.

In current releases of Oracle's solution, the default workspaces include a tab for the audit log. Custom workspaces may have the auditlog embedded on another tab or removed from the workspace for some reason. If you do not have an Audit Log tab for the record types below, contact the administrator for Oracle's solution for your site to determine how to access the audit log.

Audit logs are associated with the types of records listed below:

- Incidents
- Answers
- Contacts
- Organizations
- Sales Opportunities
- Tasks

In addition, several marketing records include the Audit Log as an embedded tab on the main Summary tab:

- Campaigns
- Surveys
- Mailings
- Audiences (segments and contact lists)
- Documents

Thread Contacts Attachments Web Visit Details Tasks Audit Log				
When	Who	What	Description	
03/09/2011 09:12 AM	System	Survey Sent		
03/09/2011 09:12 AM	Admin2 Admin	Edited	From Incident Multi-Edit, Client IP Address:199.2.44.227	
03/09/2011 09:12 AM	Admin2 Admin	Changed Status	Solved	
03/04/2011 09:32 AM	Admin1 Admin	Changed Status	Updated	
03/04/2011 09:32 AM	Admin1 Admin	Changed Queue	Tier 2	
03/04/2011 09:32 AM	Admin1 Admin	Created	From Data Import, Client IP Address:208.72.88.124	
03/04/2011 09:32 AM	Admin1 Admin	Assigned	To Admin / Admin1 Admin	

FIGURE 25: ORACLE'S SOLUTION: AUDIT LOG EXAMPLE

SYSTEM LOGS

Oracle's solution allows agents to see a complete history of the current interaction with a customer. Any additions to the interaction are automatically captured with a date and time stamp. Any phone, web, or email communications are captured in an interaction. In addition, a detailed record of each change can be seen on the details tab by clicking the Audit log button.

The Audit Log contains a detailed listing of every change to the record. This log is complete with type of change, name of person making the change, date, and time of the change.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

Oracle Response:

Privileged access for specific audiences is configurable in Oracle's solution. We look at Administrative, and end user access in this section.

Administrative Access – Oracle's solution provides for configuration of administrative access levels for staff members. With full access, any and all configuration is accessible via graphical user interface (GUI) settings. Depending on the user profiles set up by the administrator, other staff members may be limited. Because Oracle's solution is entirely a web-based application, staff members can access the administrative side of the program, (provided they have appropriate security clearance) from a browser at any location.

The roles or privileges that can be applied or removed from user profiles include the following:

- Accessible Interfaces
- Views
 - Edit Administration
 - Change
 - Default Incident View
 - Default Customer View
 - Default Answer View
- Modify Profiles/Groups/Accounts
- Incidents (Add/Update, Send Response, Assign to other groups, and Delete)
- Answers
- Customers/Companies (Add, Update, and Delete)
- Canned Reports
- Custom Reports (Add/Update)
- Live (Phone/Chat/Monitor)
- Modify Administrative Settings
- Modify Business Process Settings

End User Access – Oracle’s solution includes the ability to easily configure or designate knowledgebase articles as viewable or not viewable to specific audiences in two different ways. The first way is to designate knowledge items as either public, (viewable on the public website) or private, (viewable only to designated internal personnel).

Another option, on the customer-facing side of Oracle’s solution, can be used to configure access using a feature called Privileged Access. Privileged Access enables certain users to automatically gain specific information access privileges after they are logged in.

Privileged Access in Oracle’s solution allows you to grant certain contacts and organizations the ability to view answers in your knowledgebase that are not available to all end users. For example, if you had a group of contacts that purchased a higher-level of customer support, you could create additional answers that would not be viewable to the general public on your end user interface, but would be viewable only to those contacts with privileged access. Access can be controlled in self-service options, web form submission, chat, and even email based on service levels, through required end user log ins.

Security features tied to web form submissions provide you an extra layer of security against malicious botnets and other attacks attempting to compromise site integrity and security.

An abuse detection system constantly monitors incoming web form traffic for any signs of an attack. If abuse is detected, the system begins injecting CAPTCHA verification dialogs into the pages. When a user successfully completes the CAPTCHA question, the system allows their session to continue as it normally would, and abusive sessions from botnets are terminated.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

Oracle Response:

Please see section 1.Oracle Cloud Security Policy of the Oracle Cloud Enterprise Hosting and Delivery Policies found in Attachment 7.2.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

Oracle Response:

Oracles policies includes several protocols designed to be read in conjunction with each other as indicated in the Oracle Cloud Enterprise Hosting and Delivery Policies, specifically section 3.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

Oracle Response:

Oracle’s solution has been developed using a logical three-tier Internet architecture consisting of presentation, application logic, and data management layers. Because of the tiered separation, Oracle’s solution is highly scalable, allowing expansion at the presentation and application logic tiers and at the data management tier. Oracle has experience deploying Oracle’s solution in highly available, highly scalable, load-balanced web server and clustered database server configurations. Oracle’s solution

supports most commonly available operating systems (Linux, Sun Solaris, Microsoft Windows Server) and databases (Oracle, Microsoft SQL Server, MySQL).

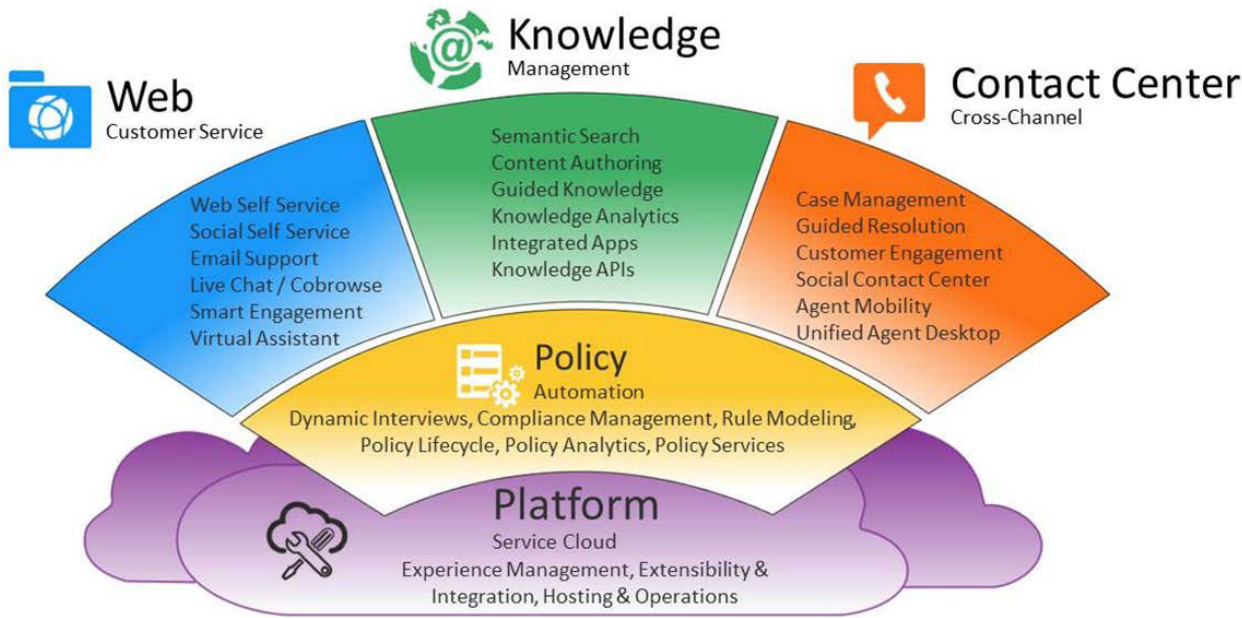


FIGURE 26: ORACLE SERVICE CLOUD OVERALL ARCHITECTURE

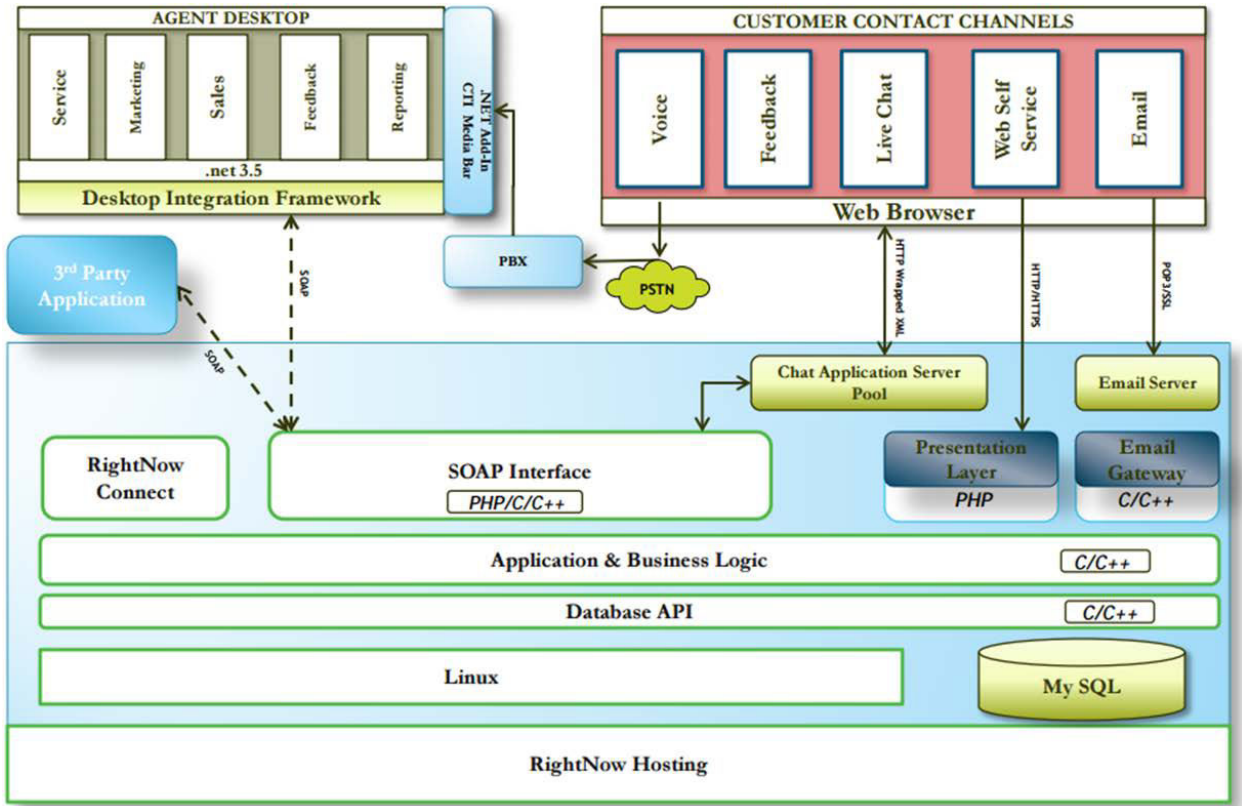


FIGURE 27: ORACLE SERVICE CLOUD PRODUCT ARCHITECTURE

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

Oracle Response:

US employees who have access to client data have passed background checks. Only a small subset of developers has access to client production data—for the purposes of troubleshooting or correcting customer issues.

