

Supplement 2

Project Requirements

TABLE OF CONTENTS

1.0	MOVED TO PART ONE: EXECUTIVE SUMMARY SECTION OF RFP	9
2.0	MOVED TO PART ONE: EXECUTIVE SUMMARY SECTION OF RFP	10
3.0	MOVED TO PART ONE: EXECUTIVE SUMMARY SECTION OF RFP	11
4.0	STATE / OFFEROR: BUSINESS PARTNER RELATIONSHIP	12
4.1	OVERVIEW.....	12
4.1.1	RFP ACTIVITY, DELIVERABLE AND INFORMATION CONVENTIONS.....	12
4.2	POTENTIAL BUSINESS MODELS	12
4.3	LEASE OF SOCC SPACE IN EXCHANGE FOR FACILITY AND OPERATING IMPROVEMENTS	13
4.4	PROHIBITION ON SUB-LEASING SOCC SPACE TO STATE AGENCIES, BOARDS, COMMISSIONS ...	14
4.5	CONTRACTOR USE OF SOCC 3 RD FLOOR FOR NON-STATE FUNCTIONS.....	14
4.6	PROVISION FOR INTERIM CONTRACTOR MANAGED SERVICES STAFFING DURING IMPLEMENTATION PERIOD.....	15
4.7	SPECIFIC STATE AND CONTRACTOR RESPONSIBILITIES AND DEPENDENCIES.....	15
4.7.1	CONTRACTOR RESPONSIBILITIES	16
4.7.2	CONTRACTOR STAFF.....	17
4.7.3	TERM AND STATE RESPONSIBILITIES	17
4.8	TERM AND TERMINATION	17
4.8.1	RETURN OF SOCC TO STATE.....	17
4.8.2	FACILITY RENOVATIONS AND IMPROVEMENTS	18
4.8.3	CONTRACTOR SOURCED AND MANAGED CONTRACTS	18
4.8.4	EXIT PERIOD	19
4.9	CONTRACTOR'S PROPERTY.....	19
4.10	STATE OWNED OR PROVIDED HARDWARE, SOFTWARE, NETWORKING AND ASSOCIATED MAINTENANCE	19
4.11	MANAGED SERVICE CONTRACT END TRANSITION SERVICES.....	20
4.11.1	CONTRACT END TRANSITION RESPONSIBILITIES	21
4.11.2	CONTRACT END TRANSITION SERVICES PLAN	22
4.11.3	CONTRACT END TRANSITION MANAGEMENT TEAM.....	22
4.11.4	CONTRACT END OPERATIONAL TRANSFER	23
4.12	STATE STANDARDS, SECURITY & PRIVACY AND OTHER PERTINENT INFORMATION	23
5.0	PROJECT MANAGEMENT REQUIREMENTS	24
5.1	OVERVIEW OF SCOPE	24

5.2	TEAM ORGANIZATION	25
5.2.1	25	
5.3	MOBILIZATION EFFORT.....	25
5.4	KICKOFF MEETING.	25
5.5	PROJECT PLAN DEVELOPMENT AND MANAGEMENT	26
5.6	MEETING ATTENDANCE AND REPORTING REQUIREMENTS	27
5.7	UTILIZE OIT’S DOCUMENT SHARING/COLLABORATION CAPABILITY	27
5.8	PROJECT COMMUNICATIONS	28
5.9	PROJECT MANAGEMENT METHODOLOGY, MINIMUM STANDARDS.....	28
6.0	WORK AREA 1: FACILITY POWER AND COOLING UPGRADES.....	32
6.1	IMPORTANT CONSIDERATIONS	32
6.2	CONTINUOUS OPERATIONS, UNSCHEDULED OUTAGE PERFORMANCE GUARANTEE	32
6.3	DEFINITIONS.....	33
6.4	CURRENT TECHNICAL SPECIFICS.....	34
6.5	PROVISION AND USAGE OF AN UN-PROTECTED POWER SOURCE.....	34
6.6	UPS – UNINTERRUPTED POWER ENHANCEMENTS.....	35
6.7	AIR CONDITIONING AND CHILLER ENHANCEMENT	36
6.8	FACILITY CONTROLS AND MANAGEMENT ENHANCEMENTS	36
6.9	FACILITY COOLING EFFICIENCY ENHANCEMENTS	37
6.10	FACILITY PROCESSES AND DOCUMENTATION ENHANCEMENTS	37
7.0	WORK AREA 2: AGENCY COMPUTING MIGRATION.....	39
7.1	OVERVIEW.....	39
7.2	2ND FLOOR PHYSICAL REDESIGN ACTIVITIES.....	40
7.3	IMPLEMENTATION OF 2ND FLOOR IMPROVEMENTS	41
7.4	POWER PROFILE ASSESSMENT, ASSIGNMENT AND IMPLEMENTATION	41
7.5	DETAILED MIGRATION PLANNING TASKS	43
7.6	AGENCY COMMUNICATIONS AND READINESS ACTIVITIES.....	45
7.7	SOCC PHYSICAL ENVIRONMENT MIGRATION EXECUTION	45
7.8	SOCC VIRTUAL MIGRATION EXECUTION	48
7.9	MIGRATION TESTING AND VALIDATION	50
7.10	AGENCY VALIDATION TESTING SUPPORT	51
7.11	CONSOLIDATION OF SOCC NETWORK MANAGEMENT CENTERS & FUNCTIONS	51
7.11.1	CURRENT STATE: HIGH LEVEL SOCC NETWORKING AND CONNECTIVITY INFORMATION	53
7.12	MIGRATION TO PRODUCTION STEADY STATE OPERATIONS (MANAGED SERVICE)	55

7.13	COMPUTING INFRASTRUCTURE MIGRATION PROCESS REFINEMENT AND DOCUMENTATION .	56
8.0	WORK AREA 3: SOCC OPERATING MODEL IMPROVEMENTS	57
8.1	SPECIFIC ITIL PROCESSES TO BE DESIGNED AND IMPLEMENTED	57
8.2	USE OF STATE EMPLOYEES FOR ONGOING MANAGED SERVICES OPERATIONS.....	59
8.3	DETERMINING SPECIFIC INITIAL AND FINAL OPERATIONAL ROLES AND RESPONSIBILITIES AND STAFFING LEVELS.....	60
8.4	KEY CONTRACTOR PERSONNEL.....	61
8.5	TRAINING PROGRAM, KNOWLEDGE TRANSFER, AND CHANGE MANAGEMENT	62
8.5.1	TRAINING DESIGN	64
8.5.2	TRAINING DELIVERY	65
8.5.3	POST-TRAINING RESPONSIBILITIES	65
8.5.4	CHANGE MANAGEMENT	66
8.5.5	KNOWLEDGE AND SKILL TRANSFER / VALIDATION	67
8.6	ORGANIZATION OF SERVICE DELIVERY AREAS:	67
8.7	DESIGN SERVICES.....	67
8.7.1	PLANNING AND ANALYSIS SERVICES	67
8.7.2	STATE INFRASTRUCTURE ENVIRONMENT DESIGN-BUILD SERVICES	68
8.7.3	MIGRATION SERVICES	71
8.8	DESIGN, IMPLEMENT AND PROVIDE ONGOING STEADY-STATE RUN SERVICES.....	72
8.8.1	STEADY STATE OPERATIONS AND MAINTENANCE SERVICES	72
8.9	DESIGN AND IMPLEMENT NON-DISCRETIONARY SERVICES	73
8.9.1	LEVEL 2 AND 3 SUPPORT.....	73
8.9.2	BREAK/FIX SUPPORT	73
8.9.3	ENVIRONMENT TECHNICAL SUPPORT.....	74
8.9.4	SYSTEM/ENVIRONMENT ADMINISTRATION SUPPORT	74
8.9.5	ENVIRONMENT PREVENTIVE MAINTENANCE	74
8.9.6	PRODUCTION CONTROL AND SCHEDULING	75
8.9.7	OPERATIONS SUPPORT.....	75
8.9.8	SOLUTION AND OPERATIONS REPORTING.....	76
8.9.9	AD-HOC REQUESTS	76
8.9.10	MINOR INFRASTRUCTURE ENHANCEMENTS.....	76
8.9.11	DATA CENTER AND INFRASTRUCTURE MANAGEMENT SERVICES	77
8.9.12	SYSTEMS MANAGEMENT AND ADMINISTRATION	77
8.9.13	SECURITY SERVICES	78

8.9.14	IT NETWORK CONNECTIVITY & MONITORING SERVICES.....	79
8.10	SOLUTION DOCUMENTATION.....	80
8.11	QUALITY ASSURANCE	80
8.12	SERVICE DESK DESIGN AND IMPLEMENTATION	81
8.12.1	SIZING CONSIDERATIONS: INFRASTRUCTURE SERVICES DIVISION (ISD) CALL CENTER	81
8.12.2	PROBLEM MANAGEMENT	82
8.12.3	ADDITIONAL SERVICES.....	82
8.12.4	SERVICE DESK TOOLS	82
8.13	IT INFRASTRUCTURE MANAGEMENT SERVICES	83
8.13.1	CAPACITY PLANNING	83
8.13.2	CONTINUOUS IMPROVEMENT	83
8.13.3	IT INFRASTRUCTURE PROVISIONING	83
8.13.4	DISASTER RECOVERY (DR) AND BUSINESS CONTINUITY (BC) SUPPORT PROCESSES	83
9.0	ONGOING FACILITY TECHNICAL MANAGEMENT SERVICES.....	86
9.1	OVERVIEW.....	86
9.2	DOCUMENT LIBRARY	86
9.3	WORK REQUIREMENTS.....	86
9.4	INTERIOR AIR QUALITY TEST	87
9.5	WIRING MAINTENANCE PLAN	87
9.6	FACILITY TECHNICAL SYSTEM MAINTENANCE	88
9.7	EXCLUDED SERVICES	89
9.8	HVAC OPERATION AND MAINTENANCE.....	89
9.9	LIMITED GENERAL CONSTRUCTION	90
9.10	STAFFING REQUIREMENTS	90
9.10.1	TECHNICAL MANAGER (ON-SITE):.....	90
9.10.2	BUILDING ENGINEER.....	91
9.10.3	REGISTERED COMMUNICATIONS AND CABLING DESIGNER	91
9.10.4	BUILDING ELECTRICIANS.....	92
9.11	DRUG TESTING	92
9.12	EXCLUSIONS	92
9.13	TRANSITION PERIOD.....	92
9.14	BUILDING OPERATION PLAN.....	92
9.15	SYSTEMS MAINTENANCE PLAN.....	93
9.16	PROPERTY MANAGEMENT APPROACH.....	94

9.17	TENANT COMPLAINT RESOLUTION PLAN.....	94
9.18	QUARTERLY TENANT MEETINGS.....	94
9.19	SITE DISASTER RECOVERY PLAN.....	94
9.20	TRANSITION PLAN	94
9.21	SUPPORT REQUIREMENTS.....	94
10.0	WORK AREA 4: SOCC AND SERVICE GOVERNANCE IMPLEMENTATION	96
10.1	SCOPE OF GOVERNANCE TO BE IMPLEMENTED	97
10.2	IMPLEMENTING ROLES & RESPONSIBILITIES FOR SOCC SERVICES.....	98
10.3	ESTABLISHMENT OF SERVICE MANAGEMENT OVERSIGHT COMMITTEE	99
10.4	CREATION OF A DISPUTE RESOLUTION CAPABILITY	99
10.5	OTHER GOVERNANCE PROCESSES TO BE IMPLEMENTED.....	99
10.5.1	REMEDIATION PROJECT COMMUNICATIONS AND OVERSIGHT	99
10.5.2	CHANGE AND SCOPE MANAGEMENT/AUDIT COMPLIANCE.....	99
10.5.3	EFFICIENCY OVERSIGHT AND OPTIMIZATION	99
10.5.4	ADMINISTRATION	99
10.5.5	AUDIT AND ENFORCEMENT.....	100
10.5.6	POLICY AND STANDARDS	100
11.0	SERVICE LEVELS AND STANDARDS.....	101
11.1	SERVICE LEVELS AS A RESULT OF “CO-MANAGED” SERVICES.....	101
11.1.1	DETERMINATION OF SERVICE LEVEL FAULT	101
11.1.2	OTHER SLA PRINCIPLES PERTINENT TO DETERMINATION OF FAULT AND CREDITS	103
11.2	SERVICE LEVEL FRAMEWORK.....	103
11.3	SERVICE LEVEL SPECIFIC PERFORMANCE CREDITS.....	104
11.4	SERVICE LEVEL EXCLUSIONS AND OTHER CONSIDERATIONS.....	105
11.5	TREATMENT OF FEDERAL, STATE, AND LOCAL FINES RELATED TO SERVICE DISRUPTION	105
11.6	OVERALL CONTRACT PERFORMANCE	106
11.7	MONTHLY SERVICE LEVEL REPORT.....	106
11.8	CRITICAL AND NON-CRITICAL APPLICATIONS.....	106
11.9	PERIOD SERVICE LEVEL IN FULL EFFECT AND IN-PROGRESS SERVICE LEVELS	107
11.10	SERVICE LEVEL REVIEW AND CONTINUAL IMPROVEMENT.....	107
11.10.1 SERVICE LEVEL AGREEMENT REVIEW AND CHANGE PROCESS	107
11.10.2CONTINUOUS IMPROVEMENT	108
11.11	MONTHLY SERVICE LEVEL REPORT.....	108

11.12	SERVICE LEVEL SCOPE	108
11.13	SERVICE LEVEL TARGETS	109
11.14	SERVICE LEVEL SPECIFICATIONS	110
11.14.1	INCIDENT RESOLUTION – MEAN TIME TO REPAIR (PRIORITY 1 OUTAGES)	110
11.14.2	INCIDENT RESOLUTION – MEAN TIME TO REPAIR (PRIORITY 2 OUTAGES)	111
11.14.3	INCIDENT RESOLUTION – MEAN TIME TO REPAIR (PRIORITY 3 OUTAGES)	112
11.14.4	INCIDENT RESOLUTION - ISSUE TRIAGE, CLOSURE AND RECIDIVIST RATE	113
11.14.5	SERVICE AVAILABILITY – NON CRITICAL INFRASTRUCTURE AVAILABILITY	114
11.14.6	SERVICE AVAILABILITY – VIRTUAL SERVER AVAILABILITY	115
11.14.7	SERVICE AVAILABILITY – DATA CENTER LAN AVAILABILITY	116
11.14.8	CAPACITY MONITORING & PLANNING – CAPACITY UTILIZATION	117
11.14.9	SCHEDULED PROVISIONING – VIRTUAL MACHINES	118
11.14.10	SCHEDULED PROVISIONING – PHYSICAL MACHINES	119
11.14.11	USER INTERACTION - COMPLETION OF ADMINISTRATIVE USER DELETES	120
11.14.12	USER INTERACTION - COMPLETION OF ADMINISTRATIVE USER ADDS & CHANGES	121
11.14.13	SECURITY – SECURITY COMPLIANCE	122
11.14.14	SECURITY – ANNUAL SECURITY REVIEW	123
11.14.15	MONITORING & AUDITING – SECURITY BREACH DETECTION	124
11.14.16	ASSET MANAGEMENT & REFRESH – ASSET INVENTORY ELEMENT ACCURACY	125
11.14.17	CAPACITY MONITORING AND USAGE REPORT	126
11.14.18	OPERATIONAL PROCESS CONTROL & REPEATABILITY – CHANGES TO PRODUCTION ENVIRONMENTS	127
11.14.19	SYSTEM PERFORMANCE & RESPONSIVENESS	128

11.14.20	SERVICE QUALITY – SYSTEM CHANGES	129
11.14.21	SERVICE TIMELINESS – SYSTEM CHANGES	130
11.14.22	SERVICE LEVELS – DELIVERY DATE COMPLIANCE	131
12.0	CONTRACT GOVERNANCE AND CHANGES	132
12.1	REGULAR MEETINGS AND CONFERENCE CALLS	132
12.2	SYSTEM CHANGES	132
12.3	EXTRAORDINARY EVENTS	132
12.4	DISPUTE RESOLUTION	133
12.4.1	INFORMAL DISPUTE RESOLUTION	133
12.4.2	INTERNAL ESCALATION	133
12.4.3	ESCALATION FOR REPETITIVE SERVICE LEVEL FAILURES	134
12.4.4	NO TERMINATION OR SUSPENSION OF SERVICES	134
12.5	BILLING, INVOICING AND REPORTING	134
12.5.1	BILLING FORMAT AND TIMING	134
12.5.2	BILLING DETAIL	134
12.5.3	INVOICING	134
12.5.4	REPORTING	134
12.5.5	BACK-UP DOCUMENTATION	135
12.5.6	CORRECTION OF ERRORS	135
12.5.7	COST OF LIVING ADJUSTMENTS	135
12.6	BENCHMARKING	135
12.6.1	GENERAL	135
12.6.2	FREQUENCY & DESIGNATION OF BENCHMARKER	136
12.6.3	METHODOLOGY	136
12.6.4	STANDARD	137
12.6.5	ADJUSTMENTS	137
12.6.6	DISPUTES	138
12.6.7	CHARGES REVIEW	138
12.7	CONTRACTOR BEST PRACTICES	138
12.8	MEETINGS	138
12.9	OBLIGATIONS	138
12.10	SSAE 16 TYPE 2 REPORTING	138

12.11 **AUDIT** 139

12.11.1 **ONSITE OPERATIONAL AND FINANCIAL EXAMINATIONS**
..... 139

12.11.2 **CONSENT TO EXAMINATIONS**
..... 139

12.11.3 **RIGHT TO TERMINATE AS A RESULT OF AUDIT FINDINGS**
..... 139

12.12 **CRIMINAL BACKGROUND CHECK OF PERSONNEL** 139

12.13 **CONFIDENTIALITY** 140

12.14 **HANDLING THE STATE’S DATA** 141

12.14.1 **RETURN OF STATE DATA**
..... 142

12.14.2 **CONFIDENTIALITY AGREEMENTS**
..... 143

1.0 Moved to Part One: Executive Summary Section of RFP

This page is intentionally left blank

2.0 Moved to Part One: Executive Summary Section of RFP

This page is intentionally left blank

3.0 Moved to Part One: Executive Summary Section of RFP

This page is intentionally left blank

4.0 State / Offeror: Business Partner Relationship

4.1 Overview

As part of this Project, the State wishes to establish a Contract with a highly Qualified Offeror to implement the requirements of the project contained herein, as well as to take an active role in the ongoing operation of the SOCC.

4.1.1 RFP Activity, Deliverable and Information Conventions

To assist offerors in responding to the RFP, the following notation conventions have been adopted throughout Supplement 2 of this RFP:

- Activities, responsibilities, work products and other delivery artifacts are formatted as per this sentence preceded by a square bullet (■).
- ★ Items that require a formal deliverable, State review and acceptance or may result in payment approval (if applicable) are formatted per this sentence and are preceded by a red star (★) and items that are elements, components or clarifying elements of a deliverable are marked with a red square (■).
- Items that are additive, clarifying or attributes of an activity, deliverable, work product and/or responsibility are formatted as per this sentence and preceded by an arrow point (➤).