All user and administrative accounts are managed by the corporate security manager. Administrative access is provided to hosting administrators via use of the 'sudo' command. The root password is known only by the corporate security manager, the IT director, the hosting manager, and any people designated by all three of the parties listed previously. All non-hosted support accounts are given away on a need-to-know basis.

All access to application and supporting computer networks by system administrators, operators, development, and audit staff is logged. All logs are sent via syslog to a central syslog server where they are parsed in real-time for failed login attempts using logsurfer.

All failed login attempts are logged showing the time, date, and user name used. Failed login attempts are emailed to the security team and monitored on a quarterly basis. These logs are retained on the systems for at least 2 weeks and available via tape for a year. Upon termination, employees are removed from the access list immediately.

All user accounts are locked out of the bastion hosts after five failed log in attempts. The security manager, IT director, or hosting manager for Oracle's solution must manually unlock an account.

Other personnel procedures are as follows:

- Remote log-in only via ssh to a bastion server only from specific addresses.
- All hosting systems administrators have passed criminal and social security background checks.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

Oracle Response:

Data at rest will be encrypted using FIPS 140-2 compliant AES at a moderate-level. Oracle will need to understand what level of FIPS 140-2 compliance is required by Oracle's solution based on your determination of data sensitivity.

Oracle's solution is designed and certified to meet many of the compliance requirements of the most demanding environments. The security landscape continues to evolve, and you can rely on Oracle's solution to stay ahead of threats. Note that some compliance offerings are unique to Oracle's solution, and not all regulatory frameworks listed below are applicable to all available Oracle Service Cloud environments.

- PCI DSS Service Provider Level 1 (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- Family Education Rights and Privacy Act
- GLBA (Gramm-Leach-Bliley Act)

- NIST 800-53 Moderate Control (National Institute of Standards and Technology 800-53)
- FISMA (Federal Information Security Management Act)
- U.K. Data Protection Act 1998, and all other E.U. National Legislation
- E.U. Data Privacy Directive 95/46/EC
- DIACAP (DoD Information Assurance Certification and Accreditation Process)
- FIPS 140-2 (Federal Information Processing Standard)
- SSAE 16 (Statement on Standards for Attestation Engagements 16)
- E.U. – U.S. Safe Harbor Registration SOC 1/SOC 2 (Service Organization Controls)

PCI CLOUD

Oracle offers a PCI-certified Cloud option. This option provides an environment certified as PCI Service Provider Level 1 – the highest-level possible for service providers.

As part of industry-wide PCI compliance efforts, Oracle's solution includes several features to improve security processes used to store and manage contact passwords in the knowledgebase. The features are:

- **Removal of Password Visibility on Oracle's Solution Console** – Oracle's solution provides increased security by removing the contact password field from scripts and workspaces so that staff members can no longer view passwords in any workspace or merge field functions.
- **Removal of the Email Me My Password Feature** – When customers have forgotten their password, they can request that the password be reset. The current password is then invalidated and a message containing an encrypted link is sent to the customer's primary email address. When the customer clicks the email link, a Change Password window requires the entry and confirmation of a new password.
- **New Reset Password Button** – If your organization requires providing staff members with the option to change customers' passwords, a Reset Password button can be added to the ribbon on custom incident, contact, opportunity, and task workspaces. Clicking this button invalidates the current password and sends a password reset email to the contact's primary email address.
- **New Transaction Types** – The following transaction types appear on the Audit Log tab in the contact workspace: Password Changed, Password Reset by Customer, and Password Reset by Administrator. Each transaction notes when and by whom passwords were changed.

These password security procedures are part of requirements that Oracle's solution has fulfilled to become fully compliant with the Payment Card Industry Data Security Standard, often referred to as PCI compliance. Oracle's solution offers a PCI-certified cloud option. This option provides an environment certified as PCI Service Provider Level 1 – the highest-level possible for service providers.

PCI compliance is necessary to ensure maximum security of customer information. All customer data, including passwords, is encrypted at rest in the PCI environment of Oracle's solution, using file system encryption (with automated key management), so the entire database is encrypted, and all customer data is encrypted using SSLv3 in transit. As part of this compliance, passwords are encrypted on the Customer Portal side as well as the agent side of Oracle's solution.

Your organization will benefit from:

- Compliance with government mandated legislation and regulations, both current and proposed
- Being able to meet the PCI compliance process

In Oracle Database Cloud – Database as a Service databases, data security is provided for data in transit and data at rest. Security of data in transit is achieved through network encryption. Data at rest security is achieved through encryption of data stored in database data files and backups.

Data in Oracle Database files, including backups, is secured by the use of encryption implemented through a key management framework. Security of data across the network is provided by native Oracle Net encryption and integrity capabilities.

Upon termination of services or expiration of production services under the ordering document or at customer's request, Oracle will delete the environments and any production data residing therein in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the environments. For a period of up to 60 days after the termination or expiration of production services under the ordering document, Oracle will make available customer data then in the production services environment for the purpose of retrieval by customer. Oracle has no obligation to retain the data for customer purposes after this 60 day post termination period. Oracle Customer Support Identifiers (CSIs) are terminated at the end of the 60 day period.

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

Oracle Response:

The Corporate Security Incident Handling Plan for Oracle's solution specifies that all affected parties should be notified of medium and high-risk security incidents within 12 hours of incident confirmation. Incident confirmation will occur when it has been determined, which parties have been affected by an incident and to what extent.

Migration and Redeployment Plan (RFP #8.7)

Provided below is the information requested in section 8.7 of the RFP.

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

Oracle Response:

Please see our Oracle Cloud Enterprise Hosting and Delivery Policies, specifically section 7. This document is available as Attachment 7.2 of this response and available here:
<http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

Oracle Response:

Please see our Oracle Cloud Enterprise Hosting and Delivery Policies, specifically section 7. This document is available as Attachment 7.2 of this response and available here:
<http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

Service or Data Recovery (RFP #8.8)

Provided below is the information requested in section 8.8 of the RFP.

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

- a. Extended downtime.
- b. Suffers an unrecoverable loss of data.
- c. Offeror experiences a system failure.
- d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.
- e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

Oracle Response:

The following response is excerpted from Attachment 7.2, "Oracle Cloud Enterprise Hosting and Delivery Policies":

3. ORACLE CLOUD DISASTER RECOVERY SERVICE POLICY

3.1 Scope

This Policy applies only to Customer's production environments within Oracle Cloud Services. The activities described in this Policy do not apply to Customer's own disaster recovery, business continuity or backup plans or activities, and Customer is responsible for archiving and recovering any non-Oracle software.

Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Oracle, that leads to loss of a data center and corresponding service unavailability.

For the purposes of this Policy, a disaster means an unplanned event or condition that causes a complete loss of access to the primary site used to provide the Oracle Cloud Services such that the Customer production environments at the primary site are not available.

3.2 System Resilience

Oracle Cloud Services maintains a redundant and resilient infrastructure designed to maintain high levels of availability and to recover services in the event of a significant disaster or disruption. Oracle designs its cloud services using principles of redundancy and fault-tolerance with a goal of fault-tolerance of a single node hardware failure.

Oracle Cloud Services provide an infrastructure that incorporates a comprehensive data backup strategy. The Oracle Cloud includes redundant capabilities such as power sources, cooling systems, telecommunications services, networking, application domains, data storage, physical and virtual servers, and databases.

Oracle has two separate data centers that function as primary and secondary sites for Oracle Cloud Services. Customer's production standby (secondary site) environment will reside in a data center separate from Customer's primary site. Oracle will commence the disaster recovery plan under this Policy upon its declaration of a disaster, and will target to recover the production data and use reasonable efforts to re-establish the production environment at the secondary site. For a major regional jurisdictional area (for example, the United States or the European Union), Oracle operates both a production and secondary site within that region.

Customer data is replicated in physically separate facilities in order to restore full services in the event of a disaster at a primary site. Backups are for Oracle's sole use in the event of a disaster.

3.3 Disaster Recovery

Oracle provides for the recovery and reconstitution of its production Cloud Services to the most recent available state following a disaster.

Oracle has established alternate processing sites to accommodate full operating capability in the event of loss of service at a primary facility. Oracle maintains a Disaster Recovery Plan that describes recovery procedures.

Disaster recovery operations apply to the physical loss of infrastructure at Oracle facilities. Oracle reserves the right to determine when to activate the Disaster Recovery Plan. During the execution of the Disaster Recovery Plan, Oracle provides regular status updates to Customers.

Note: the RTO and RPO described below do not apply to Customer customizations that depend on external components or third-party software. During an active failover event, non-critical fixes, and enhancement requests are not supported. Customer will be solely responsible for issues arising from third-party software and customizations (CEMLIs) to Oracle programs and services.

3.3.1 Recovery Time Objective

Recovery time objective (RTO) is Oracle's objective for the maximum period of time between Oracle's decision to activate the recovery processes under this Policy to failover the service to the secondary site due to a declared disaster, and the point at which Customer can resume production operations in the standby production environment. If the decision to failover is made during the period in which an upgrade is in process, the RTO extends to include the time required to complete the upgrade. The RTO is 12 hours from the declaration of a disaster.