4.2 Potential Business Models

The State has developed a variety of revenue estimating models for commercial data centers using data gathered in the fall of 2010. Under these revenue models, there appears to be an opportunity to offset the State's cost of operating the SOCC in part or in total. Offerors should note that the State is not in the business of operating the facility on a "for profit" basis, but would welcome business models that could reduce the overall operating cost of the facility as well as funding the remediation, consolidation and optimization efforts described elsewhere in this document.

The business models (and variations) that follow in this section may be subject to, or influenced by, provisions associated with the availability of capital funding, the outcome of mid-biennial budget review processes and other factors that are outside of the scope of this RFP. These provisions are anticipated to conclude coincident with the close date of this RFP. At this time the State believes that these business models are conceptually feasible and can be implemented by the State and Contractor. Should conditions change during the RFP process, the State will notify offerors affected by the change as to the impact of the change via the process described in the RFP.

The State wishes to establish a partnering arrangement that results in the best possible outcome and business value to the State for one or more of the following scenarios which are not necessarily mutually exclusive:

1. The State identifies **qualified market interest** in providing capital to the State to complete the remediation of the SOCC and consolidation of agency computing environments, data center processing and services in the SOCC and works with the State in one or more of the following:
 - a. Delivery of certain Data Center services to the State under the defined Statement of Work (Collectively Sections 5.0 – 12.0 of this Document) and under a set of binding service level agreements;
 - b. Assisting the State in consolidating all non-SOCC data centers to the SOCC while driving incremental revenue to the SOCC (to offset the cost of improvements in the remediation/consolidation process) under a separate Statement of Work or RFP solicitation;
 - c. Assisting the State in migrating higher education, K-12 and, pending the award of grants, OSC to utilize the SOCC to a higher degree under a separate Statement of Work or RFP solicitation.
2. The State **determines, in consideration of offeror proposals, that there is qualified market interest** for occupants for lease of unused space at the SOCC (generally the 3rd Floor of the facility) in exchange for tenant occupancy fees (e.g., "rent") to be based on commercially reasonable rates while deriving some form of

mutually equitable revenue share designed to offset the cost of remediating the SOCC and otherwise performing the activities described within this RFP.

Offerors are encouraged to design their responses and propose a business partnership leveraging one or more of the preceding concepts to the State in such as manner as to:

1. Minimize the State’s direct investment and costs in realizing the objectives contained in this RFP;
2. Ensure that all objectives, deliverables, work products and activities required by this RFP are delivered as per specification;
3. Design their responses and cost proposals in such a manner as to reduce or eliminate any “up front” investment or costs by the State and include the SOCC remediation costs, capacity increases and operational process optimization activities within an ongoing recurring fee to the State that is reduced or offset by any revenues paid by the State and/or via commercial, private or public 3rd parties via use of data center space within the SOCC.

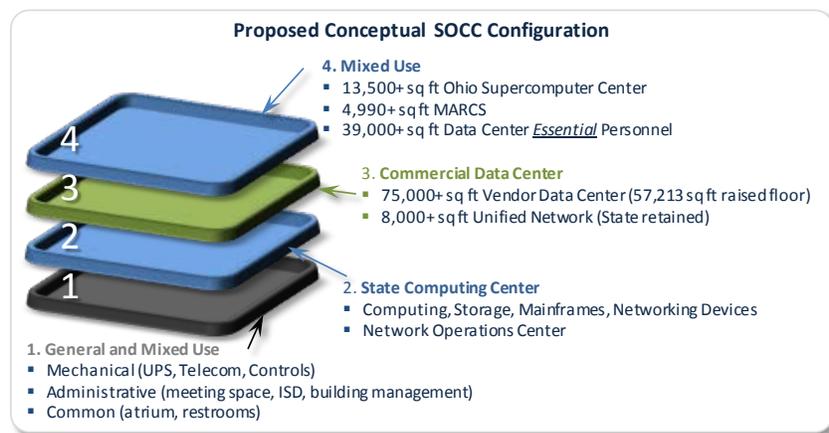
4.3 Lease of SOCC Space in Exchange for Facility and Operating Improvements

Each floor of the SOCC is approximately 85,000 sq. ft. of raised floor (and an approximately 15,000 sq. ft. of administrative and common space). So, in consideration of the State’s needs, as much as an entire floor could be made available to other non-State tenants. The State has a preference to assist State agencies, boards and commissions in the facility initially, but in consideration of even those needs, there could be substantial computing space available for other purposes. The State has also considered the universities in Ohio, Ohio Supercomputer, as well as K-12 education entities as “preferable potential tenants” as this would maximize the continued use of the facility for public benefit.

Qualified Offerors will have access to, as part of the Document Library, detailed floor plans for specific sizing, layout and access details, but in general the State will retain the Network Services Computer Room (currently 3,817 sq ft) as well as the immediately adjacent space (approximately 4,382 sq ft) for potential future State growth. Considering the net of the State’s modest occupancy of the 3rd floor, the Contractor will have approximately 57,213 square feet of useable raised floor space (of an approximate 77,000 total space) for the provision of data center services.

The Contractor will have secure access to the 3rd floor of the SOCC via integrated building security, and is otherwise responsible for all activities inclusive of building improvements, provision of power, cooling, telecommunications, cabling and other elements required to deliver commercial data center services. Offerors are to note that the space is provided on an as is, where is basis.

As a conceptual “end-state” the specific arrangement by floor of the SOCC could be viewed as the following.



Under this proposed scenario, high level concepts for offerors to consider include the following:

- Locate all State computing functions on 2nd floor to leverage existing large agency installations (DAS, OIT, Ohio Department of Job and Family Services (ODJFS), Ohio Department of Taxation (TAX)) and minimize move requirements;
- Consider investment in the SOCC for State Functions inclusive of building power uplifts, consolidating State computing onto the 2nd Floor and leading the retooling infrastructure operations
- Relocate all non-essential SOCC based State personnel to agency locations and State essential personnel to the 1st and 4th floors of the facility;
- Use (following Contractor refurbishment) of the 3rd Floor (less UNS) which effectively would become the Contractor Commercial Data Center. Additional power required for Contractor operations, to paid for by the Contractor;
- Note that additional cooling may be required depending on aggregate compute density, in support of commercial operations must paid for by the Contractor; and
- The Contractor provides managed infrastructure services to the State using a combination of State and Contractor employees.

In this RFP the terms “Leased Premises”, “Contractor Space”, “Contractor Data Center or Commercial Data Center” and other similar variants shall generally refer to the third floor of the SOCC in its entirety excepting the aforementioned UNS and expansion space as well as access and egress via existing facility features such as elevators, stairs freight elevators and the like.

4.4 Prohibition on Sub-Leasing SOCC Space to State Agencies, Boards, Commissions

The primary use of the SOCC historically has been, and shall be for the term of this Contract for the provision of a secure data center facility for purposes of providing computing functions to State Agencies, Boards and Commissions, collectively “State Bodies”. Therefore use of the facility by State Bodies shall be via established rated services provided by the Department of Administrative Services to State Bodies. The Contractor is expressly prohibited from independently soliciting or contracting State Bodies for sub-let, tenant or other relationship for the Contractor leased space (i.e., the 3rd Floor of the SOCC).

Should the Contractor seek to engage a Local Government (e.g., City, County, Municipality) that is not a State Body as a commercial tenant for sub-lease of the Contractor leased space (i.e., 3rd Floor of the SOCC), the State must be informed of the relationship between the Local Government entity and the Contractor prior to completion of contracting activities. Further, the Contractor shall offer services to Local Governments at a cost and rates no less favorable than those provided to State Bodies.

Should the Contractor obtain a separate contract with the State to provide system hosting capabilities for a State application or service where, subsequent to the award of this RFP to the Contractor, the Contractor and State determine to re-host the application or service from another Contractor location to the SOCC, the State requires this system or service to utilize State space within the SOCC (i.e., not Contractor sub-let space). In the event that it is determined by the Contractor and the State agency that due to commercial, technical, timing or availability reasons that the 3rd Floor (i.e., Contractor sub-let space) is more appropriate, the following conditions shall apply: i) the Contractor shall notify the State of the requirements and rationale for not using State portions of the SOCC; ii) the Contractor shall not charge in excess of prevailing market rates as enjoyed by other non-State sub-tenants of the Contractor on the 3rd Floor for similar services; and iii) the Contractor shall not as a direct result of moving the application or service to the SOCC charge in excess of Contractor provided rates without the written approval of the State CIO.

4.5 Contractor Use of SOCC 3rd Floor for Non-State Functions

Should the Contractor sub-lease the 3rd Floor (or portions of the 3rd Floor) of the SOCC from the State, the Contractor shall be able to use the 3rd Floor of the SOCC for non-State functions under the following set of conditions:

The primary use of the sub-leased portion of the SOCC must be in keeping with the provision and operation of data center services offered by the Contractor to the Contractor's customers.

The Contractor Customer's may include any private, public, governmental entity (subject to the exclusions in section 4.4) that are for-profit or non-profit. The Contractor may additionally use the sub-leased portion for its own use.

The Contractor's customer must not be listed as an organization on the U.S. Department of State Terrorist Exclusion List (TEL), have used any position of prominence the customer has with any country to persuade others to support an organization on the TEL; have committed an act that the Contractor knows, or reasonably should have known, affords "material support or resources" to an organization on the TEL; have hired or compensated a person the Contractor knew to be a member of an organization on the TEL; or have supported a person or company the Contractor knows, or reasonably should have known, to be engaged in planning, assisting, or carrying out an act of terrorism.

The Contractor shall implement procedures, physical security measures and controls as to prohibit any unauthorized access to any State resource whether by physical or logical network or otherwise. Unauthorized access to any State property, system, network, software, facility that are not associated with Contractor services to the State described herein by any party under the Contractor's control that are not directly involved in providing services to the State, is prohibited.

The Contractor shall adhere to mutually agreed, and then current, building access policies which include, but are not limited to: scheduled access requests; sign-in/out procedures inclusive of proof of identity; machine based and physical scans and inspection of personal effects (e.g., cell phone, laptops, brief cases and the like) by State provided security personnel.

The Contractor shall adhere to mutually agreed, and then current building equipment shipment and package scanning procedures which in general include, but are not limited to: delivery of all packages and shipments to the building loading dock; verification that packages and shipments do not contain any items that could jeopardize State functions within the facility such as weapons, toxic chemicals and explosives; and ensure that any shipments that are not associated with State functions are clearly marked and received by the Contractor as to not be confused with State functions (e.g., Customer equipment should not be mixed with State equipment and clearly marked as such, or in the case of confidential customers of the Contractor marked as FBO "Contractor" – NOT FOR STATE USE).

For the avoidance of doubt, the Contractor, and by extension the customers of the Contractor are expressly forbidden from conducting any electronic surveillance or otherwise hampering, impairing, blocking or interfering with State systems or networking operations or functions in the SOCC.

4.6 Provision for Interim Contractor Managed Services Staffing during Implementation Period

The State acknowledges that in order to realize the highest degree of efficiency for State resources, in consideration of certain "legacy knowledge" maintained by the State, the need to implement contemporary data center management and operations functions associated with ITIL, and to convey operational knowledge to Contractor personnel, it may be necessary to allow the Contractor to provide a level of Interim Managed Services Staffing until such time as the final Steady State Run organization is performing within the parameters required by this RFP.

Should interim Contractor Managed Services staffing be proposed based on offeror expertise and experience, the costs must be included in the Offeror Cost Summary Response. Under no circumstances will the State allow the Contractor to recover costs for these resources unless proposed, included in the Cost Summary Response, accepted and authorized by the State.

4.7 Specific State and Contractor Responsibilities and Dependencies

As part of this Project, the State and the Contractor will have specific responsibilities and dependencies on one another as follows.

4.7.1 Contractor Responsibilities

The Contractor has the following responsibilities:

- Provide Project Management Services to the State as required in section 5.0 of this RFP;
- Implement the project requirements as specified herein inclusive of: implementing **SOCC Agency Computing Migration** (section 7.0 of this RFP), implementation of **SOCC Operating Model Improvements** (section 8.0 of this RFP) and implementation of **SOCC and Service Governance** (section 10.0 of this RFP);
- On an ongoing basis, provide facility technical management services to the State for all tenants of the SOCC as required by section 9.0 of this RFP;
- Provide all services, facility improvements and renovations as required by section 6.0 of this RFP inclusive of:
 - Power upgrades (e.g., commercial power provision, integration); power distribution, balancing and management devices (e.g., transformers, switches, cabling, regulators, circuit breakers);
 - Power conditioning devices (e.g., surge protection, line management devices);
 - Power routing and availability devices (e.g., UPS, batteries, fuel cells or other uninterruptable power elements);
 - Relocation of in-building power and cooling devices (e.g., PDU and CRAC units) within the facility as required;
 - Demolition of existing suite walls and replacement with Contractor provided cages or other mechanisms to maximize the overall physical security of agency computing as well as the cooling and operational efficiency of State computing functions; and
 - Sufficient redundancy to maintain the overall availability profile of the facility as a Tier III capable data center.
- Be responsible for all costs associated with designing and implementing any and all improvements to the 3rd floor of the SOCC for the Contractor's use over the term of the Contract.
- Pay before any fine, penalty, interest or costs that may be added thereto, all taxes; excises; levies; license, permit fees, and other assessments; and water and sewer rents, rates and charges which may be assessed, levied, confirmed, imposed upon or become due and payable out of, or in respect of, the Leased Premises or the Building.
- Maintain in a good state of repair or working order the Leased Premises, including, but not limited to, exterior walls, roof, structural portions of the building, windows and sashes, entrance doors, fire escapes, sprinkler systems and controls, heating, venting and air conditioning systems, inside stairways and elevators, and electrical and plumbing facilities so that the Contractor may conduct its business therein at all times.
- Assume liability for plate glass breakage and replace same.
- Provide all equipment and materials necessary for installation and usage of telecommunications (voice, data and otherwise) service in the Leased Premises, where such equipment and materials are not provided by the telephone company.
- Pay all utility costs, except telecommunications services provided to the Leased Premises occupied or used by the State.
- Prior to assuming possession of the Leased Premises, change all door locks or security mechanisms and provide two (2) keys for each lock.
- Provide heating and air conditioning at 68°F - 74°F uniformly throughout the Leased Premises regardless of outside temperatures, subject only to governmental energy conservation controls.
- Provide hot and cold running water and chilled drinking water.
- Provide complete preventive maintenance for the building's mechanical systems.
- Provide access to and assessment of the building for the purpose of determining cost effective methods of increasing energy efficiency.
- Cooperate with the State to implement cost effective methods of increasing energy efficiency.

- Permit the State or its agent(s), upon twenty-four (24) hours advance notice, to enter upon the Leased Premises to examine same or to make such repairs or improvements as may be necessary to eliminate hazards to the health and safety of the occupants and the general public or to make any other repair or maintenance required hereunder. Provided, however, that the State or its agent may immediately enter upon the Leased Premises for the purpose of making emergency repairs but must promptly give notice to the Contractor of any such entry.

Additionally, the Contractor must perform/provide the following:

- Payment of all rentals as they become due.
- Abide by such reasonable rules and regulations promulgated in writing by the State to assure the proper operation of the Leased Premises, provided such rules and regulations are not inconsistent with the terms of the lease.
- Comply with any applicable laws, ordinances, orders, rules, regulations and requirements of all federal, state or municipal governments relating to the Contractor's use and occupancy of the Leased Premises.
- Pay for all telephone services furnished to the Leased Premises by the State.

4.7.2 Contractor Staff

The Contractor must provide resources for the work described herein. A Contractor resource must be a natural person who is a lawful permanent resident as defined in 8 U.S.C. 1101 (a)(20) or who is a protected individual as defined by 8 U.S.C. 1324b(a)(3).

4.7.3 Term and State Responsibilities

The State will provide the Contractor use of the third floor of the SOCC for purposes of providing commercial data center services for the Contract term which is intended for approximately a 10-11 year period.

Additionally, the State will:

- Provide and maintain landscaping and landscape services for all unpaved areas of the Leased Premises and the building;
- Provide timely removal of snow and ice from sidewalks and parking areas on or adjacent to the Leased Premises, and also provide adequate trash removal on a weekly basis;
- Provide adequate exterior lighting for the Leased Premises and such other security for the Leased Premises as the Contractor must reasonably determine to be necessary; and
- Provide for the extermination of, and keep the Leased Premises free from, infestation of rodents, pests, and other vermin.

The State will provide a Lease to the Contractor for a period consistent with the term of the Contract.

In no way will the State be responsible during the period of the lease or during any period of Contractor use of the SOCC, paid or otherwise, for any activities, revenues, lost revenues or profits, future profits, losses or any other Contractor impacting financial situation arising from the Contractor's lease or use of the 3rd Floor of the SOCC.

4.8 Term and Termination

Following the completion of the term of the Contract including any subsequent, executed renewals between the Contractor and the State, the following must apply.

4.8.1 Return of SOCC to State

The Contractor must not commit or suffer any waste on the Leased Premises. Upon the expiration of any term of the lease or upon an earlier termination hereof, the Contractor must surrender possession of the Leased Premises in substantially as good a condition as the same existed at the commencement date, except for (a) damage from fire or natural elements, (b) circumstances beyond the control of the Contractor, (c) reasonable use and normal

wear and tear, depreciation and decay, and (d) the Contractor improvements and any alterations, fixtures, additions, structures, or signs placed or erected upon the Leased Premises by either the State or the Contractor after the commencement date of the Contract. Provided, however, if the Contractor desires to remove the Contractor improvements and/or any of the items set forth herein, then the Contractor must repair all damage caused in the course of any such removal(s).

4.8.2 Facility Renovations and Improvements

All permanent facility renovations purchased, installed or implemented by the Contractor must convey to the State at the conclusion of the Contract term or upon termination of the Contract.

The following are considered to be permanent facility renovations:

- Demolition, repair, or replacement of existing walls, raised floors, cages and other physical security devices or mechanisms;
- Installation of any power or cooling distribution devices such as power distribution units (PDU), HVAC distribution devices such as CRAC units, cold water feeds/returns, power or cooling monitoring equipment or devices;
- Under floor, in wall or overhead electrical or telecommunications wiring inclusive of races, routing and cable organization devices;
- Any power protection or condition equipment such as UPS batteries, fuel cells, diesel or other fuel generators, transformers, surge/sag protection devices;
- Any cooling system support devices such as chillers, air/water cooling towers, in-rack cooling (water or air), any hot/cold aisle containment devices or similar technology as available and implemented;
- Any in building telecommunications networking equipment as it relates to supporting the State's operations within the facility and interfacing with any State provided networking; and
- Any devices that absent their presence in the facility would impair, impede, prevent or damage the State's ability to conduct day-to-day operations of the Data Center for State purposes following the exit of the Contractor.