3.3.2 Recovery Point Objective

Recovery point objective (RPO) is Oracle's objective for the maximum possible length of time during which data could be lost, in the event of a disaster. The RPO is 1 hour from the occurrence of a disaster, excluding any data loads that may be underway when the disaster occurs.

3.4 Approvals and Reviews

This Policy and the corresponding Disaster Recovery Plan is reviewed annually. The Plan is revised during the review process to incorporate problem resolutions and process improvements.

3.5 Service Restoration

This Policy identifies the purpose and scope of the Disaster Recovery Plan, the roles and responsibilities, management commitment, coordination among organizational entities, and compliance. The plan documents the procedures for recovering a Cloud Service in the event of a disaster.

Oracle is committed to minimizing down time due to any disasters or equipment failures. As part of this commitment, Oracle has a corporate business disaster recovery plan for a timely recovery and restoration of Oracle operations.

3.6 Disaster Recovery Plan Objectives

The following are the objectives of Oracle's Disaster Recovery Plan for Oracle Cloud Services:

- In an emergency, Oracle's top priority and objective is human health and safety.
- Maximize the effectiveness of contingency operations through the established Disaster Recovery Plan that consists of the following phases:
 - Phase 1 – Disaster Recovery Launch Authorization phase—to detect service disruption or outage at the primary site, determine the extent of the damage and activate the plan.
 - Phase 2 – Recovery phase - to restore temporary IT operations at the secondary site.
 - Phase 3 – Reconstitution phase - to restore processing capabilities and resume operations at the primary site.
- Identify the activities, resources, and procedures to carry out processing requirements during prolonged interruptions.
- Assign responsibilities to designated personnel and provide guidance for recovery, during prolonged periods of interruption.
- Ensure coordination with other personnel responsible for disaster recovery planning strategies. Ensure coordination with external points of contact and vendors and execution of this plan.

3.7 Plan Testing

The Cloud Services Disaster Recovery Plan is tested, as a live exercise or a table-top test, on an annual basis. The tests are used for training hosting personnel and are coordinated with all personnel responsible for contingency planning and execution. The tests verify that online backups can be recovered and the procedures for shifting a service to the alternate processing site are adequate and effective. Test plans are developed in accordance with NIST 800-34. Results of the testing are used to improve the process and initiate corrective actions.

8.8.2 Describe your methodologies for the following backup and restore services:

- a. Method of data backups
- b. Method of server image backups
- c. Digital location of backup storage (secondary storage, tape, etc.)
- d. Alternate data center strategies for primary data centers within the continental United States.

Oracle Response:

The following response is excerpted from Attachment 7.2, “Oracle Cloud Enterprise Hosting and Delivery Policies”.

2. ORACLE CLOUD SYSTEM RESILIENCY POLICY

The resiliency and backups described in this Policy apply only for Oracle Cloud services. Customer is solely responsible for developing a business continuity plan to ensure continuity of its own operations in the event of a disaster and for backing up and recovering any non-Oracle software.

2.1 Oracle Cloud Services High Availability Strategy

For business continuity in the event of an incident affecting Oracle Cloud Services, Oracle deploys the services on resilient computing infrastructure. Oracle’s production data centers have component and power redundancy with backup generators in place to help maintain availability of data center resources in the event of crisis as described below.

2.2 Redundant Power

The infrastructure design includes redundant power feeds to the data center and redundant power distribution for the data center and to the data center racks. Data center cooling components (chillers, towers, pumps, and computer room air conditioning units) include redundancy. The emergency standby power includes redundant battery backup with generator fuel stored onsite and contracts in place for refueling.

2.3 Redundant Network Infrastructure

Network designs include redundant circuits from different carriers, firewall pairs, switch pairs, and load balancer pairs.

2.4 Redundant Program Servers

Customer’s environment consists of a set of one or more physical servers or virtual servers that provide services to Customer. The overall program tier functionality may be distributed across multiple physical servers or virtual servers.

2.5 Redundant Database Servers

Databases are configured to distribute workload across multiple physical servers. High-availability is achieved through clustering and replication.

2.6 Redundant Storage

Oracle Cloud services data resides in redundant storage configurations with protection from individual disk or array failure.

2.7 Oracle Cloud Services Backup Strategy

In support of Oracle's Cloud Disaster Recovery practices (see Section 3 below), Oracle periodically makes backups of production data in Customer's Cloud Service for Oracle's sole use to minimize data loss in the event of a disaster. Database backups are stored at the primary site used to provide the Oracle Cloud Services, as well as at an alternate location for redundancy purposes. A backup is retained online and/or offline for a period of at least 60 days after the date that the backup is made. Oracle typically does not update, insert, delete or restore Customer data on behalf of Customer. However, on an exception basis and subject to written approval and additional fees, Oracle may assist Customer to restore data which Customer may have lost as a result of their own actions.

Data Protection (RFP #8.9)

Provided below is the information requested in section 8.9 of the RFP.

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

Oracle Response:

Encryption is offered end-to-end for Oracle Cloud Services. Oracle Cloud Services can provide encryption capabilities for both data in-transit as well as data at rest. Encryption technologies may vary based on cloud services and leverage technologies such as SAN encryption or database encryption.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Oracle Response:

Oracle puts security at the forefront of all our endeavors. Oracle has a consistent contract model for all programs and services globally. The standard contracts often refer to policies that may be relevant to a specific order. Links to the standard contracts and specified policies are available here.

<http://www.oracle.com/us/corporate/contracts/index.html>.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Oracle Response:

Yes, please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 1.12) found in Attachment 7.2.

Service Level Agreements (RFP #8.10)

Provided below is the information requested in section 8.10 of the RFP.

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

Oracle Response:

Please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 4: Service Level Objective) found in Attachment 7.2.

Oracle has a consistent contract model for all programs and services globally. The standard contracts often refer to policies that may be relevant to a specific order. Links to the standard contracts and specified policies are available here. <http://www.oracle.com/us/corporate/contracts/index.html>.

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Oracle Response:

The Oracle Service Level Agreement was developed with public cloud consideration to overall management and maintenance of data at the primary hosting site and well as back up site to ensure a target-level of service that is achievable and sustainable. Oracle makes available for a separate fee Oracle Cloud Support, which allows for advance support with negotiated levels of support. The details of Oracle's service levels and optional cloud support is included in the Oracle Cloud Enterprise Hosting and Delivery Policies (section 4: Service Level Objective) found in Attachment 7.2.

Data Disposal (RFP #8.11)

Provided below is the information requested in section 8.11 of the RFP.

Specify your data disposal procedures and policies and destruction confirmation process.

Oracle Response:

Upon termination of services or at a customer's request, Oracle will delete environments or data residing therein in a manner designed to ensure that they cannot reasonably be accessed or read, unless there is a legal obligation imposed on Oracle preventing it from deleting all or part of the environments or data.

More information is located in the Oracle Cloud Enterprise Hosting and Delivery Policies (section 4 and 7) found in Attachment 7.2.

Performance Measures and Reporting (RFP #8.12)

Provided below is the information requested in section 8.12 of the RFP.

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.**Oracle Response:**

Oracle works to meet a target system availability Level of 99.5% of the production service, for the measurement period of one calendar month, commencing at Oracle's activation of the production environment. More details are included in the Oracle Cloud Enterprise Hosting and Delivery Policies (Section 4) found in Attachment 7.2.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.**Oracle Response:**

Oracle works to meet a target system availability Level of 99.5% of the production service, for the measurement period of one calendar month, commencing at Oracle's activation of the production environment. Oracle measures the system availability level by dividing the difference between the total number of minutes in the monthly measurement period and any unplanned downtime by the total number of minutes in the measurement period, and multiplying the result by 100 to reach a percent figure. More details are included in the Oracle Cloud Enterprise Hosting and Delivery Policies.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.**Oracle Response:**

Yes, please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 4) found in Attachment 7.2.

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.**Oracle Response:**

Yes, please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 4) found in Attachment 7.2.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.**Oracle Response:**

Yes, please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 4) found in Attachment 7.2.

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.**Oracle Response:**

Yes, please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 3 and 4) found in Attachment 7.2.

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.**Oracle Response:**

The SmartHosting program in Oracle's solution provides real-time usage reporting, disk space monitoring, and a Customer Success Index that allows customers to compare their implementation against the commercially reasonable efforts benchmark of Oracle's solution. One component of the SmartHosting offering is a Hosting Management System (HMS). HMS is a browser-based dashboard that enables users to view hosted applications data in a manner similar to how they would view internally deployed software. It gives customers access to a full range of application statistics, including page turns and page load times. This product also allows customers to upgrade according to their own schedule, rather than leaving vendors to decide when to introduce new software versions.

Oracle's solution HMS further enhances the value of hosted applications by making it as easy to monitor and upgrade as in-house applications. There is no charge to hosted customers for this tool.

8.12.8 Ability to print historical, statistical, and usage reports locally.**Oracle Response:**

Please see our response in section 8.12.7 above.

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.**Oracle Response:**

Yes, please see our Oracle Cloud Enterprise Hosting and Delivery Policies (section 4 and 6) found in Attachment 7.2.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.**Oracle Response:**

Oracle's solution provides a horizontally scalable infrastructure model across all tiers, including SAN storage. Monitoring tools are tracking performance and utilization across the landscape, and Oracle takes proactive steps to address resource constraints.

Cloud Security Alliance (RFP #8.13)

Provided below is the information requested in section 8.13 of the RFP.

Describe your level of disclosure with CSA Star Registry for each Solution offered.

- a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.5
- b. Completion of Exhibits 1 and 2 to Attachment B.
- c. Completion of a CSA STAR Attestation, Certification, or Assessment.
- d. Completion CSA STAR Continuous Monitoring.

Oracle Response:

Oracle recognizes the unique needs of its Public Sector customers. As such, Oracle believes strongly in the need for open and interoperable standards to simplify integration with existing environments. Further, Oracle strives to help organizations comply with key security standards and compliance mandates such as the U.S. Federal Information Security Management Act (FISMA), the U.S. Federal Risk and Authorization Management Program (FedRAMP), the U.S. DOD Information Assurance Certification and Accreditation Process (DIACAP). Further, Oracle works to support and align with NIST cloud computing efforts as well as with industry bodies such as the Cloud Security Alliance in order to share and advocate standards and best practices.