The following are **not** considered to be permanent facility renovations and are therefore required to be removed from the facility at the conclusion of the Contract term or upon termination of the Contract:

- Contractor computing devices such as mainframes, servers, storage, tape or magnetic media, local (data center) networking and telecommunications interconnection equipment;
- Contractor third party telecommunications provider premise equipment;
- Furniture, telephones, personal computers, office equipment (e.g., faxes, photocopiers) and other non-permanent office fixtures;
- Power, networking or telecommunications cabling that supports any equipment that must be removed must be either removed or identified and inventoried at the State's discretion; and
- Any in-building signage that is Contractor specific and not required under building code.

4.8.3 Contractor Sourced and Managed Contracts

It is the sole responsibility of the Contractor to ensure that all Contractor sourced contracts inclusive of general building maintenance and repairs, telecommunications, environmental testing, facility mechanical maintenance (e.g., UPS and Diesel/Fuel power generation) that do not support State operations are terminated and that the State is not obligated to any ongoing financial, contractual or other obligations associated with these contracts or any Contractor or third-party services, equipment or maintenance that support these contracts.

The Contractor will ensure that the Contractor and any and all non-State sub-tenants of the Contractor will be exited completely from the facility at the conclusion of this Contract inclusive of any equipment, computing devices, office furniture, fixtures, unused network and power cabling, non-permanent lighting, office supplies and equipment and any other items that are not State owned. Should the Contractor, subcontractor or a contracted sub-tenant of the facility leave behind any items that require the State to remove these items, the actual costs for

removal and disposal shall be itemized and deducted from any payments due the Contractor from the State at the conclusion of the Contract.

4.8.4 Exit Period

The Contractor's exit period must commence no less than one (1) year in advance from the anticipated expiration of the Contract. During this period the contractor must meet with the State to:

- Present and agree upon a high level exit phasing plan inclusive of any sub-tenant exits from the facility, by month;
- Review and agree upon an access plan to identify any Contractor personnel, or contracted third parties that require access to the facility to affect the Contractor exit of the facility;
- Provide a detailed inventory and physical identification via a walk-through process of all Contractor equipment that must remain or be removed;
- Provide and agree upon a detailed plan, no later than six (6) months prior to the exit of the facility, which identifies specific Contractor tasks and activities required to return the building to the State;
- Provide and agree upon a detailed plan, no later than six (6) months prior to the exit of the facility, which identifies specific hand-over tasks that require the direct involvement or support of the State such as assumption or replacement of certain building operational functions, building or mechanical maintenance contracts, access to corridors, freight elevators, loading docks and special accommodations within parking lot and building surroundings;
- No later than forty-five (45) days following the exit of the facility, conduct a walk-through of the vacated space to ensure that all equipment, fixtures, furniture and any debris have been removed in accordance with plans, agreements and inventories provided to the State.

4.9 Contractor's Property

The State will not be liable for any injury or damage to the person(s) or property resulting from fire, explosion, any falling plaster, steam, gas, electricity, water, rain, snow, or leaks from any part of the Leased Premises including pipes, appliances, plumbing, roof, or by dampness, or by any other cause whatsoever.

Any computing hardware or devices provided by the Contractor as part of Contractor operations for in-scope services shall remain owned by the Contractor and included in the regularly scheduled fees in the Contractor's invoice to the State. The Contractor shall not invoice the State for any hardware, software or associated maintenance fees without the prior written approval of the State. At the conclusion of the Contract between the State and the Contractor or the permanent removal from service of Contractor provided hardware (e.g., reaching useful life), the Contractor shall promptly remove the hardware from State premises and properly dispose of this hardware.

4.10 State Owned or Provided Hardware, Software, Networking and Associated Maintenance

The current infrastructure computing environment and its associated hardware, software licenses, networking equipment and maintenance contracts are owned by the State and support/maintenance fees are current with all equipment and services vendors for in-scope environment elements.

The State will retain title and ownership and maintenance contracts of all hardware, software and networking elements associated with the Contractor delivering services to the State as they pertain to assets currently owned by the State. The State will maintain all software items currently owned in accordance with existing contracts with the corresponding hardware, software and networking providers and wherever possible will work with these providers to allow the Contractor direct access to support, maintenance, upgrade, bug-fix and other entitlements currently in place between the provider and the State.

Additionally, the following ownership, licensing and maintenance elements shall apply:

Where hardware, software, networking and maintenance is existing and licensed or contracted by the State as represented herein, the State will continue to retain ownership and maintenance obligations with respect to these items in accordance with existing agreements with 3rd party hardware, software and networking vendors.

Where hardware, software, networking and maintenance is specified as part of this RFP which does not exist within the State, or is otherwise not available or licensed by the State, is not provided as a included cost in the offeror's proposal, and will be required for the State to perform these services over the term of the agreement (and if required post agreement), these elements are to be specified with costs in the Cost Summary and an accompanying bill of materials (e.g., networking devices, help desk software, job schedulers etc).

Where hardware, software, networking and maintenance is provided by the Contractor as part of this RFP which is in support of the delivery of Managed Services and is not required to be licensed to the State and/or transferred to the State upon conclusion of the Contract, the offeror must price these element(s) as part of their Managed Service offering (e.g., service desk tools, inventory and SL reporting tools, asset tracking etc). Regardless of ownership, the State retains all rights to the underlying State data and reports contained in these elements.

Where software is required as part of the delivery of SOCC remediation project services (Work areas 1 to 4 collectively) that does not require the State to license this software to support the implementation/development effort (e.g., vendor enablers, tools, methodologies and frameworks), the offeror must include these software elements in the Cost Summary. Offerors should provide a detailed bill of materials that supports the required software costs inclusive of maintenance, updates and upgrades. The State is under no obligation to accept offeror provided pricing, and reserves the right to license this software directly from the OEM software provider at its sole discretion.

Any hardware purchased, loaned, leased or otherwise provided by the State to the Contractor in conjunction with the in-scope Services shall remain the State's sole ownership. The Contractor shall have no rights to the aforementioned hardware. Hardware includes, but is not limited to: computing platforms, storage devices, tape and optical management systems, networking and telecommunications devices. Any hardware provided by the Contractor in accordance with the delivery of services associated with the in-scope services shall be owned by the Contractor and any fees for this hardware shall be included in regularly scheduled invoices.

Contractor shall not include any hardware, software, networking or maintenance charges without the written prior approval of the State or that are not included in the Cost Summary.

4.11 Managed Service Contract End Transition Services

The Contractor must provide to the State the Managed Service Transition Services set forth herein in connection with the expiration or termination of the Contract. Should the Managed Service services terminate for whatever reason prior to the planned expiration of the Contract, the following must apply to the Managed Service portion of the Contract. Investments and Lease/Tenant agreements pertinent to the 3rd floor (or other floors) of the Facility as agreed and improved must not be subject to these terms unless the State reaches agreement on amount to compensate the Contractor for building improvements or the amortization of the actual costs of facility improvements has been fully recovered by the Contractor in accordance with an agreed cost recovery arrangement.

To the extent the Transition Services include any tasks which the Contractor is not otherwise obligated to perform under the Contract, the charges will be based on then-current rates for Services as proposed by the Contractor (the Rate Card) or prevailing rates at the time of termination, whichever is lower.

"Transition Services" will mean (a) to the extent requested by the State, the continued performance by the Contractor of its obligations under the Contract (including providing the services which are subject to termination or expiration), and (b) the provisioning of such assistance, cooperation and information as is reasonably necessary to help enable a smooth transition of the applicable Services to the State or its designated Third Party provider ("Successor"). As part of Transition Services, the Contractor must provide such information as the State may reasonably request relating to the number and function of each of the Contractor personnel performing the Services, and the Contractor will make such information available to the Successor designated by the State.

The Contractor must cooperate with the State in its attempts at transferring the services responsibilities to another provider in a manner in keeping with and not adversely affecting the provision of ongoing services.

4.11.1 Contract End Transition Responsibilities

Commencing six (6) months prior to expiration of this Contract or on such earlier date as the State may request due to termination or non-renewal of this Contract, the Contractor must provide to the State, or the State's designee, the transition services requested by the State to allow the Services to continue without interruption or adverse effect and to facilitate the orderly transfer of the services to the State or its designee (including a competitor of the Contractor). The Contractor will also provide transition services in the event of any partial termination of this Contract (e.g., termination of an element or other component of the Services) by the State, such assistance to commence as agreed upon following the State's notice of termination to Contractor. Transition services will include the assistance described in the following:

- The State or its designee will be permitted, without interference from Contractor, to hire any Contractor personnel primarily performing the services as of the date of notice of termination, or, in the case of expiration, within the six (6) month period (or longer period requested by the State) prior to expiration. The Contractor will waive, and will cause its subcontractors to waive, their rights, if any, under contracts with such personnel restricting the ability of such personnel to be recruited or hired by the State or the State's designee. The State or its designee will have access to such personnel for interviews and recruitment.
- If the State is entitled pursuant to this Contract to a sublicense or other right to use any software owned or licensed by Contractor, Contractor will provide such sublicense or other right.
- Contractor will obtain any necessary rights and thereafter make available to the State or its designee, pursuant to agreed terms and conditions, any third party services then being utilized by Contractor in the performance of the services, including services being provided through third party service or maintenance contracts on equipment and software used to provide the services. Contractor will be entitled to retain the right to utilize any such third party services in connection with the performance of services for any other Contractor customer.
- For a period of up to twelve (12) months following the effective date of termination/expiration under other provisions of this Contract, at the State's request Contractor will continue to provide Termination/Expiration Assistance under the then current Rate Card. Actions by Contractor under this section will be subject to the other provisions of this Contract.
- In the process of evaluating whether to undertake or allow termination/ expiration or renewal of this Contract, the State may consider obtaining, or determine to obtain, provisions for performance of services similar to the services following termination/ expiration of this Contract or to return these services to the State for ongoing operation. As and when reasonably requested by the State for use in such a process, Contractor will provide to the State such information and other cooperation regarding performance of the services as would be reasonably necessary for the State or a Third Party to prepare an informed option analysis for such services, and for the State or a Third Party not to be disadvantaged compared to Contractor, if Contractor were to be invited by the State to submit a proposal.
- Contractor acknowledges that, in the event it breaches (or attempts or threatens to breach) its obligation to provide transition services as provided in this section, the State will be irreparably harmed. In such a circumstance, the State may proceed directly to court. If a court of competent jurisdiction finds that Contractor has breached (or attempted or threatened to breach) any such obligations, Contractor agrees that, without any additional findings of irreparable injury or other conditions to injunctive relief (including the posting of bond), it will not oppose the entry of an appropriate order compelling performance by Contractor and restraining it from any further breaches (or attempted or threatened breaches).
- Contractor must provide to the State an inventory of resources (or resource full time equivalents) then performing Managed Services work under Contract to assist the State in determining the appropriate resourcing and skill model required for the State or a State contracted third party to assume the services as provided by the Contractor at the time of expiration or termination. This resource inventory will include (at a minimum); full-or part time equivalent resource models; skill and experience levels; education or technical skill certification levels required; and other mutually agreeable and pertinent information for the State to assemble or source the capabilities to perform the work described herein upon expiration or termination of the Contract

following transition of services. Contractors are to note State does not require names of individuals as part of fulfilling this requirement.

- In addition to the requirements in this section, in the event of a transfer of services back to the State and at the State's sole discretion, the Contractor must design and implement a training program for State employees designed to convey operational and technical knowledge associated with the ongoing operation of the in-scope environments that support agency applications and systems, conduct knowledge and documentation transfers for the then current operational processes and tasks and work to ensure an overall continuity of services until such time as State employees can reasonably perform the roles and responsibilities in keeping with service levels and other operational quality, timeliness and accuracy considerations associated with the delivery of the service. These services will be priced utilizing the then current Contractor rate Card at the time of the request and as approved by the State.

The Contractor must provide transition services to the State or its successor(s) in an efficient and orderly manner. The impact of the transition on the State's business (including its personnel and customers) and the internal and third party IT-related costs incurred by the State in transferring the services should be agreeable to the State under the circumstances of the transition. Transition services continue to be performed by Contractor without disruption or deterioration until the transfer has occurred: (i) consistent with the terms and conditions of this Contract, or (ii) except as approved by the State. Any disruption or deterioration of the remaining Services following the transfer (except as approved by the State or included in the Termination Assistance Plan) to the extent the same is within the control of Contractor and as agreed with the State. In an effort to facilitate transition of responsibilities, the Contractor obligations will continue to apply during the agreed transition services assistance Period.

4.11.2 Contract End Transition Services Plan

The contents of the Transition Services Plan must include, unless otherwise agreed, the services, functions, and activities as defined below:

- Documentation of existing and planned Work Area and support activities.
- Identification of the services and related positions or functions that require transition and a schedule, plan and procedures for the State or its designee assuming or reassuming responsibility.
- Description of actions to be taken by Contractor in performing Transition services.
- Description of how the transfer of (i) relevant information regarding the Services, (ii) resources (if any), (iii) operations and (iv) contracts (if any) will be achieved.
- Description in detail of any successor dependencies necessary for Contractor to perform Transition Services (including an estimate of the specific Contractor staffing required).
- Inventory of documentation and work products required to facilitate the transition of responsibilities.
- Identification of significant potential risk factors relating to the transition and in designing plans and contingencies to help mitigate the risk.
- The timeline for the transfer of each component of the services (including key milestones to track the progress of the transfer).
- A schedule and plan for Contractor's return to the State of (i) the State Service locations then occupied by Contractor (if any), and (ii) the State Confidential Information, the State Data, documents, records, files, tapes and disks in the Contractor's possession.

4.11.3 Contract End Transition Management Team

The Contractor must provide a senior Project manager who will be responsible for Contractor's overall performance of the Transition Services and who will be the primary point of contact for the State in respect of the Transition Services during the Transition Period.

The State will appoint a senior Project manager who will be the primary point of contact for Contractor during the Transition Period. Additionally, the State anticipates appointing a Transition Team that would be responsible for the review of then current services provided by the Contractor and work to facilitate an orderly transition of services.

4.11.4 Contract End Operational Transfer

The Contractor must perform the activities reasonably required to help effect a smooth and orderly transfer of operational responsibility for the Transition Services.

The Contractor must provide access to the State source code, object code, object and production libraries, reference files, field descriptions, record layouts and technical specifications along with run documentation for the State software then in the Contractor's possession, including tools, scripts, run books, production schedules and procedures as required to support the in-scope environments that support agency applications which may be used in training, knowledge transfer, sizing assessments, operational reviews and other uses required by the State at the time of transfer.

The Contractor must cooperate in a professional manner with the successors in conducting transition testing.

The Contractor must provide the State owned documents and information related to the functionality, program code, data model and data base structure, and access methods required to support the in-scope environments within the possession or control of the Contractor. The Contractor must also review this information with the Successor(s) as reasonably requested.

The Contractor must support the State's test plans, back out procedures, and contingency plans as part of the transition of Services.

4.12 State Standards, Security & Privacy and Other Pertinent Information

Throughout this RFP there are a variety of references to State IT and Networking Standards and Security and Privacy Policies. For purposes of convenience, a compendium of links to this information is provided in the table below.

Item	Link
Statewide IT Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITStandards.aspx
Statewide IT Bulletins	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITBulletins.aspx
IT Policies and Standards	http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx
DAS Standards (Computing and	(700 Series – Computing) and (2000 Series – IT Operations and Management) http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx

5.0 Project Management Requirements

5.1 Overview of Scope

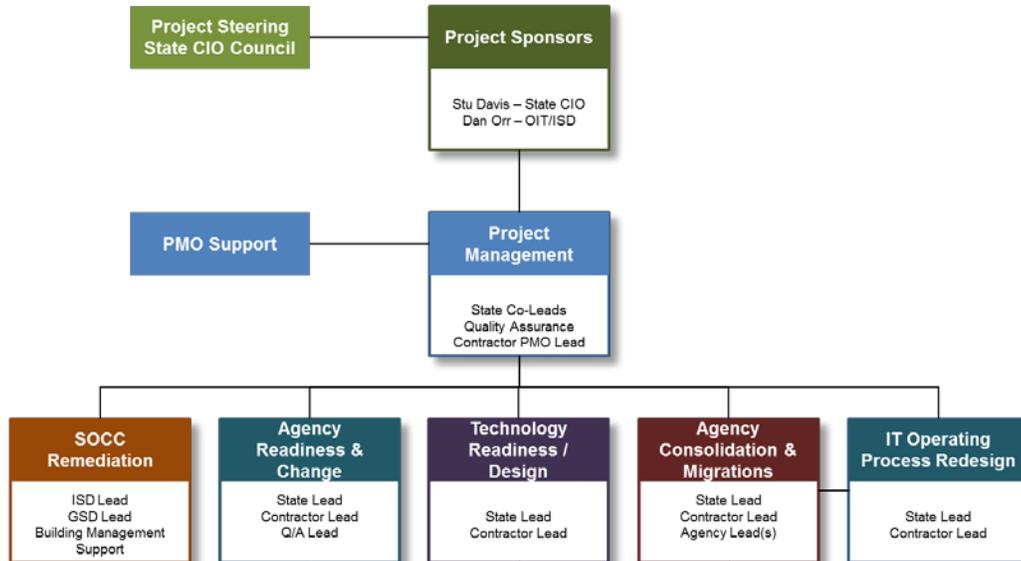
Due to the complex nature of the work contained in this RFP, the project management function is envisioned to have an overall view of the project, commencing upon agreement with the Contractor until such time as the overall project Work is completed.

To fulfill its project management responsibilities, the Contractor must provide the following services:

- Being responsible for overall project completion;
- Maintaining the overall project plan (WBS including schedule and key milestones);
- Ensuring deliverables have detailed project sub-plans (for each project area) and review steps as required by the State to ensure timely delivery and appropriate quality;
- Ensuring that the project has an effective version control mechanism for all documents, including the overall plan and each respective sub-plan, within a project document library;
- Ensuring that an appropriate “Project Kickoff” occurs, all integrated work plans are agreed to by the State prior to project activity commencement and all State and Contractor team members understand Contract responsibilities and obligations;
- Completing status reporting as agreed to during the early stages of the Project;
- Working with the State leadership to ensure that the Project is staffed appropriately;
- Ensuring that required testing activities across both technical and operational components are completed to minimize Project risk;
- Coordinating and collaborating across the various Work Areas with associated teams to ensure appropriate cross-team communication and delivery;
- Implementing the Project while minimizing disruptions to ongoing operations at the SOCC and participating agencies; and
- Managing the participation of DAS, OIT and agency IT stakeholders along with any subcontractors and OEM equipment providers to deliver elements that are “facility engineering” oriented (e.g., power risers, UPS systems, etc.).

5.2 Team Organization

Based on the State's view of the project, the following organizational chart has been created to outline the State roles as the Contractor would fit into the conceptual team structure. To the extent that the offeror believes an alternative solution would be beneficial to the State, the offeror may present an alternative organizational chart and roles and responsibilities in the response to this section.