Oracle is aware of the CSA Star Registry process. While we are not currently in the process of registering with CSA Star, we have completed self-assessments included with this response. These self-assessments include the Cloud Controls Matrix (CCM), and the Consensus Assessment Initiative Questionnaire (CAIQ) for your review Section 7.

Service Provisioning (RFP #8.14)

Provided below is the information requested in section 8.14 of the RFP.

8.14.1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.**Oracle Response:**

Since Oracle Cloud Services are built upon NIST 800-145 model for on-demand scalability, it is up to Utah to determine a need and start the standard service delivery process.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.**Oracle Response:**

Initial provisioning of cloud service environments vary by service and are defined at the order-level with services descriptions, data center location, capacity limits based on order services in other factors of the ordered service at the time of order. During the pre-order engagement with the customer Oracle can establish provisioning schedule, which vary depending on complexity of initial ordered services. Once the environment is provisioned the customer's account administrator is notified via a welcome email with the credentials needed to access a secured cloud portal to initiate the service environment. Also, please see our response for section 8.14.1.

Back Up and Disaster Plan (RFP #8.15)

Provided below is the information requested in section 8.15 of the RFP.

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

Oracle Response:

As part of the Oracle makes secured protocols available by which designated customer users can transfer data from the service. Beyond the standard service offering Oracle is willing to engage in an evaluation and solutions planning session to gain an understanding of the unique policies and requirements by Participating Entity to determine if there is an existing solution provided by Oracle or a custom solution that could be configured to achieve their objectives.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

Oracle Response:

Oracle is unaware at the time of this submission of any known specific disaster recovery risks that could be broadly applied to multiple customers. The Oracle Cloud Enterprise Hosting and Delivery Policies found in Attachment 7.2 outline the complete policy that applies to customer's production environments within Oracle Cloud Services. The activities described in this policy do not apply to customer's own disaster recovery, business continuity or backup plans or activities, and customer is responsible for archiving and recovering any non-Oracle software. Disaster Recovery services are intended to provide service restoration capability in the case of a major disaster, as declared by Oracle, that leads to loss of a data center and corresponding service unavailability. For the purposes of this policy, a disaster means an unplanned event or condition that causes a complete loss of access to the primary site used to provide the Oracle Cloud Services such that the customer production environments at the primary site are not available.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

Oracle Response:

For business continuity in the event of an incident affecting Oracle Cloud Services, Oracle deploys the services on resilient computing infrastructure. Oracle's production data centers have component and power redundancy with backup generators in place to help maintain availability of data center resources in the event of crisis. The infrastructure design includes redundant power feeds to the data center and redundant power distribution for the data center and to the data center racks. Data center cooling components (chillers, towers, pumps and computer room air conditioning units) include redundancy. The emergency standby power includes redundant battery backup with generator fuel stored onsite and contracts in place for refueling.

Other measures include but are not limited to following: a complete description is included in Oracle's Cloud Hosting and Delivery Policies in Attachment 7.2.

- Network designs include redundant circuits from different carriers, firewall pairs, switch pairs, and load balancer pairs.
- Customer's environment consists of a set of one or more physical servers or virtual servers that provide services to customer. The overall program tier functionality may be distributed across multiple physical servers or virtual servers.
- Databases are configured to distribute workload across multiple physical servers. High-availability is achieved through clustering and replication.
- Oracle Cloud Services data resides in redundant storage configurations with protection from individual disk or array failure.

Solution Administration (RFP #8.16)

Provided below is the information requested in section 8.16 of the RFP.

8.16.1 Ability of the Purchasing Entity to fully manage identity and user accounts.

Oracle Response:

You will be responsible for creating and maintaining your own user accounts within Oracle's solution. You are given complete control over accounts in the cloud environment ordered which allows flexibility manage those accounts in any way necessary to conform to the needs of the Participating Entity.

All systems and network administrators must use either SSH (for command line access to hosts) or SSL (for web-based administration tools) to administer the network.

All SSH access is filtered through a single bastion host, which exists at each datacenter. This creates a choke point for all command line access, making it easy to monitor and terminate access to server command line.

SSH and SSL access for administrative purposes is limited by the firewall to source IP addresses that are owned, controlled and/or approved by Oracle.

8.16.2 Ability to provide anti-virus protection, for data stores.

Oracle Response:

Oracle employs anti-virus software to scan uploaded files. Virus definitions are updated daily. More information on the entire environment protocols are included in the Oracle Cloud Enterprise Hosting and Delivery Policies Section 1.6.4, part of Attachment 7.2 of this response and found here: <http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

8.16.3 Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

Oracle Response:

During the use of Oracle Cloud services the Participating Entity maintains control over and responsibility for their data residing in their provisioned environment. Oracle Cloud Services provide a variety of

configurable information protection services as part of the subscribed service. Customer data uploaded or generated for use within the subscribed Oracle Cloud Service can be prepared using the secure file transfer functionality is built on commonly used network access storage platforms and uses secured protocols for transfer (such as SFTP). The functionality can be used to upload files to a secured location, most commonly for data import/export on the Oracle Cloud hosted service, or downloading files at service termination. More details on these features are included in the Oracle Cloud Hosting and Delivery Policies included in Attachment 7.1.

8.16.4 Ability to administer the solution in a distributed manner to different participating entities.**Oracle Response:**

Each cloud service environment is separate and Oracle can support multiple Participating Entities.

8.16.5 Ability to apply a participating entity's defined administration policies in managing a solution.**Oracle Response:**

The automation of customer service workflow, wherever appropriate, improves the quality and consistency of simple and complex service interactions across multiple departments and processes. This serves to reduce training time allowing customers to adapt to changing policies and expectations. The customer and agent experience is improved by improved quality and timely management to resolution. Oracle's solution will:

- Provide the business analyst/administrator with intuitive wizards and a drag and drop designer to create and manage rules and workflow without writing code.
- Automate the movement of business object instances through multiple processes controlling state progression.
- Trigger sending email messages to end users, staff members, groups, and distribution lists
- Support the update standard and custom fields.
- Automate routing and assignment of service incidents, chat sessions, tasks, and answers.
- Support rules triggered by elapsed time to perform escalations, send alerts and trigger outreach communications campaigns or surveys
- Execute custom event handlers and external processes that can drive internal custom processes or integration with other agency systems
- Allow the dynamic assignment of service level agreements for specific interactions
- Generate new object records such as task from task plans or parent/child records

THE STATE OF UTAH VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

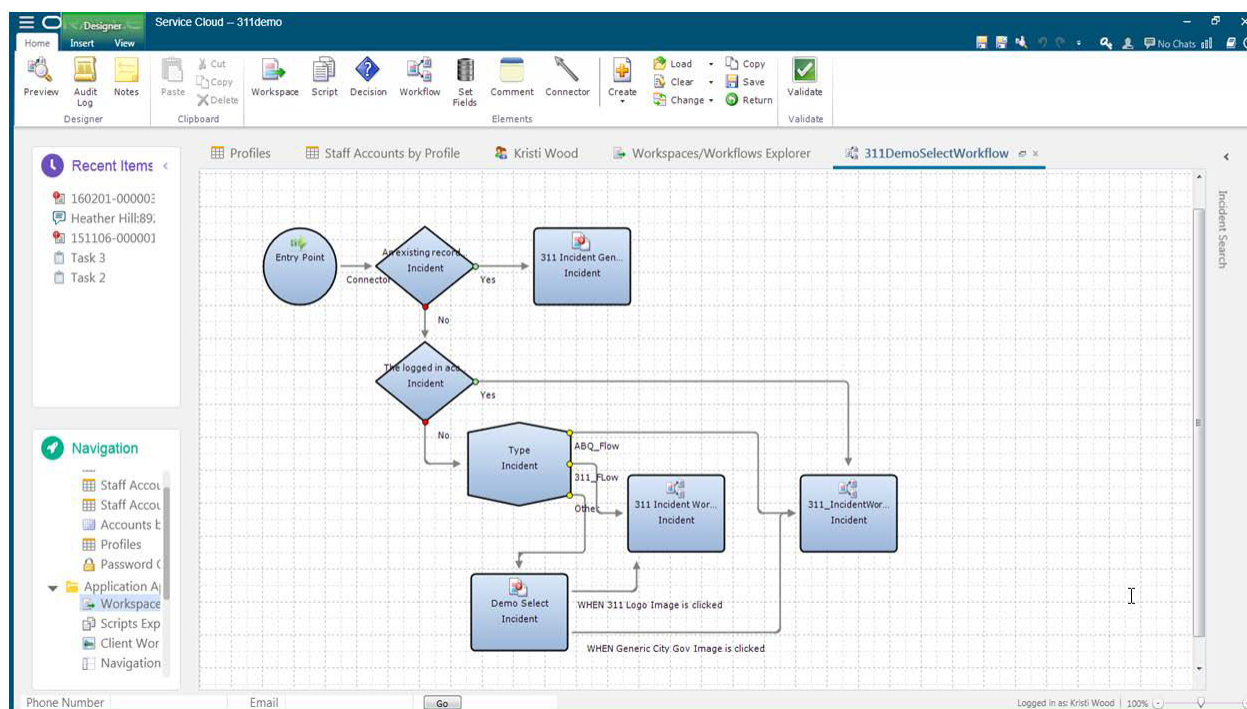


FIGURE 28: WORKFLOWS: DRAG AND DROP SIMPLICITY

AUTOMATED NAVIGATION AND DYNAMIC FORMS

In addition to workflow, our customer service solution empowers agents with automated navigation that performs functions the agent would do under certain conditions. This serves to reduce simple repetitive tasks and simplify the agent interactions with complex processes. For instance a tip about a regulatory violation is reported online; an agent reviews the tip and judges that the tip should be investigated. An automated workflow will take the agent to another view of that same tip but with areas to confirm automatically generated research tasks, review policy on the subject and present a map of the location of the potential violation. This process can happen without code and triggered by only the agent clicking a button to pursue the tip.

AUTOMATED ROUTING AND CATEGORIZATION

Oracle Services supports business improvements and processes by providing business rules as a standard component of the service. As part of a full administrative interface, Oracle provides the ability to define business rules including workflow, escalation, and automatic response rules by way of an intuitive and easy-to-use console to empower staff.

The system provides the ability to create and configure workflow rules to process the data through the construction of simple if/then statements. Configuration tools, such as text entry, radio buttons, and pull-down menus are used as tools to accomplish this functionality.

No coding knowledge is required, and users can make changes on the fly.

A list of features and benefits associated with solution workflows follows:

- **Workspace and Script Rules** – Rules dynamically adjust the display, behavior, and values of fields and controls on a workspace (based on staff member actions). Each rule is triggered by one or more events and conditions.
- **Desktop Workflow** – A sequence of workspaces, scripts, decisions, connectors, and actions presented to staff members as a dynamic interface serve to efficiently support and automate complex business processes.
- **Business Rules** – Object-based business rules control backend workflow triggered at record creation or update and time-based escalations.

ORACLE POLICY AUTOMATION (OPA)

Oracle Policy Automation (OPA) is native to Oracle's solution platform and provides an unmatched ability to adapt to changing citizen experience needs. OPA provides dynamic, precise and personalized customer advice experiences via web self-service, mobile, call center, and face-to face channels. Policy Automation enables your organization to capture, manage and deploy complex policies for self-service benefit eligibility determination, complex guided assistance, online application forms, tailored incident creation, tax obligations, business license and building permit requirement determinations, and much more. OPA enables city and county governments to elegantly deliver consistent, accurate, and transparent self-service applications processing and advice. Key Oracle Policy Automation features and functions include:

- **Dynamic Interviews** – Dynamic interviews are an intuitive way to collect information from a citizen/business during the application process without the need for the customer to download, and fill out an application form. Upon completion of the interview process, "intake" data is captured and interfaced real-time to the core processing system. Our solution supports the ability to pre-fill application data, as well as the ability to create service requests via text, email, and chat for follow-up resolution. OPA supports over 20 different written languages and can be deployed to any remote device (laptops, tablets, smartphones, etc.).
- **Rule Modeling** – Oracle Policy Automation provides a desktop modeling tool for policy creation, maintenance and deployment. Using common desktop applications like Microsoft Word or Excel business users write and maintain rules for policies in natural language. From these desktop files executable code is generated directly to your website, eliminating the need for costly IT maintenance and support.
- **Compliance Management** – Oracle Policy Automation maintains a complete audit trail of information. Each website interaction is logged and available for explanation (that is, in response to a customer complaint). Decision audit reports may be retrieved at any time.
- **Policy Analytics** – Oracle Policy Automation provides advanced policy analysis features including what-if analysis to understand the impact of new or changed policies, so that users are able to analyze and adapt policy to avoid unexpected results.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

Business License Wizard
Published 02/17/2014 02:09 PM | Updated 01/26/2016 03:14 PM

Use this interactive advice tool to work out which **business** licenses you require.

Start Food Alcohol Lottery General **Summary**

Summary [Back] [Next]

This customized list of links on information for starting a business was created based on the selected business type and your answers to the questions. Click on the links for detailed information.

Prior to applying for required permits, you must first register/file your business name. Click here for information about [registering your fictitious or "doing business as" \(DBA\) name](#).

Disclaimer: The information provided is for demonstration purposes only. You should consult an accountant and/or attorney before starting, expanding or investing in a business. This demonstration makes no guarantees regarding the completeness of the information provided.

Permit and License Links

- [Certificate of Authority to Collect Sales Tax](#)
- [Grocery Store Beer/Wine Product License \(Off Premises\)](#)
- [Alcohol Dealer Registration](#)

Business Structure

- [Sole Proprietor](#)

Employer Information

Contact Us

- [? Ask a Question](#)
- [Ask the Community](#)
- [Live Chat](#)
- Chat is not currently available.
- [Give Feedback](#)

Recently Viewed

- [Thinking About Starting a Business?](#)
- [Pothole or Other Street Surface Complaint](#)

Official Answers

- [Thinking About Starting a Business?](#)
- [How do I report graffiti on private property?](#)
- [How to get started doing business in the city](#)
- [Business Registration](#)
- [How can I report information and tips about a crime?](#)

FIGURE 29: SAMPLE OPA FUNCTIONALITY WITHIN ORACLE'S SOLUTION

Hosting and Provisioning (RFP #8.17)

Provided below is the information requested in section 8.17 of the RFP.

8.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

Oracle Response:

Provisioning of cloud service environments vary by service and are defined at the order-level with services descriptions, data center location, capacity limits based on order services in other factors of the ordered service. After order the account administrator contact listed on the Participating Entities order is notified via a welcome email with the credentials needed to access a secured cloud portal to initiate the service environment.

For example, with Oracle Service Cloud is a rich internet application that uses a standard 3-Tier architecture consisting of the following:

- **Smart Client Tier** – The client tier consists of a .NET Smart client application that presents content received from the application tier. The client tier communicates with the application tier through the Internet via Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol with Secure Sockest Layer (HTTPS).
- **Application Tier** – The application tier provides business logic for the Oracle Standard Dynamic Agent Desktop Service Cloud and transfers data from the database tier to the client tier.
- **Database Tier** – At the base of the application is the database tier containing the data users create, delete, modify, and query.

INSTALLATION METHODOLOGIES

Web-based Installation – To use the most common installation methodology, an agent simply navigates to the appropriate URL, for example: <http://interface.custhelp.com/cgi-bin/interface.cfg/php/admin/launch.php>.

The web-based installation is based upon Microsoft ClickOnce technology. ClickOnce installation is precluded when a mandatory Windows profile is detected because ClickOnce uses the user profile as the installation file destination.

Administrative Installation – Refer to the Smart Client Installation Guide for information on using the Smart Client MSI file. This guide can be found in the Library section of our site with the manuals specific to your version of Oracle Service Cloud.

8.17.2 Provide tool sets at minimum for:

1. **Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)**

Oracle Response:

This request is not applicable to our solution, since its being sold “as a Service” hosted by Oracle. Customers can deploy new services within the limits of their service agreements on either shared infrastructure or dedicated servers based on the service deployment method selected.

2. **Creating and storing server images for future multiple deployments**

Oracle Response:

This is not applicable to our solution since its being sold “as a Service” hosted by Oracle.

3. **Securing additional storage space**

Oracle Response:

This request is not applicable to our solution since its being sold “as a Service” hosted by Oracle. Customers can acquire more users or the applicable metric of the cloud services they have ordered at any time during a service term and their new purchase will be added to their existing services.

- 4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).**

Oracle Response:

During the use of Oracle Cloud services, Oracle Cloud Customers maintain control over and responsibility for their data residing in their environment. Oracle Cloud services provide a variety of configurable information protection services as part of the subscribed service.

MONITORING OF SERVERS – HOSTING

Oracle uses a variety of software tools to monitor (i) the availability and performance of Customer's production services environment and (ii) the operation of infrastructure and network components.

MONITORED COMPONENTS

Oracle monitors all levels of the service infrastructure, and currently generates alerts for CPU, memory, storage, database, network components, and transactions. Oracle's operations staff attends to any automated warnings and alerts associated with deviations of the environment from Oracle defined monitoring thresholds, and follows standard operating procedures to investigate and resolve underlying issues.

CUSTOMER MONITORING AND TESTING TOOLS

Due to potential adverse impact on service performance and availability, customer may not use their own monitoring or testing tools (including automated user interfaces and web service calls to any Oracle Cloud Service) to directly or indirectly seek to measure the availability, performance, or security of any application or feature of or service component within the services or environment. Exceptions to this are the Oracle Database Cloud Service and Oracle Java Cloud Service or if otherwise expressly permitted in the ordering document. Oracle reserves the right to remove or disable access to any tools that violate the foregoing restrictions without any liability to customer.

CUSTOMER WORKLOADS

Customer may not make significant workload changes beyond the amount permitted under the entitlements provided under ordering document.

AUTOMATED WORKLOADS

Customer may not use nor authorize the use of data scraping tools or technologies to collect data available through the Oracle Cloud Service user interface or via web service calls without the express written permission of Oracle. Oracle reserves the right to require customer's proposed data scraping tools to be validated and tested by Oracle prior to use in production and to be subsequently validated and tested annually. Oracle may require that a written statement of work be executed to perform such testing and validation work.

Trial and Testing Periods (Pre- and Post-Purchase) (RFP #8.18)

Provided below is the information requested in section 8.18 of the RFP.

8.18.1 Describe your testing and training periods that your offer for your service offerings.

Oracle Response:

FREE TRIALS

Oracle Cloud delivers the broadest selection of enterprise-grade cloud computing solutions, including SaaS, PaaS, and IaaS. Visit us on the web at cloud.oracle.com to take a free cloud trial today!