5.2.1

5.3 Mobilization Effort.

The State, with the Contractor, will initiate the project with a mobilization effort for the first 30-45 days of the project, followed by the project kick-off event. This effort will focus on planning, processes, and project methodology. The goal will be to discuss and evaluate the Contractor's proposed practices, methodologies and recommendations concerning the project.

5.4 Kickoff Meeting.

The Contractor, in conjunction with State staff, must plan and conduct a Project kickoff meeting presentation to the sponsors, key stakeholders and core project team after the mobilization effort. At a minimum, the presentation must include a high level overview of the following:

- Project scope and schedule;
- Goals of the Project;
- Methodology, approach, and tools to achieve the goals;
- Roles, responsibilities, and team expectations;
- Tasks, Deliverables and significant work products; and
- Milestones.

The State requires that all project team members from the Contractor review and understand the Contractor's role and their responsibilities under the Contract that results from this RFP process. Additionally, all Contractor project team members and State project team members must participate in the Kickoff Meeting.

5.5 Project Plan Development and Management

The Contractor must submit and present for feedback an updated Project Plan for the Contractor's tasks, in Microsoft Project or format approved by the State, to the State Project Manager or designee for review and approval as part of the mobilization effort. The detailed Project Plan must include all phases of the project for which the Contractor has responsibility including major deliverables and tasks as well as tasks and dependencies that may be outside of the Contractor's responsibility but may influence or relate to the Contractor's work and ability to complete the Contractor's tasks as planned. The Project Plan must include a more detailed task/activity level for the upcoming six month planning period. The Project Plan must be updated on an ongoing basis with a more detailed view on an agreed upon time interval. This Project Plan must be maintained on an ongoing basis by the Contractor and updated weekly.

The Project Plan must include an updated Staffing Plan (for the Contractor's resources and State resources that are required to participate in the Work including Contractor related activities). The Staffing Plan must include the number of resources by role for the high-level tasks. Additionally, the Contractor must also provide an inventory of required State resources needed by task and role.

★ In addition to the requirements above, the Project Plan must also include at a minimum the following:

- Project Integration;
- Project Scope;
- Project Time;
- Project Quality;
- Project Staffing;
- Project Communications;
- Project Risks/Issues; and
- Project Procurement.

The Contractor must participate in a planning session which ensures the following:

- A common understanding of the Project Plan has been established;
- A common vision of all Tasks, Deliverables and Milestones has been established; and
- Clarity on scope of overall Project and the responsibilities of the Contractor has been defined and agreed to by the State.

Thereafter, the Contractor must:

- Formally update the Project Plan, including work breakdown structure (WBS) and schedule, and provide the updated Project Plan as part of its reporting requirements during the Project;
- Ensure that the level of specificity of the plan for a rolling six month period is defined to the task and named resource level. Given the anticipated multi-month, multi-phase nature of this project, ensure that time periods beyond this six month period are accurately portrayed and forecasted based on the actual project performance to date and anticipated (or realized) downstream impacts to subsequent phases and (if applicable) activities. As an example, the initial project plan will include details for the first six months and activity/milestone level (sufficient to track the overall progress of the program) for the anticipated remainder of the project based on the current understanding of project scope and phasing.
- Ensure the Project Plan allows adequate time for State's review, commentary, and approval on all deliverables.

The State will work with the Contractor in advance of the presentation for review of any deliverable or work product to determine the appropriate number of business days it needs for such reviews and provide that information to the Contractor after award and during the mobilization effort. Should the State reject the plan in part or in full or associated Deliverables in part or in full, the Contractor must correct all deficiencies and resubmit it for State's review and approval until the State accepts the Deliverable, at no additional cost to the State. Should the Contractor determine that State's review of Deliverables or work products will impact the Contractor's ability

to execute the Project in accordance with the agreed and established Project Plan, the Contractor must notify the State promptly with a request for expedited review of Deliverables or work products. In no case must expedited review be requested under circumstances that are within the Contractor's direct control or as they relate to Deliverables deemed deficient by the State for good reason.

5.6 Meeting Attendance and Reporting Requirements

The Contractor's project management approach must adhere to the following meeting and reporting requirements:

- Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to the State's Project Manager or designee in accordance with the Contract Governance Section 12.0 of this RFP.
- Attend Weekly Status Meetings - The Contractor Project Manager and other Project team members must attend weekly status meetings with the State's Project Manager or designee and other members of the State Project team deemed necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda and allow the Contractor and the State to discuss any issues that concern them.
- Provide Weekly Status Reports - The Contractor must provide written status reports to the State's Project Manager or designee at least one full business day before each weekly status meeting.
- At a minimum, weekly status reports must contain the items identified below:
 - Updated GANTT chart, along with a copy of the corresponding Project Plan files (i.e. MS Project) on electronic media acceptable to the State;
 - Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
 - Issues encountered, proposed resolutions, and actual resolutions;
 - The results of any tests;
 - A Problem Tracking Report must be attached;
 - Anticipated tasks to be completed in the next week;
 - Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;
 - Proposed changes to the Project work breakdown structure and Project schedule, if any;
 - Identification of Contractor staff assigned to specific activities;
 - Planned absence of Contractor staff and the expected return date;
 - Modification of any known staffing changes; and
 - System integration/interface activities.
- The Contractor's proposed format and level of detail for the status report is subject to the State's approval.
- Prepare Monthly Status Reports – During the Project, the Contractor must submit a written monthly status report to the State's Project Manager or designee by the fifth business day following the end of each month. At a minimum, monthly status reports must contain the following:
 - A description of the overall completion status of the Project in terms of the approved Project Plan (schedule and cost, if applicable);
 - Updated Project work breakdown structure and Project schedule;
 - The plans for activities scheduled for the next month;
 - The status of all Deliverables, with percentage of completion;
 - Time ahead or behind schedule for applicable tasks;
 - A risk analysis of actual and perceived problems;
 - Testing status and test results; and
 - Strategic changes to the Project Plan, if any.

5.7 Utilize OIT's Document Sharing/Collaboration Capability

In conjunction with the delivery of the Project, the Contractor must use the State provided and hosted document management and team collaboration capability (Microsoft® SharePoint™) to provide access through internal state

networks and secure external connections to all project team members, approved project stakeholders and participants. In conjunction with the utilization of this tool, the Contractor must:

- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;
- Be responsible for the maintenance and general upkeep of the designer configurations of the tool in keeping with commercially reasonable considerations and industry best practices as to not adversely impact the project delivery efforts performed by the Contractor and State; and
- At the conclusion of the project, or upon request of the State, ensure that the State is provided a machine readable and comprehensive backup of the SharePoint™ database(s) contained within the tool that is owned by the State and not proprietary to the Contractor or otherwise required by the State to maintain ongoing project documentation and artifacts (i.e., Contractor is to remove all Contractor proprietary or non-State owned or licensed materials from the tool).

5.8 Project Communications

Building on the project kickoff-meeting(s) outlined above, the Contractor must work with State representatives to execute the communication activities. The Contractor must be responsible for the communication activities including planning, scheduling and performance reporting. Communication materials must have a consistent look, feel and message throughout all forms of media.

The SOCC maintains State operations for several critical systems for a variety of agency tenants, it is essential that a well-designed and executed communication plan be included as part of the Contractor's project management activities associated with this project. Additionally, as activities to remediate the power deficit condition in the SOCC are precursors to agency computing migrations, it is essential that all SOCC agencies are apprised of the project, its progress and milestones in advance of any conditions which may impact any day-to-day operations of the facility, as well as any localized accommodations (e.g., within a suite or affecting a PDU or other power device) that agencies may need to make in order to assist in the success of the project. Therefore, the Contractor is responsible for the following activities and deliverables:

- ★ Create an initial tenant information briefing containing overall objectives of the project, key dates and milestones;
- ★ Establish tenant points of contact (POCs) to communicate and coordinate project activities as they pertain to access to suites, power distribution devices, planning localized outages and other activities which may require tenant support, awareness or action;
- ★ Specific to OSC develop an approach, design, timing and establish regular communications to facilitate the cut-over of OSC from current protected power sources to un-protected power once available.

Over the course of the Project, ensure that updates to these communications documents remain current and are communicated (as applicable) as approved by the State in a timely manner to all impacted tenants.

5.9 Project Management Methodology, Minimum Standards

The State maintains a project management and reporting methodology that is used at varying levels for complex, transformational Information Technology projects. This methodology is designed to provide a substantive and objective framework for the reporting and review of projects to impacted stakeholders and, should the need arise, identify the need for corrective action for one or many of the participants in a project (e.g., State, Contractor, Customer, Stakeholder).

The State acknowledges that various contractors that may do business with the State may maintain unique or proprietary project management methodologies, but seeks to ensure that the overall project is delivered to the State as contracted. Therefore a minimum standard project management reporting standard has been created to serve the State's project management and oversight needs while not adversely impacting or influencing Contractor provided delivery methodologies.

The Contractor must provide a summary Project Plan as requested by the State. For purposes of a summary project plan specific phase and gate dates, effort and costs are a sufficient minimum.

Following the award of this Contract, and during the project mobilization phase Contractors must include the following deliverables and milestones within their detailed project plans and methodologies at a minimum upon commencement of the project:

State Project Management Methodology, Minimum Standards

Phase	Milestone, Activity, Deliverable, Gate	
Concept Definition	Establish Steering Committee/Oversight	A
	Establish Project Charter	D
	Create Summary Plan	A
	Establish Key Milestones	D
	Establish Key Deliverables	A
	Establish High Level Project Plan	A
	Create Cost/Time Analysis (ROM)	A
	Establish High Level Dependencies	A
	Create Concept Proposal	D
	Establish Marketing Requirements & Priorities	D
	Establish Business Case/Budget	M
	Identify Funding/Investment Model	M
	Create High Level Project Schedule	D
	Establish Baseline Service Pricing	M
	Establish High Level Scope/Statement of Work	M
Identify Likely Customer(s)	D	
△	Complete Gate 1 (G1)	G
Prioritization and Scheduling	Create Project Plan	D
	Identify / Secure Resources	A
	Create Detailed Cost/Time Analysis	A
	Create Phasing Strategy / Deliverables by Phase	D
	Conduct Policy Review	A
	Develop Incremental Policies	A
	Secure Funding/Investment Capital	M
	Initiate Procurement Activities/Plan	A
	△	Complete Gate 2 (G2)
Requirements: Functional & Technical	Create/Maintain Refined Project Plan	A
	Establish Implementation Strategy	D
	Assess Internal/External Project Dependencies	A
	Assess Internal/External Risks	A
	Create Detailed Project Plan	M
	Create Stakeholder/Customer Communications Plan	A
	Create Detailed Resource Plan	A
	Establish Level 0 System Design	D
	Establish/Manage End-User Goals	A
	Model End-User Characteristics	A
	Determine Existing Process Change Model	D
	Identify New/Enhanced Business Processes	D
	Create Impact Analysis	A
	Finalize Implementation Strategy	M
	Analyze Impact to Enterprise Architecture/Data Model	A
	Develop Deployment Strategy	D
	Finalize Development Tools and Production Requirements	A
	Validate Customer Pricing Model	D
	Validate Customer Adoption Assumptions	A
△	Complete Gate 3 (G3)	G
Design: Functional & Technical	Follow/Track Final Project Plan	A
	Establish Final Cost & Time Estimate	M
	Outline Next Phase Schedule	A
	Compile Final Impact Analysis	A
	Compile Final Risk Assessment	A
	Create Detailed Design Documents - Functional	M
	Create Detailed Design Documents - Technical	M
	Establish Performance Requirements	D
Establish Support Requirements	A	

	Establish Operating Requirements	A	
	Obtain System Application Software, Tools	A	
	Create Process Flows with Key Inputs/Outputs	D	
	Create Interface Control Documents	D	
	Create Conversion/Migration Plan	D	
	Create Integration Plan	D	
	Develop Stakeholder Communications Materials	A	
	Establish Technical Requirements	M	
	Create Solution System Architecture Documents	D	
	Update Enterprise Architecture Documents	A	
	Create High Level Storage Requirements	A	
	Create System(s) Sizing Requirements	A	
	Establish Test Environment Plan	A	
	Establish SDLC Environments	M	
	Brief/Update User Stakeholders/Customers	M	
	△	Complete Gate 4 (G4)	G
	Component Construction	Develop/Compile Overall Test Plan	A
		Establish Final Processes	D
		Develop Test Analysis Report	A
		Establish Q/A Metrics	A
Create/Refine Development Plan		A	
Develop Code/Solution		D	
Gather and Report Q/A Metrics		A	
Develop UAT Plan, Scripts and Cases		D	
Complete Final Sizing Analysis		D	
Establish Operational Performance Baseline		M	
Publish Committed Capacity Plan		A	
Prepare Component Test Analysis Report		D	
Develop Training Scripts		A	
Develop Training Guide		A	
Component Test	Establish Component Test Expected Results	D	
	Establish Test Plan & Procedures	A	
	Create Test Procedures	A	
	Execute Component Test	M	
	Collect Performance Metrics	A	
	Produce Test Analysis Report	D	
Create Component Technical Documentation	D		
System Integration Test	Establish System Test Expected Results	A	
	Establish Integration Test Expected Results	A	
	Establish UAT Expected Results	A	
	Establish Test Plan & Procedures	D	
	Create System Test Procedures	A	
	Collect Performance Metrics	A	
	Produce System Test Report	M	
	Create System Operational Documentation	D	
	Document/Publish Final Policies & Procedures	D	
	Publish Final Procedures	A	
	Create System Technical Documentation	D	
	Publish Version / Release Document	D	
	Develop Training Scripts	A	
Develop Training Guide	A		
△	Complete Gate 5 (G5)	G	
User Acceptance Testing	Perform User Acceptance Test	M	
	Document/Publish Issue/Bug List	A	
	Prioritize Issues/Bugs	D	
	Remediate Launch Critical Issues/Bugs	A	
	Create Remediation Effort/Schedule for Outstanding Issues/Bugs	A	
	Perform Final Performance Testing	M	
	Perform Final Sizing Analysis	D	
	Create Operational Documents	D	
	Create User Job Aids	A	
	Update User Stakeholders / Communications	A	
	Update Job Schedules and Dependencies	D	
△	Complete Gate 6 (G6)	G	
Deployment	Compile Release Checklist	D	
	Update Business Contingency / Continuity Plan	A	
	Transition Operational Procedures	M	
	Publish Job/Control Schedule	A	

	Establish SLA Parameters	A
	Assemble Audit Impact Statement (integrity, security, privacy)	A
	Create Release Verification Checklist	D
	Execute Operations Training	A
	Perform Release Verification	M
	Update Enterprise Architecture and Data Model	A
	Update Data Center Environments	M
	Perform User Training	M
	Disseminate Documentation and Procedures	A
	△	Complete Gate 7 (G7)
Operate and Maintain	Establish Ongoing Operations Budget	A
	Establish Ongoing Enhancement/Development Budget	A
	Establish Ongoing Maintenance Budget	A
	Perform Break/Fix	A
	Establish Upgrade Plans	D
	Monitor Technical and Operational Performance against SLAs	A
	Monitor Customer Adoption and Usage	A
	Market Services to Additional Customers	A
	Perform Operations	A
	Support Audit Functions	A
Remediate Audit Findings	D	
△	Complete Gate 8 (G8)	G

6.0 Work Area 1: Facility Power and Cooling Upgrades

6.1 Important Considerations

As the SOCC facility is currently at its practical limits with respect to protected power availability, it is important for offerors to note that this area is central to the success of the overall project. Additionally, the State relies on the facility for ongoing production operations of key IT systems and services. Therefore, the State believes that until the overall power capacity of the facility is increased or OSC (currently consuming approximately 27% of the facilities protected power) and administrative personnel power consumption is partitioned from existing power sources, it may be difficult to move forward with larger scale computing device relocation within the facility and from other State data processing facilities activities (which is out of scope) associated with Agency computing migrations (described in general below and in more detail in **Section 7.0** of this RFP) in a parallel fashion as opposed to completing Facility and Power Upgrades before the commencement of Agency Computing Migration and SOCC Operating Model Improvements.

IMPORTANT: Offerors are to design their approach to addressing the aforementioned items in such a manner as to the greatest extent to minimize, any unplanned disruptions to State systems, communications, access and other functions currently in operation at the SOCC.

Work Area 1 is fundamentally a facility engineering exercise designed to increase the available protected power (i.e., un-interruptible power supply – UPS) of the facility. The power is backed up by on-site diesel generation. The Contractor must provide for the availability of un-protected and conditioned power (i.e., conditioned commercial power feeds) and determine if additional cooling capacity is needed to accommodate the anticipated future aggregate computing use of the facility. The Contractor must design and implement additional capacity needed. The figures, estimates, technical specific and other related values (collectively “Requirements”) presented in this section of the RFP are pertinent to State computing use as described in Section 4.0 of this RFP. These Requirements are reflective of the State’s intended use of portions of the first floor (administrative and general space), the 2nd Floor State Computing Center, portions of the 3rd Floor (Unified Network Services and Telecommunications) and the 4th Floor of the Facility (Ohio Supercomputer, MARCS, Administrative Power for Critical Personnel etc.) as described in Section 4.0 of this RFP. As these requirements relate to any offeror contemplated use of the Facility, they must be viewed as the minimum standard for State use.

Any additional power, cooling, wiring, racks, conduits, HVAC, water or other improvements as required for Contractor onward sub-lease or Contractor operations, commercial or otherwise, as they relate to the 3rd floor or have dependencies on any other element of the facility are the responsibility of the Contractor to design, specify, implement and operate over the term of the Contract following award of this RFP. Any additive facility, power, cooling or space fitment items that are not for direct State use are specifically outside of the scope of this RFP, the sole discretion and responsibility of the Contractor, and not to be included in proposed costs or quoted to the State as part of this solicitation.

6.2 Continuous Operations, Unscheduled Outage Performance Guarantee

The SOCC is a facility that supports the 24x365 operation of critical State systems. During the facility remediation period described herein, it is essential that these operations continue without interruption, and that all engineering, electrical, HVAC or other related Contractor activities not interfere with the continuous operations profile of the facility. The State acknowledges that some Contractor activities may require taking elements of the facility “off-line” briefly from time-to-time in accordance with the requirements herein. In all cases, these outages must: (i) Be designed in such a manner as to minimize any outage duration; (ii) be scheduled in advance with the State to occur at a mutually agreeable time and date; (iii) be communicated to any impacted parties including personnel and agencies as well as the State facility manager in advance, in writing; (iv) include contingency plans and rollback or reversibility techniques (in the event of a non-successful installation) so that operations within the building can be restored as quickly as possible; (v) leverage the existing high availability and compartmentalization features of the facility to minimize facility-wide outages, and, to the greatest extent possible, limit outage

frequency, duration and impact to the smallest subset of the entire facility (i.e., riser, floor, suite, PDU, rack) for the duration of the scheduled outage.

Performance Guarantee. The continuous operation of the computer and telecommunications systems located at the SOCC is vital to the State. For failures affecting critical components causing an interruption of service experienced by any computer or telecommunications system (outage), the Contractor must agree to utilize any and all resources to immediately correct the cause of such outage at no additional expense to the State.

As the damages sustained by the State due to an interruption of service are difficult to determine, the Contractor agrees to reimburse the State for an interruption of services experienced by any computer or telecommunications system located at the SOCC by any negligence of Contractor or its subcontractors in the amount of \$10,000.00 for the first occurrence. The Contractor must reimburse the State in the amount of \$20,000.00 for every other occurrence of an interruption of service after the first occurrence for any 12 month rolling period with no cap. If there is only one interruption of service within a 12 month rolling period, the next interruption cost remains at \$10,000.

The State reserves the right to decline any payment, or part thereof, from the Contractor when evidence or inspection may nullify the whole or part of any previous payment to extent as may be necessary, in the State CIOs opinion, to protect the State from loss because of: 1) damage caused by the Contractor and 2) failure to comply with the requirements of chapter 4115, Ohio Revised Code, "Wages and Hours on Public Works."

6.3 Definitions

The term **Protected Power** contained herein and elsewhere in this document must refer to fully redundant componentry, routing paths and cording, supported by near instantaneous cutover to an uninterruptable power source (UPS) that is designed to operate until such time as facility diesel power generation can occur or the restoration of commercial power, whichever is sooner. **Unprotected Power** must mean any provision of commercial power that does not contain one or more of the attributes of Protected Power, particularly UPS support. In neither case must either term be construed as **Unconditioned Power** that may contain surges, spikes or other attributes detrimental to the operation of computing equipment.

The Contractor is required to design, procure and implement power to meet the aggregate power requirements for the SOCC indicated in the table below.

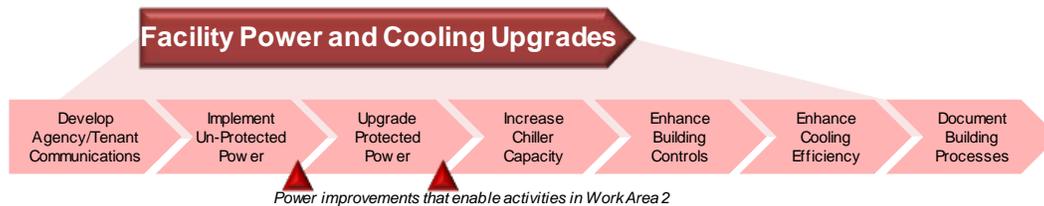
Power Area	Protected (UPS) Power		Unprotected Power	Total Power
	West Riser	East Riser	New Riser(s)	
Current Protected Power (total) - Baseline	1.5 MW	1.5MW	n/a	3MW
OSC Usage of Current Total	0.38 MW	0.38 MW	n/a	0.75 MW Included in total
State Usage of Current Total	1.12 MW	1.12 MW	n/a	2.25 MW Included in total
Implement Unprotected Power - New	0 MW	0 MW	2 MW	2MW (new)
Remove OSC from Current Protected Power	(0.38 MW)	(0.38 MW)	1 MW	1MW included in unprotected power
Remove Administrative functions from Current Protected Power	0.10 MW (Estimated)	0.10 MW (Estimated)	0.20 MW (Estimated)	0.20MW included in unprotected power
Implement Additional Protected Power - New	2MW	2MW	n/a	4MW additional
Total SOCC Power implemented for State Exclusive Use	3.5MW	3.5MW	2MW	7MW Protected + 2MW Unprotected

To this end, the State's requirements fall into 3 categories (1) - Remove OSC from Current Protected Power, (2) - Remove Administrative functions from Current Protected Power and (3) - Implement Additional Protected Power – New. These requirements are designed to increase the available protected power by 4 MW, provision additional non-protected (i.e., "wall power") by 2MW, integrate new power sources with existing power management and monitoring capabilities as well as re-design the use of space within the facility in a more efficient manner.

Offerors are instructed to provide a complete bill of materials (BOM) for all power and cooling devices that are required to implement these improvements as part of their Cost Summary Responses. The BOM must include (at a

minimum): make, manufacturer, model number and capacities as well as anticipated cost (list price or typical selling price) with a notation as to assumptions made with respect to creation of the BOM.

Activities in this Work Area are essential to enabling IT consolidation across the State. Building on the conceptual project overview described in section 4, a logical view of this Work Area is as follows:



6.4 Current Technical Specifics

Two power feeds from Columbus Southern Power provide the SOCC with its electrical requirements. [Note: Columbus Southern Power is an operating company of American Electric Power (AEP).] The power voltages are both 13,200 volts (nominal) with a fluctuation tolerance of plus-five percent and are referred to as the “preferred” and “alternate” circuits. These circuits are separately routed to the SOCC and converge at their respective exterior metering cubicles located at the fuel tank pit. Power is stepped down to 480 volts through seven transformers for the main building ranging from 750 kilo-volt (kV) amperes (KVA) to 3,000 KVA and distributed to load. There is also one, 13.2 kV transformer dedicated to the fire pump.

The tenant computing systems, which includes storage, networking and other computer related systems, are supported by two Liebert UPS systems which also provide power conditioning, thereby enabling the SOCC to experience near zero KVA reactive (KVAR). The UPS systems also support the raised floor office space furniture, a few office space cubicles in the executive suite on the first floor, including security and the task lighting on all office space furniture throughout the SOCC. In addition, with the furniture on the UPS, any personal devices plugged into that furniture are also being supported by the UPS.

The UPS systems each utilize four alternating current/direct current (AC/DC) modules (750 KVA/675 kW); output has been limited to 600 kW, and DC battery support with a capability to carry the load for up to 20 minutes. All of the batteries in the battery room were replaced in 2010 at which time thermo-graphic studies were performed on the UPS. The studies indicated that connections through the UPS met the standards for connection. In addition, the entire UPS and about 90 percent of the equipment and systems are backed up by six parallel Caterpillar diesel generators arranged as two sets of three parallel generators, one set producing 5,259KW and the other producing 6,000KW through eight RussElectric automatic transfer switches. There are two, 20,000-gallon double-walled fiberglass underground fuel storage tanks (total of 40,000 gallon capacity).

The current load on the UPS generators is 2,735 kW. The load on the building standby generators is 3,110 kW. Based on this load and 35,000 gallons of fuel in the ground with no load shedding for fuel conservation, there are approximately 2.9 days’ worth of fuel for generating capacity with provisions for replenishment.

Additional technical elements and design drawings will be provided to Qualified Offerors prior to final proposal submission.

6.5 Provision and Usage of an Un-Protected Power Source

The State will work with the Contractor to determine the practicality of utilizing an alternate power provider and be responsible for the contracting and provisioning of this power to an agreed upon building demarcation point as a service to the Contractor. However, the Contractor must meet the following regarding provision and usage of an unprotected power source:

- ✦ In keeping with the current design attributes of the current power feeds (described in section 6.2), design and implement an additional power feed from either AEP or an alternative power provider to service the

distribution of non-protected (i.e., not covered by UPS, but covered by in building diesel generation) power service.

- ★ Design and install requisite transformers, power conditioning devices required cross-connects or power switching equipment as to:
 - Feed a newly provisioned riser;
 - Incorporate building emergency power as provided by on-site diesel generation equipment;
 - Monitor and meter this power as to verify power provider bills, aggregate usage and to ensure delivery to un-protected PDUs located within the facility; and
 - Include requisite fire suppression and cooling ductwork to ensure the operation of the power feed in accordance with building code, existing building design and normal data center conventions.
- ★ Install a new power riser within the facility (currently viewed as the “North Riser”) to facilitate the distribution of power to the various floors of the facility. This riser must include monitoring provisions as included in the existing design of the facility and include provisions for fault detection, under/over voltage conditions, surges and similar power distribution considerations in keeping with a modern data center.
- ★ Relocate and provision the use of the new unprotected power source for 10 PDUs (as identified by the State) from the 3rd and 4th Floors to the second floor computing area to service devices requiring (or best suited to) non-protected power (e.g., development, testing, demonstration, training) located within, or anticipated to move to the 2nd floor.
- ★ Fully implement Liebert SiteScan® software or similar compatible software for the monitoring and power metering of these newly relocated PDUs and integrate monitoring functions in keeping with building controls.
- ★ Develop a longer-term design that can accommodate the addition of unprotected power PDUs as required throughout the building without significant cost implications other than the purchase of PDUs and nominal electrical contracting activities.

6.6 UPS – Uninterrupted Power Enhancements

The State has identified approximately 20,000 square feet of contiguous space on the ground floor of the SOCC that is currently occupied by storage/administrative space and has an adjacent space that was formerly occupied by a commercial kitchen/cafeteria in the facility. It is the State’s preference to leverage the storage/administrative space for the provision of additional UPS capacity and associated power interconnection and building controls integration. However, should the additional space as afforded by the commercial kitchen be required, the Contractor may use this space to meet the UPS requirement.

Contractor Deliverables are as follows:

- ★ Assess space requirements to install additional UPS power as required by the table in section 6.2 of this RFP and conduct facility improvements in the form of demolition, construction or repurposement of the mentioned administrative/storage space, and if required and agreed with the State, the commercial kitchen space.
- ★ Implement fire suppression, HVAC and integrate with existing building controls for the new UPS space consistent with existing implemented capabilities at the SOCC or in the absence of implemented capabilities, National Fire Protection Association (NFPA) Data Center Standards.
- ★ Specify, design, procure and install additional UPS capacity as required by the table in section 6.2 of this RFP and integrate with existing building power, diesel generation, monitoring and metering capabilities to ensure that the additional UPS capacity is available to all tenants, computing areas and devices in keeping with the existing design of the facility and as provided currently by the east and west electrical risers.
- ★ Rebalance loads strategically between the east and west risers to ensure proper redundancy, failover, accommodation of swing loads etc. based on current data center conventions and building design considerations.
- ★ Review the current balance of UPS loads in consideration of the overall capacity (i.e., current UPS and the additionally installed UPS described in this section) and, if required, rebalance the loads of the UPS, if required, individual cells of the UPS.

- ✦ Design a PDU placement strategy and associated designs for the 2nd Floor computing area to accommodate multi-tenant occupancy of the 2nd Floor to maximize the efficiency of the PDUs and UPS, placement of the PDUs in a manner as to minimize ongoing management and ongoing electrical contracting complexity.
- ✦ Relocate protected power UPS PDUs currently located on the 4th and 3rd Floors to the 2nd floor computing center in parallel with activities described in section 7.0 of this RFP (SOCC Agency Computing Migration) in such a manner as to support continuous operation post remediation and to ensure that N+1 power conventions are adhered to (i.e., devices that require redundant power are serviced by multiple PDUs that have sufficient redundancy with respect to risers, UPS, diesel and other power considerations).
- ✦ Implement Liebert SiteScan[®] or compatible software on all protected PDU devices and to the centralized collection/monitoring console to measure both point in time, time window and aggregate power consumption per PDU as well as monthly usage statistics to facilitate reconciliation of power bills (to AEP) and creation of internal billing elements for purposes of onward invoicing of agency/tenants of the SOCC.

6.7 Air Conditioning and Chiller Enhancement

The SOCC currently has approximately 4,000 tons of cooling capability in external cooling towers supporting the CRAC units distributed throughout the facility. There are four (4) 1,000-ton cooling towers outside the facility. Only three of the four towers are in daily operation. The office areas and common areas are cooled using two 450-ton centrifugal chillers.

Within the facility, 69 Liebert 20-ton units were replaced with upgraded network compatible Liebert DS™ units. Currently, there are six, 30-ton units operating within the facility along with 76, 20-ton units total as follows:

Unit and Size	Total Quantity	Active (Running*)
20-ton units	76	70
30-ton units	6	5
5-ton units for communication rooms	2	2
3-ton unit in security control room	1	1
3-ton unit in communication room	1	1
30-ton units for UPS room cooling	6	6
TOTAL	92	85

*(Note: Units "running" does not necessarily mean they are fully loaded)

Given the cooling capacity mentioned above, the total CRAC capacity installed on raised floor for the SOCC is approximately 1,720 tons of cooling. The currently available headroom for additional cooling, if needed, is calculated as follows:

$$\text{Estimated Available Headroom} = \text{Cooling Tower Capacity} - \text{Current CRAC Capacity}$$

$$\text{Estimated Available Headroom} = 4,000 - 1,720 = \underline{2,280 \text{ Tons}}$$

Through computing infrastructure consolidation efforts described in section 7.0 of this document, and to accommodate potential future growth the State envisions effectively doubling the amount of computing devices located within the SOCC as part of IT Infrastructure consolidation efforts, therefore an additional cooling capacity is not needed for State use. Contractor Deliverables are as follows:

- ✦ Relocate all CRAC units that are no longer required on the 3rd and 4th Floors to the 2nd floor computing area in parallel with computing device consolidation activities described in section 6.0 of this document.
Integrate all relocated CRAC units with existing building controls including the building management system - currently Honeywell DDC monitoring 18, HVAC network control panels throughout the system as well as five life safety panels and 13 access control panels.

6.8 Facility Controls and Management Enhancements

The State wishes to more effectively monitor and meter building power consumption to drive continuous improvements with respect to consumption, distribution and support the ongoing drive to green computing within the facility. Additionally, the State wishes to ensure that power deficit conditions are identified and addressed on a proactive basis as the computing use of the facility increases and workloads shift from mainframe/distributed computing to distributed/cloud computing and other emerging computing models.

Therefore the Contractor deliverables are as follows:

- ✧ Implement power monitoring and metering at the suite, cage, PDU and rack level and integrate this capability into a building-wide power metering, monitoring and management system that can integrate or replace existing functions as provided by Liebert SiteScan® software.
- ✧ Create procedures for the ongoing management of power, cooling and cabling requests from tenants and Agencies.
- ✧ Create the capability to produce building, suite, cage, PDU and rack level power and space usage reports to tenants and Agencies.
- ✧ Design and implement the removal of the following identified power single points of failure as they stand today that are of concern to the State:
 - Single feed from AEP ideally from a different provider and alternate sub-station, but at a minimum, an additional circuit entering the facility from alternate location and conduit;
 - Redeploy existing building HVAC and controls from the current single riser design to one that utilizes both (east and west) risers to offer higher levels of redundancy;
 - Provide the building telecommunications room with alternate protected power by leveraging both the east and west protected power risers; and
 - Implement automated start of diesel generation in the event of a UPS failure and/or loss of line voltage condition affecting one or more of the UPS subsystems.
- ✧ For non-OIT based computing functions (i.e., tenants that do not consume OIT virtual services): design, procure and implement rack level PDUs that are integrated with power metering and monitoring capabilities as provided by Liebert SiteScan® software or compatible software.

6.9 Facility Cooling Efficiency Enhancements

As the SOCC is approaching 20 years of continuous operation to the State and has served many purposes, over the years the overall efficiency of cooling within the facility could be improved. In general the cooling of the facility is via air movement both within suites via under floor ductwork and via CRAC units. The State has identified the need to review power, networking and other cabling currently located in air passageways below the raised floor and effect relocation to gain additional efficiencies with respect to cooling.

Therefore the Contractor deliverables are as follows:

- ✧ Inventory second floor computing suite under floor cabling (power/networking) serving computing functions and remove unused/obsolete cabling (power, networking and other) wherever practicable.
- ✧ Perform assessment pertaining to feasibility of converting to water cooling for high-density computing environments.
- ✧ Implement in-row cooling for all computing racks located or proposed for consolidation activities (as a result of section 7.0 consolidation activities) leveraging Contractor recommended and designed hot/cold aisle racks, cold air containment or other contemporary techniques to maximize the effectiveness and efficiency of the facility cooling systems.
- ✧ Utilize existing and recently installed (7/2011) (2nd floor only) under-floor cable trays for the installation of new wiring (power, networking and other) as required to support consolidation of all computing devices to the 2nd floor computing area.

6.10 Facility Processes and Documentation Enhancements

Following the State's significant investment in the SOCC pertaining to increasing the power and cooling capabilities of the facility, it is important that all building operational documentation be contemporary with these new capabilities and be able to serve as the basis for the ongoing operation, maintenance and enhancements to the facility.

Therefore the Contractor deliverables are as follows:

- ✧ Creation of a comprehensive document library containing all elements pertaining to the building's power distribution Enhancements inclusive of designs, specifications, operating instructions, manufacturer information, pertinent contact details and other elements that were created as part of this project.
- ✧ Creation of an inventory of all computing support devices such as PDUs, CRAC units, etc. that is included in automated building monitoring capabilities inclusive of their locations, make, manufacturer and other identifying information.
- ✧ Creation of operational documentation for building power and cooling functions suitable to operate (the facility), start, adjust, recycle, or restart these functions during normal and unplanned operating conditions.
- ✧ Create policies for the ongoing administration of building power and cooling.

7.0 Work Area 2: Agency Computing Migration

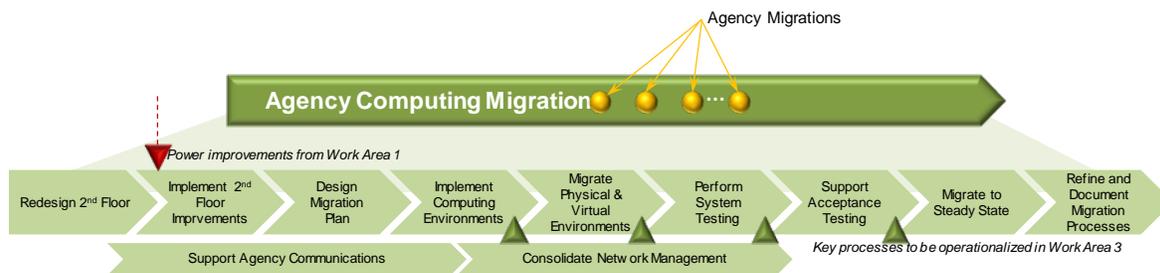
7.1 Overview

In consideration of the overall features and capabilities of the SOCC, the investments over the nearly 20 year history of the facility, and in light of several large agency tenants in the facility (particularly on the 2nd floor), the State has elected to leverage the 2nd floor of the facility as the point of consolidation for Statewide IT infrastructure. Key benefits of this strategy include:

- The abundance of space on the floor (approximately 85,000 square foot in total);
- Existing large scale installations for DAS, OIT, ODJFS, TAX and other agencies;
- Availability of planned virtual computing cloud services and server images offered by OIT;
- High concentrations of local and wide area networking in the building (currently the 3rd floor); and
- The availability of space to migrate/consolidate other smaller agency computing functions.

In short, the view of consolidation around these large “anchor tenants” is logical and can be implemented with minimal to no disruption to existing large agency functions within the facility.