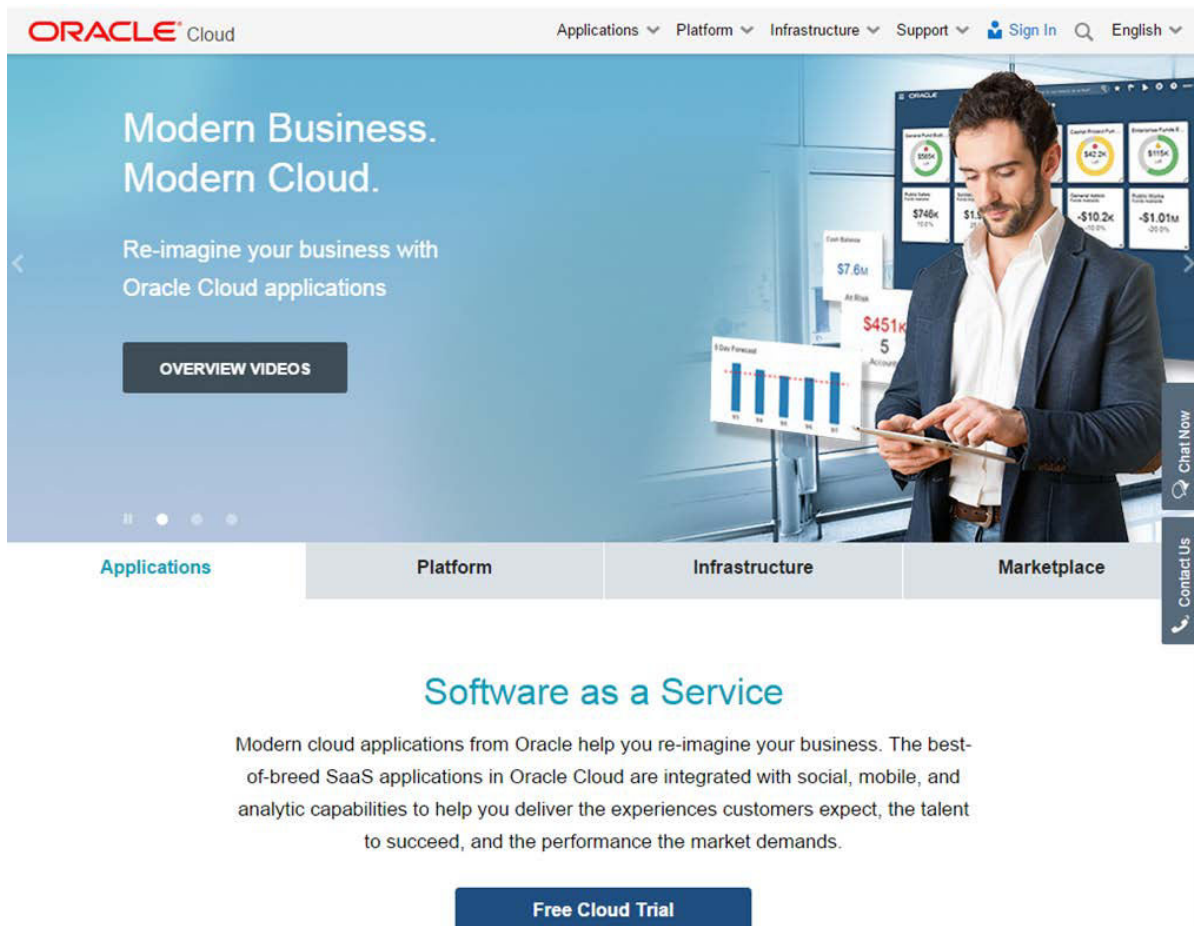


FIGURE 30: ORACLE CLOUD FREE TRIAL OFFER

TESTING

The goal of the user acceptance testing plan is to verify that Oracle Service Cloud works as designed and satisfies your business requirements.

- Verification that the system has been properly configured
- Verification that customizations and integrations are working as designed
- Confirm that all user acceptance test scripts satisfy pre-defined acceptance criteria

During the Discovery phase, when business requirements are documented and gaps identified, unique test scenarios should begin to become evident. These test scenarios are added to the standard list of scenarios so that the system can be tested to validate results during the system test process.

Prior to testing the system for results, the Oracle Service Cloud consultant and/or Oracle Service Cloud application engineer will complete unit testing. Unit testing is a task performed by Oracle Service Cloud to verify correct configuration or a module's inputs, outputs, and decision logic. For the Oracle Service Cloud application engineer, the objective of unit testing is to test possible program logic paths and combinations of data and to ensure that the module meets the technical design requirements described in the Statement of Work (SOW). The result of unit testing is error-free code that processes data accurately and reliably according to specifications.

After unit testing is complete, the implementation team (including subject matter experts from your company) performs acceptance testing to confirm that technical customizations meet the functional requirements without breaking core functionality. The focus of system testing is data integrity, integration, and usability of the functionality. Application performance is a secondary focus. Testing of multiple modules is conducted to ensure the accurate completion of the entire function. The outcome of system testing is an application that functions according to the Oracle Service Cloud standard specifications set forth in the conceptual design and any additional specifications outlined in the SOW.

The final step in the overall test cycle is to conduct user acceptance testing (UAT). The purpose of this stage is to gain consensus from your company that the system and users are ready to move the application into production. The Oracle Service Cloud project manager works with your project manager to organize and distribute the test scripts to the appropriate users according to the user test plan. The users follow the test outlined in the test scripts and record the results. Any failures are reviewed and resolved by configuration changes or code changes where appropriate.

DEVELOPMENT OF ACCEPTANCE TEST PLAN AND USER ACCEPTANCE TEST PLAN

The goal of this process is to produce detailed test plans to support all phases of testing. Your project manager and the Oracle Service Cloud project manager will work together to produce the required use cases that directly reference the documented and agreed upon business requirements. Equally important, both Oracle Service Cloud and your company must ensure that sufficient, accurate data exists to support execution of the test cases.

Each test plan shall contain:

- A list of use cases organized by role
- A list of credible data elements to support the test cases
- Assignment of test owners
- Relevant supporting information (interfacing requirements, assumptions/constraints, risks and contingency plans)

The Oracle Service Cloud project manager works to produce the test plan strategy document that outlines the purpose, objective, and approach to the overall test phase. The Oracle Service Cloud project manager works with your project manager to produce and organize the test use cases. These use cases need to map directly to the confirmed business requirements and SOW requirements. Your project manager will assign users to each set of test scenarios. Your project manager presents this test plan to the users to verify that all use cases have been identified to cover normal processes and exception processing.

The Oracle Service Cloud project manager will create the User Acceptance test kick-off meeting agenda. This kick-off meeting should be delivered to any person involved with testing to ensure that each stakeholder is aware of the goals/objectives of testing and his/her role and responsibilities. Equally important, the Oracle Service Cloud project manager will work with the developers and other support personnel to prepare the test environment well in advance of the actual test days to allow for any technical issues to be resolved. Your project manager also coordinates the testers' schedules to coincide with the system's availability after unit testing is completed.

Upon the completion of the test plan, a sign-off is received from your project manager.

Training – Depending on the extent of your Oracle Service Cloud platform needs and configuration, education levels range from simple business users to advanced HTML programmers. Oracle Service Cloud is cloud-based and is designed to be up and running with little or no configuration from administrators of your company and yet be flexible enough to be extensively configured to match your business process.

TRAINING

Training is a critical element of any successful project. Best practices dedicate that the project team learn the software capability and the end users on the configured software. This practices speeds implementation and facilitates maximum adoption and optimal result. Typically training will be provided by the firm selected to perform the implementation/configuration.

In addition, Oracle has a training arm called Oracle University. We create our courses in collaboration with the Oracle product development teams as to deliver top quality instruction and premium training content from the experts.

Courses are available in a variety of formats to make training convenient.

- **In-class Training** – Attend our scheduled classes at an Oracle learning center.
- **Live Virtual Class Training** – Attend live, hands-on training from anywhere in the world.
- **Training On Demand** – Access full classroom training and labs in an on-demand format.
- **Self-Study** – Stretch your budget or supplement other learning with self-paced courses.
- **Private Training** – Train a group at your site or at an Oracle learning center.

8.18.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Oracle Response:

The Oracle Account team can arrange for a demonstration of one of the Cloud Service offerings and often provide for a trial environment for the customer to access and use for their own proof of concept. Each customer's needs vary depending on use case for the cloud environment and mitigation concerns so through an engagement session the Oracle Account team, which includes sales professionals and engineers, can recommend a wide range of options that may include demonstrations, trial environments, or connection with a reference client who has a similar need that is deployed in one of the Oracle Cloud Services.

In addition, see response to 8.18.1. **Free Trials:** Oracle Cloud delivers the broadest selection of enterprise-grade cloud computing solutions, including SaaS, PaaS, and IaaS. Visit us on the web at cloud.oracle.com to take a free cloud trial today!

8.18.3 Offeror must describe what training and support it provides at no additional cost.

Oracle Response:

CLOUD SERVICES SUPPORT

Oracle Cloud Services include the support described below and further defined in the service level agreement (SLA) documents in Attachment 7. Additional fees are applicable for additional Oracle support services that may be ordered by a Participating Entity

Support Services for Oracle Cloud consists of:

- Diagnosis of problems or issues with the Oracle Cloud Services
- Reasonable commercial efforts to resolve reported and verifiable errors in the Oracle Cloud Services so that they perform in all material respects as described in the associated Program documentation
- Support during change management activities described in the Oracle Cloud Change Management Policy
- Assistance with technical service requests 24/7
- 24/7 access to a Cloud Customer Support Portal designated by Oracle (for example, My Oracle Support) and live telephone support to log Service Requests
- Access to community forums
- Non-technical customer service assistance during normal Oracle business hours (8:00 to 17:00) local time

CLIENT SUCCESS SPECIALIST

Oracle believes in assisting its customers with understanding deployment of their data in the cloud not just through self service tutorials typically found in a SaaS-based world, but with people. The Client Success Specialist team works with the Oracle Account team and other members that may be assembled, such as an executive sponsor, for large enterprise data migration or cloud deployment developed solutions. A Client Success Specialist helps to look after your success after your implementation.

The implementation success manager helps during your startup and crossover. Of course your Oracle Account team is there to keep you informed of the latest and greatest innovations and help answer any questions you have along the way. Lastly, Oracle Support is there via phone, chat, and email to answer your most pressing questions.

People Committed to Your Success

Support for your business in the cloud



FIGURE 31: ORACLE PROVIDES COMPREHENSIVE CLOUD SUPPORT AT ALL LEVELS

Integration and Customization (RFP #8.19)

Provided below is the information requested in section 8.19 of the RFP.

8.19.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

Oracle Response:

INTEGRATION

A move to the cloud requires the agility to integrate easily with legacy applications, future applications, and other third-party technologies.

Integration Overview – Oracle’s solution has the ability to integrate (in real-time) with primary, secondary, and future systems, as discussed below. More specifically, we imagine that many system integrations will be bi-directional and employ one or more of the capabilities available below.

Integration Capabilities – Oracle Connect Service Cloud is a standards-based service-oriented architecture (SOA) framework that enables smooth integration to existing systems regardless of operating system, programming language, or hardware platform.

Integration Patterns – Oracle Connect Service Cloud provides a set of open, standards-based integration capabilities for the three integration patterns:

- **Data Integration** – Real-time access and synchronization of data regardless of location: back office, contact center, web, and social

- **Desktop Integration** – Extend, unify, and automate the Oracle Standard Dynamic Agent Desktop Service Cloud including agent workflow, scripting, and contextual workspaces
- **Web Integration** – Extending the CX experience to existing web products through integration of data and services at the application server, website, or Agent Desktop

Integration Methods – Oracle Connect Service Cloud Web Services for SOAP is used to communicate with Oracle’s solution from external systems, providing full CRUD (Create, Read, Update, Delete) access to data contained within Oracle’s solution.

Oracle Connect Service Cloud for PHP (HyperText Preprocessor) is used to extend or customize your web support experience in the Customer Portal. The PHP API is based on the Connect Common Object Model – (the same object model as Connect Web Services for SOAP), offering CRUD capabilities for the Connect Object Model.

Oracle Connect Service Cloud Desktop Add-In Framework is used to extend the Agent Desktop. It allows integration developers to build custom .NET components that live in the Agent Desktop of Oracle’s solution, and to automate, extend, and integrate the Agent Desktop with other systems to create a unified business process.

Custom Integration – In addition, Oracle offers custom integration offerings to seamlessly tie third-party technology with Oracle’s solution components. Oracle has integrated our products with everything from commercial enterprise software to custom-developed applications and other on demand services.

Oracle’s solution accelerators are designed to demonstrate how an integration scenario could be built using the public integration and extension capabilities of Oracle’s solution. They are provided to help customers and partners confidently leverage our platform to meet their own unique integration needs.

8.19.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

Oracle Response:

Oracle’s solution offers configuration throughout the system to adapt to your changing business needs by supporting the following configurations without the use of code:

- Specify system behavior, user roles, and permissions
- Extend the data model, support multiple business processes and policies
- Tailor dynamic campaign and survey flows, campaign online forms and staff user interfaces
- Automate workflow
- Report and analyze results

Oracle understands your need for a cloud-solution across diverse departments, recognizing their unique requirements and policies without sacrificing efficiency and agility of a single cloud solution. These fluid policies affect a broad lifecycle of citizen and employee advice, determinations, and compliance, yet each department needs to operate its own programs and ensure that the right information gets to the right people effectively and consistently.

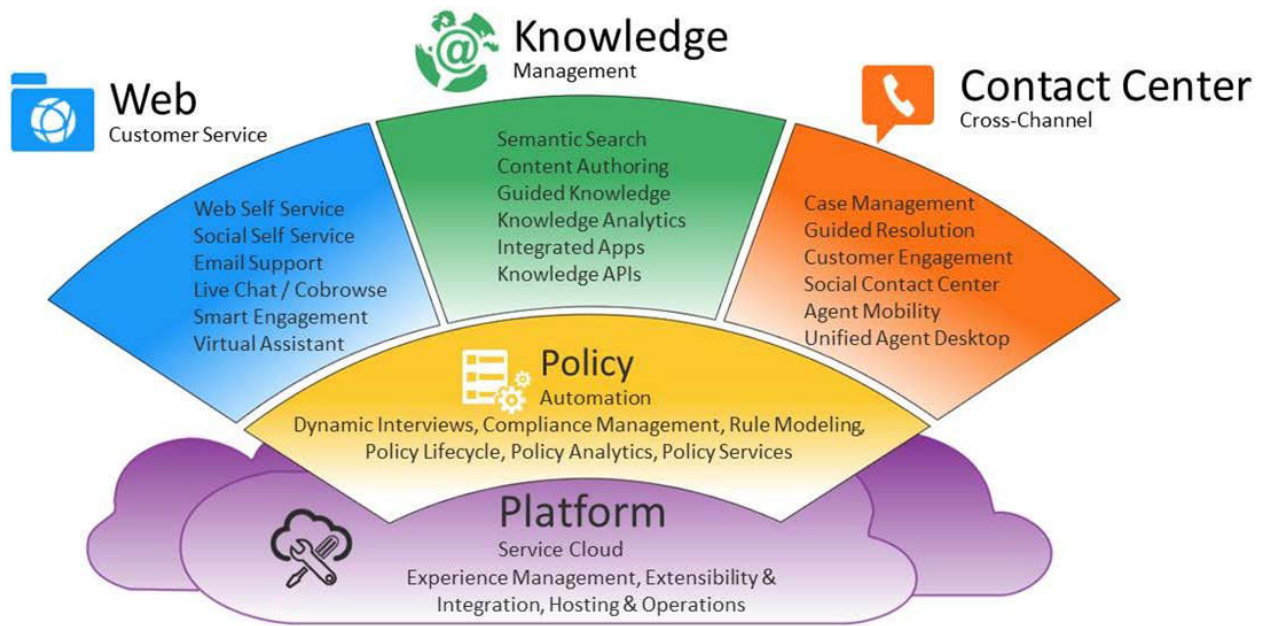


FIGURE 32: THE ORACLE SERVICE CLOUD FOOTPRINT

Marketing Plan (RFP #8.20)

Provided below is the information requested in section 8.20 of the RFP.

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Oracle Response:

It is contemplated that Oracle will be approved to release a press announcement and create supporting marketing materials that can be positioned to its extensive list of Public Sector customers that have an install base of Oracle on premise software and hardware. Oracle's dynamic position in the market allows for customers to maintain a portion of their architecture in an on premise environment while they explore the cloud for their approved cloud use cases. As a matter of standard Oracle offers to quote customer's expanding their use of Oracle or new Oracle products the cloud equivalent to the on premise solution which will be part of the marketing strategy to promote the use of the Master Agreement. A key to marketing the Master Agreement will be the hundreds of outside and inside sales representative that are engaged with customer daily promoting the Oracle entire architecture capabilities.

Oracle has an in-house marketing division that will be used for custom call, mail and electronic media campaigns to promote the use of the Master Agreement. Annually Oracle host several events including the global user conference known as Oracle OpenWorld and regional events such a Cloud Days and Tech Days throughout the country during which the master Agreement will be promoted to the target customers.

It is Oracle's intention to approach the Participating Entities to allow for the addition of authorized resellers by State who will also factor into the marketing and development of the Master Agreement through their direct marketing efforts.

Related Value-Added Services to Cloud Solutions (RFP #8.21)

Provided below is the information requested in section 8.21 of the RFP.

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

Oracle Response:

Please see response to 8.18.2. Additionally, Oracle Consulting Services (OCS) is a division of Oracle that offers complete resource for consulting, integration, development, and training. Our professionals provide the expertise, experience, and skills to assess and optimally apply our technology to your needs.

With almost a decade of experience and more than 3,000 successful implementations to its credit, OCS is the ideal resource for those essential skills, insight, and expertise. No other service organization in the world is better equipped to help you achieve the results you seek with the resources you have. And no other partner can bring you Day1 Advantage while also providing the long-term support you need to continuously optimize your frontline sales, marketing, and service processes.

Key capabilities offered by OCS for Oracle's cloud solutions include:

- Business process consulting services for needs assessment, project planning, implementation support, and ongoing performance optimization.
- Data migration readiness and portability planning.
- Integration services to ensure existing enterprise applications remain aligned with cloud services.
- Building customized solutions Customer training and information aware and materials for easy adoption.

Supporting Infrastructure (RFP #8.22)

Provided below is the information requested in section 8.22 of the RFP.

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

Oracle Response:

This is not applicable to our solution since its being sold "as a Service" hosted by Oracle.

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

Oracle Response:

This is not applicable to our solution since its being sold "as a Service" hosted by Oracle.

Alignment of Cloud Computing Reference Architecture (RFP #8.23)

Provided below is the information requested in section 8.23 of the RFP.

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

Oracle Response:

Yes, please refer to section 4 of Attachment 7.2, our Oracle Cloud Enterprise Hosting and Delivery Policies. The most recent copy of this living document is always available <http://www.oracle.com/us/corporate/contracts/cloud-ent-hosting-del-policies-1881438.pdf>.

In addition, the Oracle Service Cloud has been FedRAMP JAB Certified. JAB Provisional Authorizations: Cloud systems listed under the FedRAMP P-ATO path have undergone a rigorous technical review by the FedRAMP PMO, been assessed by a FedRAMP accredited 3PAO, and received a P-ATO from the DHS, DOD, and GSA CIOs.

The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a “do once, use many times” framework that saves an estimated 30% to 40% of government costs, as well as both time and staff required to conduct redundant agency security assessments. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.

7. Confidential, Protected or Proprietary Information

All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write “None” in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

Oracle Response:

Please refer to the following pages.

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

CLAIM OF BUSINESS CONFIDENTIALITY

Pursuant to Utah Code Annotated, Subsections 63G-2-305(1) and (2), and in accordance with Section 63G-2-309, Oracle America, Inc. (company name) asserts a claim of business confidentiality to protect the following information submitted as part of this solicitation. Pricing/Cost Proposals may not be classified as confidential or protected and will be considered public information. An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY".

- ☐ Non-public financial statements
- ☒ Specific employee name and contact information
- ☐ Specific customer information, client lists, or subscription lists
- ☒ Other (specify): Consensus Assessments Initiative Questionnaire and Compliance with Cloud Controls Matrix

This claim is asserted because this information requires protection as it includes:

☒ trade secrets as defined in Utah Code Annotated Section 13-24-2 ("Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy).

☒ commercial information or non-individual financial information obtained from a person if: (a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future; [and] (b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access.