Activities in this work area are the first meaningful step for the State in consolidating IT infrastructure assets within the SOCC. Building on the conceptual project overview described in section 4, a logical view of this work area is as follows:



From a technical perspective, the State maintains mainframe computing operations, storage virtual tape and other “enterprise computing” foundation platforms on the 2nd floor.

Existing personnel on the 2nd floor are to be relocated to the 4th floor, or ideally, to another State facility more suitable to performing routine administrative functions. In consideration of the relative “ease of moves”, the relocation of personnel on the 2nd floor has benefits to the State. Offerors are directed to review the current and proposed configurations of space on the 2nd floor in detailed design diagrams to be provided to Qualified Offerors as determined by the State during the RFP process.

Current 2 nd Floor Tenants	Current SOCC Tenants to Move from other floors to the 2 nd Floor	Current Tenant Computing Space Requirement (sq ft)*
<ul style="list-style-type: none"> ▪ DAS Desktop Computing ▪ GOSIP/Network Services ▪ ODJFS ▪ OIT ▪ TAX ▪ Environmental Protection Agency (EPA) 	Bureau of Workers Compensation	2,710
	Department of Public Safety	6,300
	Department of Youth Services	780
	Department of Education	1,144
	eTech Ohio	649
	Department of Health	3,859
	Department of Mental Health	320
	Ohio Department of Transportation	4,550
	Secretary of State	1,040
	Office of the Treasurer	1,064

* Assuming “like for like” moves of existing computing equipment. Virtualization, rack consolidation and other factors may reduce or minimize these requirements.

Central to this approach is the State's desire to develop, test, rehearse, and refine migration and consolidation processes in support of the first phase of IT server consolidation for "in building" devices. The premise is that during this first phase the State will consolidate computing platforms located within a variety of suites in the SOCC to the 2nd floor computing center including implementation and validation by agency customers. During this process, the Contractor and State would have reduced exposure to unanticipated risks (e.g., security, equipment damage, network connectivity, uncertain timing, testing effectiveness and other factors) prior to migrations outside of the SOCC. It may be feasible, based on the progress made during the first "in building" consolidation, to begin the second "outside of building" consolidation phase in parallel. The "outside of building" consolidation phase is outside the scope of this RFP.

The State will be responsible for relocating personnel within the SOCC from the 2nd to 3rd or 4th floors, and if applicable to alternate State agency facilities, therefore remediation or facility improvements to administrative space within the SOCC (other than those specified in this RFP) are not required and as such are out of scope for this RFP.

7.2 2nd Floor Physical Redesign Activities

The State has mapped all existing SOCC tenant computing functions from their current "suite based" occupancy to available space on the second floor of the SOCC and has made accommodations for segmentation of these tenants based on:

- Power considerations;
- Physical access and security;
- Future growth;
- Leverage of planned OIT cloud services;
- Segmentation of production and non-production environments; and
- Other factors.

Specific design documentation of "as-is" suite occupancy for the 2nd, 3rd and 4th floors of the SOCC, as well as "to-be" designs inclusive of tenant and use segmentation will be provided to Qualified Offerors as determined by the State during the RFP process.

The Contractor is required to review these designs and define activities to complete the following deliverables:

- ★ Develop a detailed device level inventory of all agency SOCC computing devices that are to be moved to the 2nd floor computing center.
- ★ Assemble a power distribution strategy based on the use of protected and unprotected power made available as a product of activities described in this RFP inclusive of the placement of PDU and CRAC units in consideration of contemporary hot/cold aisle designs.
- ★ Develop a rack level schematic for each computing device identified in the device level inventory that includes rack specifications, aggregate mapping and placement of devices within racks and hot/cold aisle containment requirements for each rack and row;
- ★ Develop an improvement plan in keeping with the maximization of power distribution and cooling of the aforementioned racks and inclusive of demolition of existing suites, dividing walls, passageways and the implementation of a single, secure caged space that will serve as the basis for the 2nd floor computing center.
- ★ Design physical cages, security access and floor level access policies and procedures to ensure that the overall security of the facility (both during and after construction), tenant cages, computing devices, storage, networking and data is not compromised.
- ★ Design the improvements to the 2nd floor through the procurement, installation and validation of all impacted power, cooling, networking, security and access components as designed and specified in the preceding deliverables.

- ✧ Review and develop communication materials based on the “to be” designs to to be communicated to Stakeholders and Tenants by OIT to ensure understanding of design considerations and potential changes to building access procedures.

7.3 Implementation of 2nd Floor Improvements

Contractor deliverables are as follows:

- ✧ Develop a design with the State to prepare the 4th floor for personnel occupancy considering all personnel currently on 2nd and 3rd moving into common logical arrangements on 4th, less the relocation of all non-critical personnel from the SOCC to agency locations outside of the SOCC.
- ✧ Initiate, manage and complete all demolition, refurbishment or construction of all 2nd floor improvements as agreed with the State while ensuring that floor access, egress and construction activities to not adversely impact ongoing building operation, security and availability.
- ✧ If required, erect temporary barriers to contain debris, dust or other elements associated with the construction effort that may have an adverse impact to existing computing devices and/or functions currently on the 2nd floor.
- ✧ Implement the improvements to the 2nd floor through the procurement, installation and validation of all impacted power, cooling, networking, security and access components inclusive of controls, monitoring and metering systems.
- ✧ Assemble and secure all tenant caging and computing racks and certify the operation of cage access mechanisms, access codes or badges (or similar).
- ✧ Complete and verify data center connectivity to each rack inclusive of power (protected/unprotected as applicable), networking and other connections as required.
- ✧ Design and implement a badging system, or if practicable enhance the existing badge system to adhere to FIPS certified key card (or equivalent) access at a minimum.
- ✧ Document final “as implemented” master floor plan, update relevant building drawings (to be provided by the State in “as is” form) that highlights agency/tenant locations on the 2nd floor along with common computing areas, placement of electrical and networking devices and demarcation points and other relevant elements as to support the ongoing management, usage and planning activities pertaining to the floor.

7.4 Power Profile Assessment, Assignment and Implementation

As part of the State computing element migration from the various floors of the SOCC to the 2nd floor computing suite, the Contractor will work with tenant Agencies to review the actual power needs for each in-scope infrastructure element. In general three power profiles will be created to meet the operational requirements of the out-of-scope applications that reside on the in-scope infrastructure elements. These profiles have been designed, at a high level, to meet certain continuous availability requirements for State and life critical applications as well as to apportion power based on actual requirements of these applications. Historically, all infrastructure devices implemented at the SOCC, regardless of requirements, have been implemented in “N+1” or Tier III compatible frameworks (e.g., dual cording, dual PDU, dual UPS and dual power generators). However, in consideration of the actual up-time and operational needs, certain applications and non-production environments that rely on in-scope infrastructure elements may not require this level of power infrastructure. While the State believes that there may be significant opportunity (as much as 15-25%) to reduce the power distribution and usage complexity in the SOCC via the implementation of these profiles, in all cases, **the Contractor is to seek approval from a tenant agency prior to implementing a power profile for an infrastructure element, device or service.**

For offeror estimating and planning purposes, the following analysis should serve as a basis for understanding the number, nature and profiles (at a high level) for all applications in the State. Note, many of these applications may not currently reside in the SOCC and are presented for estimating purposes only.

Power Profile (Uptime Institute)	State System Profile and <u>Examples</u>	% Statewide Systems that Appear to Require this Profile
----------------------------------	--	---

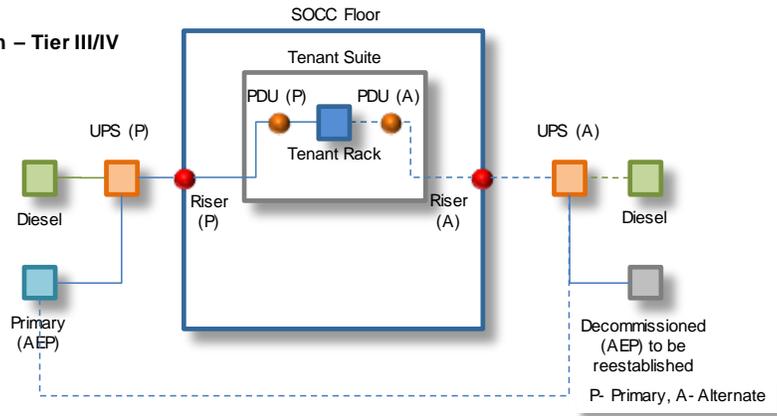
Basic “<N” or Similar to Tier I <ul style="list-style-type: none"> ▪ Single path for power and cooling distribution ▪ May not have raised floor, UPS or Generator ▪ 28.8 hours of annual downtime ▪ Must be shut down completely to perform preventative maintenance ▪ May utilize in-rack UPS or be tolerant to orderly shutdown/restart 	<ul style="list-style-type: none"> ▪ Applications that have low availability requirements ▪ Common office/productivity applications that could be virtualized ▪ Applications used seasonally or intermittently ▪ Maintenance schedules can be coordinated without impacting users/processes ▪ Reference or archive data or systems ▪ Non-Production environments that support minor enhancements, break/fix, testing, training, demonstration and the like 	41 %		
Enhanced “N, N+” or Similar to Tier II – Redundant Components <ul style="list-style-type: none"> ▪ Single path for power and cooling distribution ▪ Redundant components ▪ Raised floor, UPS and generator ▪ Slightly less susceptible to disruptions than tier 1 ▪ 22.0 hours of annual downtime ▪ Maintenance of power path and other parts of the infrastructure require a processing shutdown 	<ul style="list-style-type: none"> ▪ Applications that are mostly limited to normal business hours ▪ Maintenance would need to be scheduled during non-working hours ▪ Low/Medium risk to availability ▪ Non-Production environments that support large scale SDLC project or software development (>\$5M or as requested) 	39 %		
Redundant “N+1, N+1+” – or Similar to Tier III Concurrently Maintainable <ul style="list-style-type: none"> ▪ Multiple power and cooling distribution paths (only one active path) ▪ Redundant components ▪ Allows for any planned site infrastructure activity without disrupting computer hardware operation ▪ 1.6 hours of annual downtime ▪ Includes raised floor and sufficient capacity and distribution to carry load on one path while performing maintenance on the other 	<table border="0" style="width: 100%;"> <tr> <td style="vertical-align: top;"> Public Safety <ul style="list-style-type: none"> ▪ Law Enforcement ▪ Fire/Rescue ▪ Emergency Management ▪ Justice/Public Protection Essential Citizen Services <ul style="list-style-type: none"> ▪ Children/Family Services ▪ Medicaid ▪ Family Stability ▪ Unemployment ▪ Workers Compensation ▪ Health and Human Services </td> <td style="vertical-align: top;"> Maintaining Legal / Regulatory / Statutory Compliance <ul style="list-style-type: none"> ▪ Ohio Revised Code Compliance ▪ Federal Filings ▪ Interstate Data Exchange ▪ Local Government Interaction / Coordination Revenue Collection <ul style="list-style-type: none"> ▪ Taxation ▪ Education Critical Employee Services <ul style="list-style-type: none"> ▪ Payroll ▪ Benefit disbursement </td> </tr> </table>	Public Safety <ul style="list-style-type: none"> ▪ Law Enforcement ▪ Fire/Rescue ▪ Emergency Management ▪ Justice/Public Protection Essential Citizen Services <ul style="list-style-type: none"> ▪ Children/Family Services ▪ Medicaid ▪ Family Stability ▪ Unemployment ▪ Workers Compensation ▪ Health and Human Services 	Maintaining Legal / Regulatory / Statutory Compliance <ul style="list-style-type: none"> ▪ Ohio Revised Code Compliance ▪ Federal Filings ▪ Interstate Data Exchange ▪ Local Government Interaction / Coordination Revenue Collection <ul style="list-style-type: none"> ▪ Taxation ▪ Education Critical Employee Services <ul style="list-style-type: none"> ▪ Payroll ▪ Benefit disbursement 	20 %
Public Safety <ul style="list-style-type: none"> ▪ Law Enforcement ▪ Fire/Rescue ▪ Emergency Management ▪ Justice/Public Protection Essential Citizen Services <ul style="list-style-type: none"> ▪ Children/Family Services ▪ Medicaid ▪ Family Stability ▪ Unemployment ▪ Workers Compensation ▪ Health and Human Services 	Maintaining Legal / Regulatory / Statutory Compliance <ul style="list-style-type: none"> ▪ Ohio Revised Code Compliance ▪ Federal Filings ▪ Interstate Data Exchange ▪ Local Government Interaction / Coordination Revenue Collection <ul style="list-style-type: none"> ▪ Taxation ▪ Education Critical Employee Services <ul style="list-style-type: none"> ▪ Payroll ▪ Benefit disbursement 			

As these profiles relate to the systems currently maintained at the SOCC for agency tenants, the following statistics are provided as estimates to aid offerors in formulating a response to this RFP. Note, these values are subject to confirmation with agencies, may or may not reside in part or in total at the SOCC, may include active/active operation with agency provided data centers and are provided for estimating purposes only.

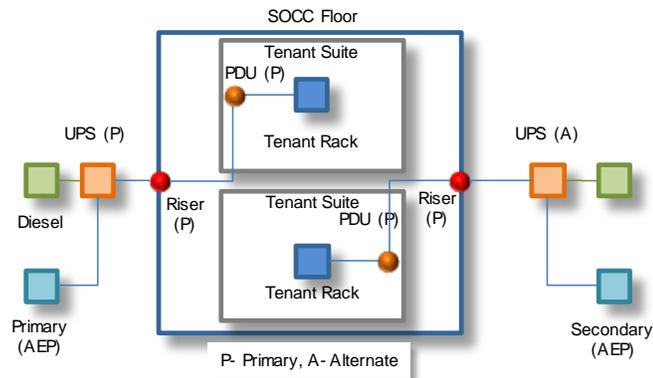
Power Profile / Tier	Approximate Number of SOCC Agency Applications	% of TOTAL
Basic “<N” or Similar to Tier I	227	32 %
Enhanced “N, N+” or Similar to Tier II – Redundant Components	295	42 %
Redundant “N+1, N+1+” – or Similar to Tier III Concurrently Maintainable	177	25 %
TOTAL	699 (of State’s 1626 Total)	100% SOCC Total (Estimate)
Application Counts by Large SOCC Agencies¹		
	Number of Applications	Relative Percent
Department of Public Safety	222	32%
Department of Administrative Services	115	16%
Department of Job & Family Services	79	11%
Department of Education	72	10%
Department of Health	71	10%
Department of Transportation	46	7%
Department of Youth Services	32	5%
Bureau of Workers' Compensation	22	3%
Department of Taxation	22	3%
Ohio Treasurer of State	14	2%
Office of Budget and Management	4	1%
TOTAL	699	100

Conceptually, the State’s goal is to ensure that all State infrastructure elements are apportioned the correct amount, redundancy and profile for power without “over designing or implementing” power redundancy for applications or environments that do not warrant N+1 (or higher) power. To illustrate conceptual implementation profiles for each of these profiles, the following diagrams are provided:

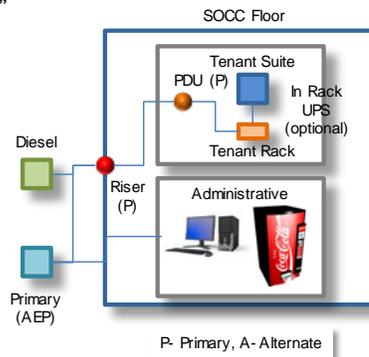
**Current Conceptual SOCC Design – Tier III/IV
“N+1 Services”**



Conceptual SOCC Design – Tier II “N, N+1 Services”



**Conceptual SOCC Design – Tier I and Administrative
“<N Services”**



7.5 Detailed Migration Planning Tasks

The migration of computing devices to the 2nd floor suite will be conducted in accordance with a written plan (the “Migration Plan”). The Contractor must prepare a detailed migration plan for each logical grouping of computing devices (e.g., function, suite or agency based). The plan must be an integrated plan inclusive of both physical and virtual environments.

- ★ The Migration Plan deliverable must contain (at a minimum):

- An estimate of the schedule and work effort for both the State and the Contractor for the design, development, implementation and training required for each phase contained in the plan
- An inventory and description of the IT devices and services being migrated;
- Baseline configuration, network connectivity and performance attributes of the system(s)/environment(s) being migrated to validate that system operation post-migration is not adversely impacted as a result of the migration;
- A description of the methods and procedures, personnel and organization the Contractor will use to perform the migration;
- A schedule of migration activities;
- A detailed description of the respective roles and responsibilities of the State and the Contractor;
- Identify any the State dependencies or personnel requirement assumptions
- A schedule that specifies a detailed level of activity, including the planned start dates, completion dates, hours and other required resources for activities to be performed by the Contractor and the State where applicable;
- Identify any pre-existing software components (e.g., code libraries) and tools to be used;
- Licensing or purchase requirements of any third party components, tools or software elements including Systems software, operational tools and instrumentation, operational productivity aids and other tools required to deliver the solution to the State;
- Include a detailed list of the deliverables and milestones (with planned delivery/completion dates) and the phase management reports that will be provided;
- Describe any assumptions made in compiling the plan;
- Such other information and planning as are necessary so that the migration takes place on schedule and without disruption to the State operations;
- A definition of completion criteria for each phase of the Migration Plan, so that the Parties may objectively determine when such phases have been completed in accordance with the plan;
- A process by which the State may require the Contractor to reschedule all or any part of the migration if the State determines that such migration, or any part of such migration, poses a risk or hazard to the State's business interests and allowing the State to require the Contractor to reschedule all or any part of the migration for any other reason; and
- Tasks to ensure the validation of a successful migration inclusive of user acceptance and assessment of acceptable performance with respect to comparison to baseline performance attributes collected during preceding phases (i.e., design, build, and test) outlined herein.

The Contractor will be responsible for revising and finalizing the Migration Plan, provided that: (1) the Contractor will cooperate and work closely with the State in finalizing the Migration Plan (including incorporating the State agreed upon comments); and (2) the final Migration Plan will be subject to written approval by the State.

The State will:

- Reasonably cooperate with the Contractor to assist with the completion of the Migration; and
- Approve or reject the completion of each phase of the Migration Plan in accordance with the acceptance criteria after written notice from the Contractor that it considers such phase complete, such approval not to be unreasonably withheld.

7.6 Agency Communications and Readiness Activities

In general, the current operating model within the SOCC has been autonomous agency activities located within “rented” suites that are managed nearly exclusively by agency tenants. As the State moves to a shared computing infrastructure provided as a service by OIT, certain communications and coordination processes will need to be implemented to ensure a smooth migration from existing suites to a shared infrastructure. Therefore it is essential that communications between the project team and agency tenants be well designed and executed to facilitate this migration and then expanded upon following the migration to support steady state run activities.

The level of visibility and attention the SOCC receives is anticipated to increase substantially as the project moves closer to go-live. Expectation management is essential to help ensure that the State and SOCC agencies are prepared for the Managed Service transition and rollout and understand go-live capabilities and the timeline for future improvements.