This statement of reasons supporting the claim of business confidentiality applies to the following information in this proposal:

Page	Paragraph	Reason
Section 7	All of Oracle's Responses in Attachment 3 in Section 7	The Consensus Assessments Initiative Questionnaire (CAIQ) (RFP Exhibit B.1): These responses contain confidential and trade secret information of Oracle. These responses are compilations of information which is used in Oracle's business. This information is based on Oracle's proprietary offerings and is gleaned from a detailed review of Oracle's proprietary documentation. Compiling this information is a complicated task that took members of the Oracle technical teams many hours and which required them to go through and match each requirement in the RFP to a line in the documentation and determine whether or not, and to what degree, the Oracle offering meets the stated RFP requirement. This information clearly presents an opportunity to obtain an advantage over competitors responding to the same requirements, as they could compare how Oracle's offering measures to their own and use that information to become more competitive with Oracle in the future. In addition, this type of information is protected within Oracle and by Oracle in disclosing it to third parties. Oracle requires its employees to sign non-disclosure agreements whereby employees agree not to disclose Oracle proprietary and/or confidential information. Requests for Proposals

ORACLE

THE STATE OF UTAH
VALUEPOINT MASTER AGREEMENT FOR CLOUD SOLUTIONS

RFP #: CH16012

		relating to software and cloud services frequently contain functional requirements matrices, each of which is unique to the particular procurement. Oracle goes through the same line-by-line process for each such matrix and requirement and is very careful in labeling the information as proprietary and taking other reasonable measures to ensure its protection from unauthorized disclosure.
Section 7	All of Oracle's Responses in Attachment 4 in Section 7	Compliance with Cloud Controls Matrix (CCM) (RFP Exhibit B.2): These responses contain confidential and trade secret information of Oracle. These responses are compilations of information which is used in Oracle's business. This information is based on Oracle's proprietary offerings and is gleaned from a detailed review of Oracle's proprietary documentation. Compiling this information is a complicated task that took members of the Oracle technical teams many hours and which required them to go through and match each requirement in the RFP to a line in the documentation and determine whether or not, and to what degree, the Oracle offering meets the stated RFP requirement. This information clearly presents an opportunity to obtain an advantage over competitors responding to the same requirements, as they could compare how Oracle's offering measures to their own and use that information to become more competitive with Oracle in the future. In addition, this type of information is protected within Oracle and by Oracle in disclosing it to third parties. Oracle requires its employees to sign non-disclosure agreements whereby employees agree not to disclose Oracle proprietary and/or confidential information. Requests for Proposals relating to software and cloud services frequently contain functional requirements matrices, each of which is unique to the particular procurement. Oracle goes through the same line-by-line process for each such matrix and requirement and is very careful in labeling the information as proprietary and taking other reasonable measures to ensure its protection from unauthorized disclosure.
Section 5 Section 7	Section 5, Organization Profile All of Oracle's Responses in Attachment 10 in Section 7	Resume of Oracle Contract Manager: Oracle considers the names, contact information, and experience of its key personnel to be confidential commercial information that could injure Oracle if disclosed and competitors attempt to hire these employees away from Oracle. Oracle has a keen interest in prohibiting access to the names, contact information and expertise of employees to protect Oracle's competitiveness in the marketplace.

Please use additional sheets if needed.

You will be notified if a record claimed to be protected herein under Utah Code Annotated § 63G-2-305(1) or (2) is classified public or if the governmental entity determines that the record should be released after weighing interests under Utah Code Annotated § 63G-2-201(5)(b) or Utah Code Annotated § 63G-2-401(6). See Utah Code Annotated § 63G-2-309.

Mark C. Johnson
Mark C. Johnson (Title 8, 2016)

Signed: _____

On behalf of (company): Oracle America, Inc.

Date: Mar 9, 2016

(Revision 6/4/2015)

ORACLE

USE OR DISCLOSURE OF DATA CONTAINED ON THIS SHEET IS SUBJECT TO THE RESTRICTIONS IN THE LAST PARAGRAPH OF THE GENERAL

104

TERMS AND CONDITIONS OF ORACLE'S PROPOSAL INCLUDED IN THIS RESPONSE..

ORACLE CONFIDENTIAL

8. Exceptions and/or Additions to the Standard Terms and Conditions

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing. Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations.

If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

Oracle Response:

Oracle's exceptions and/or additions to the standard terms and conditions are presented in Attachment 8.

9. Attachments

Please refer to the following pages.

1. Acknowledgement of Amendments (RFP #5.3)

Please see the file entitled “1. Oracle Acknowledgement of Amendments to RFP #CH16012.pdf” in the zip file entitled “Oracle Attachments - RFP #CH16012.zip.”

2. Identification of Service Models (RFP Attachment H)

Please see the file entitled “Oracle Identification of Service Models (RFP Attachment H).docx” in the zip file entitled “Oracle Attachments - RFP #CH16012.zip.”

3. The Consensus Assessments Initiative Questionnaire (CAIQ) (RFP Exhibit B.1)

Please see the embedded file entitled “3. Oracle CAIQ (RFP Exhibit B.1).doc” in Section 7 (Confidential Information) of the digital version of this response.

4. Compliance with Cloud Controls Matrix (CCM) (RFP Exhibit B.2)

Please see the file entitled “4. Oracle CCM (RFP Exhibit B.2).xlsx” in Section 7 (Confidential Information) of the digital version of this response.

5. Oracle Annual Report FYE May 31, 2015

Please see the file entitled “5. Oracle 10K, FYE 31MAY 2015.pdf” in the zip file entitled “Oracle Attachments - RFP #CH16012.zip.”

A copy of Oracle’s most recent Form 10-K and Annual Report is available at:

<http://d1lge852tjjqow.cloudfront.net/CIK-0001341439/ee127b2b-13a7-4bdb-a384-d27bb7c5bddb.pdf>.

6. Oracle Annual Report FYE May 31, 2014

Please see the file entitled “6. Oracle 10K, FYE 31MAY 2014.pdf” in the zip file entitled “Oracle Attachments - RFP #CH16012.zip.”

A copy of Oracle’s 2014 Form 10-K and Annual Report is available at:

<http://d1lge852tjjqow.cloudfront.net/CIK-0001341439/495da947-b778-4d53-89be-fa66ffb9c3a9.pdf>

EARLIER FORM 10-K/ANNUAL REPORTS

Historical annual reports are available within the SEC Filings on the Financial Reporting tab at this website:

<http://investor.oracle.com/financial-reporting/sec-filings/default.aspx>.

7. Oracle Cloud SLAs

Oracle's Cloud SLAs are comprised of multiple parts depending of the cloud services ordered. The documents below are referred to in this response as Oracle's SLAs.

7.1. Hosting and Delivery Policies for PaaS

Please see the file entitled "7.1. Oracle Cloud Hosting and Delivery Policies (PaaS).doc" in the zip file entitled "Oracle Attachments - RFP #CH16012.zip."

7.2. Hosting and Delivery Policies for SaaS

Please see the file entitled "7.2. Oracle Cloud Enterprise Hosting and Delivery Policies (SaaS).doc" in the zip file entitled "Oracle Attachments - RFP #CH16012.zip."

7.3. Data Processing Agreement for Oracle Cloud Services

Please see the file entitled "Data Processing Agreement for Oracle Cloud Services.doc" in the zip file entitled "Oracle Attachments - RFP #CH16012.zip."

7.4. Oracle Cloud Services Agreement

Please see the file entitled "7.4. Oracle Cloud Services Agreement.docx" in the zip file entitled "Oracle Attachments - RFP #CH16012.zip."

8. Oracle Exceptions and/or Additions to Standard Terms and Conditions

Please see the file entitled “8. Exceptions to the standard T&Cs for RFP #CH16012.docx” in the zip file entitled “Oracle Attachments - RFP #CH16012.zip.”

9. Oracle's Services Privacy Policy

Please see the file entitled "9. Oracle's Services Privacy Policy.docx" in the zip file entitled "Oracle Attachments - RFP #CH16012.zip."

10. Résumé of Oracle's Proposed Contracts Manager

Please see the file entitled "Oracle Contract Manager Resume.doc" in Section 7 (Confidential Information) of the digital version of this response.

Attachment E**SAMPLE ORDERING DOCUMENT FOR REFERENCE PURPOSES ONLY****ORDERING DOCUMENT**

Oracle America, Inc.
500 Oracle Parkway
Redwood Shores, CA 94065

Your Name		Your Contact	
Your Location		Phone Number	
		Email Address	

Cloud Services		Services Period:				
Data Center Region:	Quantity	Term	List Fee	Discount %	Unit Net Price	Net Fee

Consulting / Professional Services Ordered	Quantity	List Fee	Discount %	Net Fee
Other Fees				

Fee Description	Net Fee
Cloud Services Fees	
Consulting / Professional Services Fees	
Total Fees	

A. Terms of Your Order**1. Agreement**

This ordering document incorporates by reference the terms of the NASPO ValuePoint Master Agreement and all amendments and addenda thereto by and between the State of Utah, as lead state, and Oracle America, Inc. ("**Oracle**"), together with the Participating Addendum and all amendments and addenda thereto by and between _____ and Oracle (the "**Master Agreement**," Oracle reference number: _____; NASPO ValuePoint reference number _____). The defined terms in the Master Agreement shall have the same meaning in this ordering document unless otherwise specified herein.

2. Payment Terms:

Net 30 days from invoice date

3. Payment Frequency:

Quarterly in arrears

4. Currency:

US Dollars

5. Offer Valid through:

_____, 20__

6. Services Period

The Services Period for the Services commences on the date stated in this order. If no date is specified, then the "Cloud Services Start Date" for each Service will be the date that the User login names and password are issued to you to access the Services, and the "Consulting/Professional Services Start Date" is the date that Oracle begins performing such services.

7. Service Specifications

Service Specifications applicable to the Cloud Services and the Consulting/Professional Services ordered may be accessed at www.oracle.com/contracts.

SAMPLE ORDERING DOCUMENT FOR REFERENCE PURPOSES ONLY

8. Customer Reference

Oracle may refer to You as an Oracle customer of the ordered Services in sales presentations, marketing materials and activities.

9. Renewal of Cloud Services

Notwithstanding any statement to the contrary in the Services Specifications, the parties expressly agree that the Cloud Services acquired under this order will not Auto-Renew.

B. Additional Order Terms

[Order-specific terms to be added]

[Customer Name]

Signature:

Name:

Title:

Signature Date:

Cloud Solutions
Contract No. 43230000-NASPO-16-ACS

Exhibit C

CONTRACTOR SELECTION JUSTIFICATION FORM

Customers must complete this Contractor Selection Justification Form and attach it to the Purchase Order.

Date: Click or tap here to enter text.

Contractor's Name: Click or tap here to enter text.

Service Model:

SaaS ☐

PaaS ☐

IaaS¹ ☐

1 In accordance with Rule 60GG-3.004, F.A.C., "The acquisition of data center services, including IaaS, will be accomplished by customer entities submitting a Service Request to the State Data Center."

Level of Risk:

Low Risk Data ☐

Moderate Risk Data ☐

High Risk Data ☐

Description of Services:

Click or tap here to enter text.

Estimated Total Contract Value: Click or tap here to enter text.

Justification for Selection of Contractor:

Click or tap here to enter text.

Completed By: Click or tap here to enter text.

Title: Click or tap here to enter text.