Regarding communications and readiness activities, the Contractor will complete the following tasks:

- Support the State in creation of all communication materials with content direction from the State;
- Support the State to maintain and update a stakeholder impact analysis to foster effective communications;
- Support the State by updating and maintaining the communications plan and assist with facilitation of any meetings necessary to keep the communications plan up-to-date;
- Support creation of presentations for the IT leadership meetings, briefings, and various other presentations as required by the State based upon already established templates and formats;
- Assist with ensuring messages to key stakeholders, sponsors and supporters are equipped with the appropriate messages and materials to influence behaviors and alignment throughout the organization;
- Support specific communication activities, workshops, and employee forums to build awareness and create support for the project;
- Assist with communications to all project participants for up-to-date views of the status, progress, objectives and success criteria for the overall program;
- Ensure that all communications provide in-depth project information to build a stronger sense of understanding of the Project and the value it will bring to the State;
- Attend meetings as required by the State;
- Support creation of communications to support the preparation of participating agencies who will be affected as they roll into the Managed Service;
- Support creation of communications to support the preparation of impacted outside contractors and third-parties who will be affected in the way they operate due to revised operating procedures in the SOCC;
- Support creation of targeted communications and awareness aids to facilitate change activities associated with effectively managing the SOCC;
- Validate communications approach and plan for after go-live; and
- Provide guidance in OIT marketing materials and enterprise communications.

7.7 SOCC Physical Environment Migration Execution

No functionality of the IT operations being migrated will be disabled until the new equipment location is demonstrated to conform to the requirements set forth in this Statement of Work, performs operationally conformant to agreed-upon Service Levels, and has been accepted by the State.

While a detailed physical device level inventory does not exist at this time for agency computing devices located at the SOCC, the following table is provided to assist Offerors in sizing the migration effort. Offerors are instructed to utilize these estimates for construction of cost, timing, resource loading and planning responses to the State. A key task and deliverable (outlined below) is the construction this detailed inventory for purposes of planning, designing and executing the computing migration within the SOCC. Should there be a deviation from these estimates the State and Contractor agree to work in good faith at terms and cost considerations no less favorable than those proposed on an aggregate “per device” basis in consideration of the total cost of the migration based on the total number of devices to be relocated. **Migration of non-SOCC based computing infrastructure to the SOCC is specifically out of the scope of this RFP.**

Detailed inventories of make, model, manufacturer, CPU, RAM Limit, disk, network and other technical configuration details for servers located within the SOCC do not exist. However, at a summary level Statewide server data based on the most recent automated survey (all locations) is as follows:

Agency	System Count	Agency	System Count	Agency	System Count	Agency	System Count
ADA	36	DOH	281	EPA	18	PUC	34
ProLiant BL460c	10	(1) 2599 MHz Processors	1	Not Provided	1	(1) 2405 MHz Processors	1
ProLiant DL320	1	(2) 3192 MHz Processors	1	OptiPlex GX270	1	(4) 3400 MHz Processors	1
ProLiant DL380	3	(4) 3600 MHz Processors	1	PowerEdge 1750	1	HP d530 CMT(dk667a)	1
ProLiant DL385	2	AT/AT COMPATIBLE	3	PowerEdge 2600	4	ProLiant DL100 Storage Server	1
VMware Virtual Platform	20	Not Provided	53	PowerEdge 2800	1	ProLiant DL360	2
AGR	18	OptiPlex GX270	1	PowerEdge 2850	7	ProLiant DL380	24
Not Provided	1	PowerEdge 2650	1	PowerEdge 2950	2	ProLiant DL580	2
PowerEdge 6950	1	ProLiant BL20p	50	VMware Virtual Platform	1	StorageWorks NAS 1500s	1
ProLiant DL320	1	ProLiant BL25p	17	INS	58	VMware Virtual Platform	1
ProLiant DL360	4	ProLiant BL45p	8	Not Provided	4	RSC	85
ProLiant DL380	11	ProLiant DL380	1	PowerEdge 2850	3	AT/AT COMPATIBLE	65
BWC	704	ProLiant DL580	6	PowerEdge 2950	5	Not Provided	19
Not Provided	28	ProLiant DL585	10	ProLiant DL380	19	ProLiant ML570	1
ProLiant BL20p	114	ProLiant ML350	1	VMware Virtual Platform	27	TAX	394
ProLiant BL25p	152	ProLiant ML370	15	JFS	1222	(2) 3200 MHz Processors	1
ProLiant BL40p	14	ProLiant ML530	13	-[88362KX]-	1	AT/AT COMPATIBLE	3
ProLiant BL45p	12	ProLiant ML570	17	CPV5370 System	1	Not Provided	214
ProLiant BL465c	33	VMware Virtual Platform	82	Dell Server	21	ProLiant DL360	12
ProLiant BL490c	20	DOT	334	ES 3020	6	ProLiant DL365	3
ProLiant DL360	1	(1) 2400 MHz Processors	1	HP ProLiant ML370	1	ProLiant DL380	58
ProLiant DL380	81	(1) 3200 MHz Processors	2	IBM eServer 336	1	ProLiant DL385	1
ProLiant DL385	11	(1) 3400 MHz Processors	1	IBM P5	1	ProLiant DL585	17
ProLiant DL580	8	(4) 2333 MHz Processors	1	Not Provided	44	ProLiant ML370	31
ProLiant DL740	6	AT/AT COMPATIBLE	4	PowerEdge 1750	2	ProLiant ML530	3
ProLiant ML370	14	Not Provided	6	PowerEdge 1950	4	VMware Virtual Platform	51
VMware Virtual Platform	210	OptiPlex GX1 350MTbr+	2	ProLiant DL360	194	TOS	13
COM	119	OptiPlex GX270	4	ProLiant DL380	201	AT/AT COMPATIBLE	1
(1) 2992 MHz Processors	1	PowerEdge 1300/500	1	ProLiant DL385	135	eserver xSeries 345 -[867031X]-	1
Not Provided	11	PowerEdge 1300/600	1	ProLiant DL580	18	eserver xSeries 345 -[8670K1X]-	1
PowerEdge 1955	7	PowerEdge 1650	3	ProLiant DL585	2	Not Provided	3
PowerEdge 2850	5	PowerEdge 1950	3	ProLiant LD360	1	ProLiant DL380	5
PowerEdge M610	7	PowerEdge 2600	2	ProLiant ML370	465	ProLiant DL580	2
VMware Virtual Platform	88	PowerEdge 350	1	SUN Count	3		
DAS	87	PowerEdge 860	1	Sun Fire X4200 M2	3		
AT/AT COMPATIBLE	2	ProLiant BL680c	14	Sun SunFire 280R	1		
Not Provided	3	ProLiant DL320	2	Sun SunFire v240	1		
PowerEdge 2650	10	ProLiant DL360	7	Sun SunFire v440	1		
PowerEdge 2850	4	ProLiant DL380	79	Unisys Aquanta ES202141Z	1		
PowerEdge 2950	5	ProLiant DL385	9	Unisys Aquanta HP Vectra VL 18	3		
VMware Virtual Platform	63	ProLiant DL580	1	Unisys Aquanta OS2000111-Z	4		
DEV	40	ProLiant ML350	1	VMware Virtual Platform	107		
Not Provided	2	ProLiant ML370	1	LIS	18		
PowerEdge 2850	1	ProLiant ML530	1	ProLiant DL360	12		
PowerEdge 2950	1	Virtual Machine	10	ProLiant DL380	5		
ProLiant BL490c	6	VMware Virtual Platform	176	ProLiant DL580	1		
ProLiant DL380	19	DPS	291	LOT	23		
ProLiant DL385	3	(1) 2400 MHz Processors	1	Not Provided	2		
ProLiant ML530	3	(1) 2994 MHz Processors	2	ProLiant DL320	15		
ProLiant ML570	5	(12) 3000 MHz Processors	1	ProLiant DL380	2		
DMH	176	(16) 3000 MHz Processors	4	ProLiant DL580	4		
AT/AT COMPATIBLE	2	(2) 186 MHz Processors	1	OBM	153		
OptiPlex GX110	1	(2) 2400 MHz Processors	1	AT/AT COMPATIBLE	4		
OptiPlex GX260	1	(4) 3060 MHz Processors	1	Latitude E6400	1		
OptiPlex GX620	1	(4) 3400 MHz Processors	1	Not Provided	74		
ProLiant BL25p	20	(4) 701 MHz Processors	3	PowerEdge 1950	1		
ProLiant BL460c	8	(8) 3000 MHz Processors	1	PowerEdge M600	3		
ProLiant BL465c	11	ES7000-ONE	4	PowerEdge R900	1		
ProLiant BL490c	4	Not Provided	48	ProLiant DL380	3		
ProLiant DL360	40	OptiPlex 755	2	VMware Virtual Platform	65		

Agency	System Count	Agency	System Count	Agency	System Count	Agency	System Count
ProLiant DL380	12	OptiPlex GX620	1	X7DBR-3	1		
ProLiant DL380	1	PowerEdge 1850	2	ODE	177		
ProLiant ML350	2	PowerEdge 2550	4	AT/AT COMPATIBLE	2		
ProLiant ML370	1	PowerEdge 2650	31	Not Provided	14		
ProLiant ML530	1	PowerEdge 2850	60	OptiPlex 745	3		
VMware Virtual Platform	71	PowerEdge 2950	51	PowerEdge 2950	2		
DMR	79	PowerEdge 6650	6	ProLiant BL25p	5		
PowerEdge 1750	3	PowerEdge 6850	14	ProLiant BL45p	2		
PowerEdge 1850	3	PowerEdge R710	1	ProLiant DL365	2		
PowerEdge 2650	2	PowerEdge R900	2	ProLiant DL380	54		
PowerEdge 2800	2	VMware Virtual Platform	49	ProLiant DL385	5		
PowerEdge 2850	4	DRC	44	ProLiant DL580	2		
PowerEdge 2950	1	PowerEdge 1650	2	ProLiant DL585	2		
PowerEdge 4400	2	PowerEdge 1750	4	System Name	1		
PowerEdge 4600	2	PowerEdge 2600	4	VMware Virtual Platform	83		
ProLiant DL160	2	PowerEdge 2650	12	OIT	368		
ProLiant DL360	3	PowerEdge 2800	1	Not Provided	9		
ProLiant DL380	41	PowerEdge 2850	10	PROLIANT	1		
ProLiant DL580	1	PowerEdge 2950	8	ProLiant BL20p	48		
ProLiant ML350	4	PowerEdge 6600	1	ProLiant BL25p	14		
ProLiant ML370	5	ProLiant DL360	2	ProLiant BL40p	7		
ProLiant ML530	1	DYS	85	ProLiant BL45p	15		
server dx2300	1	AT/AT COMPATIBLE	1	ProLiant BL460c	17		
server rx3600	1	Evo D510 CMT	2	ProLiant BL465c	39		
SRKA4	1	HP Compaq dc7700 Small Form	1	ProLiant BL480c	2		
DNR	101	HP Compaq dc7800 Small Form	1	ProLiant BL490c	20		
(2) 1596 MHz Processors	1	hp workstation xw6000	2	ProLiant BL680c	2		
(4) 2993 MHz Processors	1	hp workstation xw6200	1	ProLiant BL685c	5		
(8) 1596 MHz Processors	13	Not Provided	4	ProLiant DL360	8		
440BX	1	ProLiant DL360	25	ProLiant DL380	43		
AT/AT COMPATIBLE	3	ProLiant DL380	31	ProLiant DL385	13		
Not Provided	16	ProLiant ML350	1	ProLiant DL580	20		
PowerEdge 1950	1	ProLiant ML370	2	ProLiant DL585	2		
PowerEdge 2450	1	ProLiant ML530	2	ProLiant DL740	4		
PowerEdge 2600	2	VMware Virtual Platform	12	ProLiant ML370	3		
PowerEdge 2650	1			VMware Virtual Platform	96		
PowerEdge 2850	2						
PowerEdge 6450/700	1						
PowerEdge R200	2						
ProLiant ML110	1						
VMware Virtual Platform	54						
X6DH8-XB	1						

For purposes of planning, Offerors are to assume that approximately 92% of all SOCC based servers are Microsoft Windows® based, with the remainder a variety of Linux/Unix platforms such as AIX, HP-UX and Solaris. The State's virtualization standard is VMWare which has been deployed on approximately 98% of virtual environments.

Current SOCC Tenants to Move to the 2nd Floor	<i>Estimated</i> Number of SOCC Based Physical Computing Servers	<i>Estimated</i> Number of SOCC Based Storage and Networking Devices
Bureau of Workers Compensation	395	59
Department of Public Safety	233	35
Department of Youth Services	58	9
Department of Education	74	11
eTech Ohio	20	3
Department of Health	157	24
Department of Mental Health	82	12
Ohio Department of Transportation	115	17
Secretary of State	68	10
Office of the Treasurer	10	3
Environmental Protection Agency	18	7
Estimated Total	1,212	183

As part of the physical environment migration, the Contractor must:

- ★ Inventory, track and report all software and applications on supported physical servers, storage, support and networking devices;
- ★ Report CPU, memory, networking and storage counts, attributes and requirements on supported devices.
- ★ Identify the required consents, licenses, keys, usage devices (e.g., hardware dongles) necessary to transition such software on a supported server.
- ★ Identify the power requirements of the devices to be migrated and, based on discussions with Agencies as to the usage profile of the device (e.g., critical, production, non-critical)

- ✦ Assemble a plan to allocate and implement the appropriate power profile (e.g., fully protected: N+1, resilient: N+, or utility: unprotected power) for each device.
- The Contractor will be responsible for managing the process and preparing a scope and operations portion of the Migration Plan which will include assessing the resource requirements (either hardware, software or personnel), time requirements, known impact or dependencies on other Projects, and other information as required as mutually agreed to by the Parties
- The Contractor will provide support to the State in the creation and evaluation of proposed strategies and standards to coordinate information and technical architecture across the State business units and to develop recommendations on information and technology use within the State.
- ✦ The Contractor will define a high-level solution blueprint and operational/technical change plan that includes each logical functional or service domain areas (a combination of “user/services type”, “file server”, “compute server”, “database server”, etc.).
- The Contractor will conduct progress reviews with appropriate the State personnel.
- The Contractor will identify potential risks due to uncertainty with the solution’s complexity and feasibility.
- The Contractor will coordinate and confirm the State approval of phase requirements as stated above.
- ✦ The Contractor will develop a deliverable to identify all physical devices that could be virtualized as part of the migration (and addressed via activities described below) to an OIT hosted virtual environment or an agency provided virtual environment.

The State reserves the right to monitor, test and otherwise participate in the migration as described in the Migration Plan. The State and the Contractor will develop a mutually agreed upon responsibility matrix including Contractor, OIT, agency and other third party responsibilities for discrete activities tasks as part of the detailed migration planning process. The State will provide availability to its infrastructure group to the Contractor according to such agreed-to responsibility matrix in the Migration Plan.

7.8 SOCC Virtual Migration Execution

No functionality of the IT operations being migrated will be disabled until the new equipment location is demonstrated to conform to the requirements set forth in this Statement of Work, performs operationally conformant to agreed-upon Service Levels, and has been accepted by the State.

While a detailed virtual server inventory does not exist at this time for agency computing servers located at the SOCC, the following table is provided to assist Offerors in sizing the virtual machine migration effort. Offerors are instructed to utilize these estimates for construction of cost, timing, resource loading and planning responses to the State. A key task and deliverable (outlined below) is the construction this detailed inventory for purposes of planning, designing and executing the computing migration within the SOCC. Should there be a deviation from these estimates the State and Contractor agree to work in good faith at terms and cost considerations no less favorable than those proposed on an aggregate “per virtual device” basis in consideration of the total cost of the migration based on the total number of devices to be relocated. **Migration of non-SOCC based computing infrastructure to the SOCC is specifically out of the scope of this RFP.**

Current SOCC Tenants to Move to the 2nd Floor	<i>Estimated</i> Number of SOCC Based Virtual Computing Servers
Bureau of Workers Compensation	168
Department of Public Safety	-
Department of Youth Services	10
Department of Education	68
eTech Ohio	-
Department of Health	68
Department of Mental Health	58
Ohio Department of Transportation	152
Secretary of State	2
Office of the Treasurer	1
Environmental Protection Agency	6
Estimated TOTAL	527

As part of the virtual migration, the Contractor will:

- ✧ Inventory, track and report all software and applications on supported virtual machine images, attached storage, support and networking devices.
- ✧ Report CPU, memory, networking and storage counts, attributes and requirements on supported devices.
- ✧ Identify the required consents, licenses, keys, usage devices (e.g., hardware dongles) necessary to transition such software on a supported server.
- ✧ Identify the power requirements of the devices to be migrated and, based on discussions with Agencies as to the usage profile of the device (e.g., critical, production, non-critical).
- ✧ Assemble a plan to allocate and implement the appropriate power profile (e.g., fully protected: N+1, resilient: N+, or utility: unprotected power) for each device.
- ✧ Develop a virtual machine to physical machine mapping matrix to serve as the basis for migration, sizing and baseline capacity planning activities.
- ✧ Apportion, design and implement the correct power profile (“N”, “N+1” etc.) to each row, rack and slot within the 2nd floor computing center to all SOCC based devices as required.
 - Due to the nature of virtual machine computing (i.e., multiple virtual images on a physical device) the Contractor may identify a variety of critical or production images that are co-mingled with non-critical (e.g., testing, development etc.) servers. In cases where a critical production image is identified the Contractor must ensure the appropriate power profile is allocated to the underlying physical device that support the critical production image.
- ✧ As part of the migration process, and as commercially practicable, the Contractor must develop a re-mapping of all non-critical servers that could be re-hosted onto physical devices computing devices that are better aligned with power provision and consumption required by the virtual environment. For example non-production development, testing, training, demonstration virtual environments may be able to be provisioned on a server with an “N” or “less than N” non-protected power profile whereas all critical environments, production or otherwise, must be deployed on “N+1” protected power (or higher) servers.
 - The Contractor will be responsible for managing the process and preparing a scope and operations portion of the Migration Plan which will include assessing the resource requirements (either hardware, software or personnel), time requirements, known impact or dependencies on other Projects, and other information as required as mutually agreed to by the Parties
 - The Contractor will provide support to the State in the creation and evaluation of proposed strategies and standards to coordinate information and technical architecture across the State business units and to develop recommendations on information and technology use within the State.
- ✧ The Contractor will define a high-level solution blueprint and operational/technical change plan that includes each logical functional or service domain areas (a combination of “user/services type”, “file server”, “compute server”, “database server”, etc.).
 - The Contractor will conduct progress reviews with appropriate the State personnel.

- The Contractor will identify potential risks due to uncertainty with the solution’s complexity and feasibility.
- The Contractor will coordinate and confirm the State approval of phase requirements as stated above.

The State reserves the right to monitor, test and otherwise participate in the migration as described in the Migration Plan. The State and the Contractor will develop a mutually agreed upon responsibility matrix including Contractor, OIT, agency and other third party responsibilities for discrete activities tasks as part of the detailed migration planning process. The State will provide availability to its infrastructure group to the Contractor according to such agreed-to responsibility matrix in the Migration Plan.

7.9 Migration Testing and Validation

The new environment (all in scope physical and virtual servers, storage, network constructs and devices, backup/restore and other supporting devices) must be subject to a formal testing and acceptance process that uses objective and thorough test or validation criteria established by the State and Contractor that will allow the State and Contractor to verify that each migration meets the specified functional, technical and where appropriate, performance requirements. The testing and acceptance process must be developed for each logical migration grouping (e.g. agency, physical/virtual, production/non-production, etc..) as soon as possible after establishing the business and user requirements. The testing and acceptance process must include a capability for tracking and correcting problems.

The tasks and activities that Contractor must perform as part of the testing and acceptance process must include the following:

- ★ Development and maintenance of test data repositories as agreed appropriate.
- ★ Development and execution of system test plans, scripts, cases and schedules as agreed appropriate.
- ★ Performance of the following testing activities for in-scope components and assessment of quality and completeness of results including: 1) System test / assembly validation; 2) integration testing; and 3) regression testing new releases of existing in-scope solutions inclusive of hardware, BIOS, microcode, device drivers, patches, service packs and other operating system level code elements.
- Testing as required to perform the system and user acceptance testing work for the supported servers, and where appropriate performance validation testing. The testing will be designed and maintained by Contractor so that build and subsequent testing activities will be sufficient to verify that End-User perceived performance on the new environments is consistent with the pre-migration baseline and to minimize Incidents associated with the migration of environments.
- Quality and progress reviews with appropriate State personnel.
- Coordination and confirmation of State approval of solution components and verification of applicable completion criteria for transition into deployment and production (steady state) use.
- Reports tracking the progress of Contractor’s performance of testing work, or in the case of user acceptance testing, support of State activities to the State on a weekly basis.
- In addition, the Contractor must provide timely responses to the State’s requests for information and reports necessary to provide updates to State business units and stakeholders, as reasonably required.
- ★ The Contractor must be responsible for the production deployment and roll-out of newly developed environments. Deployment includes identification of interfaces and any required data migrations, installation and testing of, installed Systems Software, and any required testing to achieve the proper roll-out of the infrastructure computing environment(s).
- The Contractor must comply with State required implementation and deployment procedures as set forth in this RFP. This may include, network laboratory testing, data migration procedures, the use of any pre-production or pseudo-production environment prior to production migration.
- ★ Contractor must submit to the State for approval, a written deployment plan describing Contractor’s plan to manage each implementation. The tasks and activities to be performed by Contractor as part of the Deployment Services also include the following:

- Execute required physical and virtual system migrations inclusive of all baseline data, configurations, patches, microcode, BIOS and other elements that are required to replicate the required system(s) environment while maintaining compatibility with application or tool requirements that utilize these system(s).
- Perform required data matching activities and error reporting.
- Document environment Incidents and provide to the State for resolution should the Contractor be unable to resolve the incident without State support.
- Coordinate and confirm State approval of environment conversion results as stated above.
- Conduct production pilots and fine tune solution as agreed appropriate.
- Compile and maintain solution Incident lists.
- Support agency communication efforts through the identification of required communication recipients and communicate deployment activities to deployment stakeholders.
- Evaluate detailed communication feedback from recipients and stakeholders and identify the effectiveness of and need for additional communication.

7.10 Agency Validation Testing Support

For a period of no less than ninety (90) days unless otherwise agreed by the State, Contractor must provide sufficient staffing to ensure the overall continuity acceptance testing of the migrated infrastructure as it pertains to delivering these services in a production environment operated by the State.

In the event that a Priority 1 or 2 issue (or any critical blocking issue) occurs during this 90 day period, this 90 day period may be extended at the sole discretion of the State for a period commencing upon satisfactory resolution of the issue in the production environment. Under no circumstances will the Contractor performance during this period or successful conclusion of this period (i.e., no issues detected for 90 days) be construed as relief from or reduction to any Warranty considerations contained in this RFP.

- **Priority 1 issues must be defined as:** An Incident must be categorized as a “Priority 1 Incident” if the Incident is characterized by the following attributes: the Incident (a) renders a business critical System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.
- **Priority 2 issues must be defined as:** An Incident must be categorized as a “Priority 2 Incident” if the Incident is characterized by the following attributes: the Incident (a) does not render a business critical System, Service, Software, Equipment or network component un-Available or substantially un-Available, but a function or functions are not Available, substantially Available or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

During this period the Contractor must:

- Provide personnel with the requisite skills and experience levels in development of the migrated infrastructure to answer questions that the State may have;
- Address and resolve any defects, gaps, omissions or errors that are discovered in the Contractor’s work as they pertain to operation in the State’s production environment;
- Resolve any configuration, performance, compatibility or configuration issues that arise as a result of migration of the Contractor’s work to operating in the production environment;
- Document any relevant changes to operational, configuration, training, installation, commentary or other documentation as a result of migration to the Contractor’s work to a production environment; and
- Assist the State or with production issue triage, root cause and remedy analysis and wherever possible propose work-arounds, fixes, patches or remedies (code-based, procedural or environmental) required to successfully migrate and operate the Contractor’s work to the State’s production environment.

7.11 Consolidation of SOCC Network Management Centers & Functions

The SOCC is the central hub of all networking for the State and in general connects to the Internet, a very large percentage of agency locations across the State, most telecommunications providers that operate in the State as an interconnection hub between the State, State Agencies and various telecommunications carriers. As such offerors are to assume that in addition to the general public for web based services, more than 64,000 State authorized end-user application type connections regularly connect to infrastructure elements maintained in the SOCC. Additionally the State has approximately 500 personnel that regularly connect directly across State networks, VPNs or other secure channels that access SOCC elements independent of applications. This access is typically at the operating system, network appliance, authentication device, database, host terminal server/service, and other elements that are infrastructure in nature, but required to build, operate and maintain agency applications.

The State has implemented application level authentication within legacy applications and recently has begun the deployment of Enterprise Identity Management (EIM) Statewide. The design, operation and maintenance of application or Enterprise level authentication requirements are out of scope for the Contractor. The infrastructure elements that support these services are in-scope. For the avoidance of doubt, and by example, servers (to the operating system prompt) and network element availability for devices that support EIM and applications are in scope, but administering end-user authentication, security and other applications of functions that reside on these servers are out of Contractor scope.

Currently many statewide agencies maintain their own voice and data network management and monitoring capabilities that in general connect agency "headquarters" functions to regional and local government offices for the purpose of conducting agency business. As the SOCC is a center hub for many Agencies with respect to this networking, several large agencies maintain network operations centers at the SOCC that are responsible for the provision, installation, monitoring, management and maintenance of these networks. As part of this project, the State wishes to pilot the process for consolidating the management of these network operation centers (NOCs) that are at the SOCC under one central point of accountability that leverage the same processes, procedures and tools.

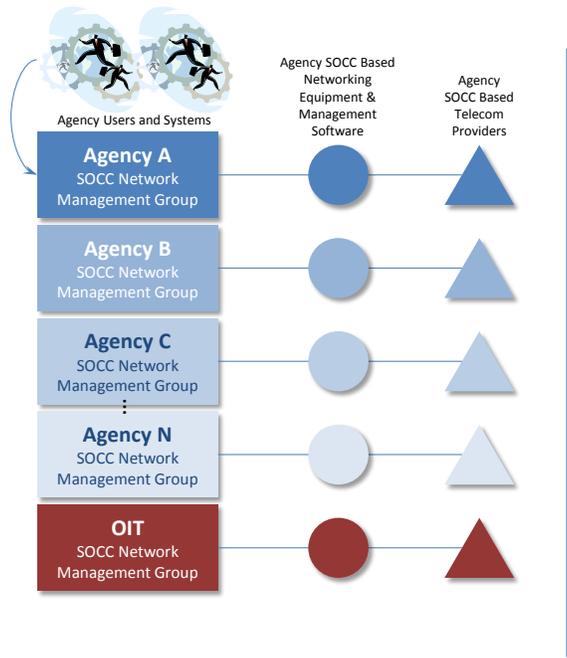
Separate from this RFP, the State may in the future based on the success and demonstrated merits of consolidating the SOCC-based NOCs, continue this consolidation for all statewide networks (voice, data, video and control) as well as determine the feasibility and practicality of this larger telecommunications consolidation. Therefore this Project is an essential "first step" in determining this feasibility. Offerors are instructed to not contemplate or consider this larger scale consolidation as part of their response to this RFP, and specifically limit their response to the scope, activities and deliverables outlined herein.

The scope of the SOCC NOC consolidation effort will include all data connectivity (data center network, telecommunications closets within the SOCC, local circuits and circuit risers within the SOCC to the telecommunications interconnection suite located within the first floor of the SOCC) for supported servers, all network SOCC service delivery LANs, and Storage and backup Devices up to and including circuit termination to a telecommunications Contractor (e.g., AT&T, Time Warner and others) provided premise equipment.

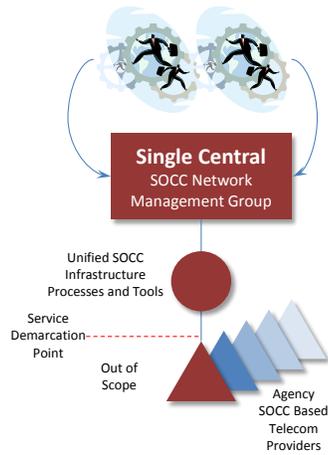
Contractor must be responsible for the consolidation of management and operations for SOCC-based service delivery center network operations for Supported Servers, Storage Devices and LAN.

The following diagram is provided to illustrate the State's goals for network consolidation.

Conceptual Current State



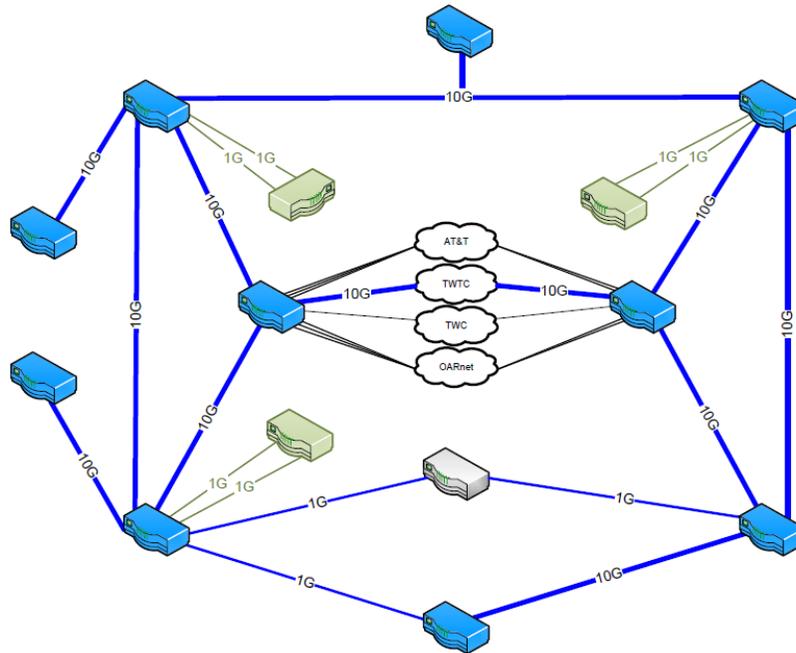
Required End State



7.11.1 Current State: High Level SOCC Networking and Connectivity Information

The following information is provided for Offeror sizing purposes as well as to convey the relative composition, size and complexity of SOCC based networking devices and capabilities.

SOCC Ohio.gov WAN Backbone and Carrier Connectivity



SOCC Access LAN Switches

- Systems monitoring across system components including identifying unauthorized access to the network, and reporting outages via the management tool set.
- Event correlation for fault managed devices and mapping of the relationship for multiple identified events.
- Allow the State to provide engineering support at agreed levels for addressing, mediating and managing critical hardware and network infrastructure Incidents.
- Develop and maintain network documentation for OIT's areas of responsibility and participating with the State in developing consolidated network documentation.
- Maintaining and supporting network components within OIT's areas of responsibility, including supporting network and supported server software required and provided protocols and security techniques as well as standard data access and transport techniques.
- Consolidation of hardware maintenance procedures and contacts for environment supported servers, remote routers, systems software, database, middleware and identified applications software products and ancillary components as required to operate the systems.
- Tracking, managing, communicating and supporting resolution of network exceptions.
- Evaluating and testing, in advance, network, hardware, and interface equipment.
- Develop and provide reports on the status of the network as set forth in a Process Interface Manual that contains all major points of interface (e.g., interactions, workflows, communication paths, escalations etc.) between data center operations and Agencies whether these interfaces be programmatic, procedural, communications or sign-off related in nature or other supporting documents. The Process Interface Manual is a master document that describes all interactions between users of the SOCC, service providers, OIT, and the Contractor pertaining to activities in the SOCC whether they be systematic or programmatic.

The State will

- Provide all network support and the necessary network connectivity up to the Contractor Service Delivery Center demarcation point, which will be as agreed to by the State and Contractor; and
- Provide additional network capacity for supported server resources that have reached critical usage levels or impacts the Contractor's ability to provide the services or relieve the Contractor of any affected service levels until such time as the required capacity is installed.

7.12 Migration to Production Steady State Operations (Managed Service)

Contractor must be responsible for the development of processes to operate and maintain the supported computing environments. The Contractor is responsible for designing, implementing and transitioning the supported computing environments to ongoing operations and maintenance activities following completion of the migration process.

Contractor must perform such activities in such a way that computing environment resources (e.g., network, hardware and associated storage) are utilized with a high degree of efficiency and in a manner as to not compromise the timely completion of such activities or service level requirements outlined in Section 11.0 (Service Levels). Contractor's general responsibilities with respect to the supported computing environment design, build and run activities include the following tasks, activities and responsibilities are described below.

The Contractor's responsibilities for Steady State Operations and Maintenance Services under this Scope of Work must pertain to the period following the completion of the migration of the supported computing environments through the transition to ongoing operations and maintenance activities, satisfying the conditions of transfer, obtaining the State's written acceptance of the deliverables constructed during the migration, and conforming to agreed-upon Service Levels.

The Contractor's Specific Operational Capabilities required to satisfy the State's requirements for Migration to Steady State Operations include (offeror note: these deliverables and capabilities are a selected subset of section 8.0 processes required to operate the new environments and are designed to be complimentary to ITIL processes to be designed and implemented in work area 3 as specified in section 8.0 of this RFP):

- Implementing a Level 2 and 3 support capability inclusive of all tools, processes and policies that is capable of, tracking, monitoring, responding to requests and Incidents and resolving Incidents consistent with the established Service Levels and referring requests to break/fix support resources for additional assistance.
- Creating documentation for State's ongoing development of or modifications to the State's Service Desk to help minimize transfers to specialized support.
- Providing the State with an updated list of Contractor-provided Level 2 Support personnel and "on call" personnel who are responsible for Level 3 Support, including contact phone numbers.
- Working to correct environment defects or problems that require environment code or operational modifications.
- Conducting all personnel training (hardware and software) for State Service desk personnel;
- Providing systems status information to the State Service Desk and updates as they occur during the migration process and until such time as the State accepts the migration in part or in full;
- Developing, maintaining and distributing an agency customer contact list, including names and telephone, pager and fax numbers, for use by State Service Desk staff to contact appropriate agency personnel for problem determination assistance and escalation and to ensure such personnel are available as required;
- Assisting the State in establishing call prioritization guidelines and escalation procedures;
- Ensuring end users within Agencies and customer groups have a basic level of understanding of the State Service Delivery processes and adhere to such processes for accessing the Services;
- Communicating support responsibilities and procedures to the State Agency Single Points of Contact and third party service providers (for example, providing Call status and resolution to the third party Contractor Service Desk) and ensuring adherence to such procedures;
- Assisting end-users, as requested and in a time frame commensurate with the assigned problem response times and any associated Service Level commitments, in the resolution of recurring problems which are the result of End User error;
- Resolving any open State third party service provider performance problems affecting the State's provision of the Services as a result of the migration process;

7.13 Computing Infrastructure Migration Process Refinement and Documentation

Following the migration of all in-scope and as agreed servers within the SOCC to the second floor computing center, the Contractor will:

- ★ Revise all migration materials in a final form to the satisfaction of the State, providing revisions do not alter the approved migration design, and transition the materials to the State.
- Formalize procedures and documentation for ensuring that the migration team is informed of updates to production after go-live as a result of post-implementation enhancements to the migration environments that impact other relevant migration activities.
- Facilitate a post-migration analysis to gather and document lessons learned and to update migration, communication and migration staff training plans accordingly.
- Assess, develop or refine the migration processes to accommodate the migration of non-SOCC based computing devices to the SOCC
- ★ Create a final master inventory and automated discovery capability to identify and monitor of building devices (power and computing) in keeping with IT asset inventory requirements as described in section 7.0.
- Develop baseline usage reports on aggregate computing capacity by computing platform profile.

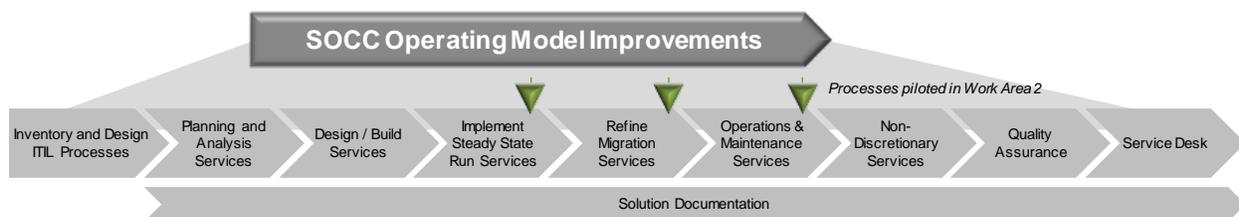
8.0 Work Area 3: SOCC Operating Model Improvements

The State is moving towards Information Technology Infrastructure Library (ITIL®) compliance. As part of this Project, the Contractor must design, implement and transfer knowledge and operation of these processes to the State as part of a Managed Service. This Managed Service will be delivered by the Contractor to the State leveraging a combination of Contractor and State resources for a set of infrastructure processes described below. It is therefore required that the Contractor propose a set of ITIL compatible concepts and techniques for managing the State's infrastructure, and operations.

Measures of the State's success in achieving ITIL compliance shall be informal from a certification or accreditation perspective, but will be measured based on a variety of factors including (but not limited to):

- Overall Compliance with Service Level Agreements described herein between OIT and Customer Agencies;
- Reduction in per-server total cost of ownership (TCO) over time from FY2011 levels (approximately \$1,700 per server, per month) to contemporary commercial levels (typically in the range of \$200-400 per server per month, depending on configuration, use and other factors);
- Higher server virtualization ratios and usage levels including moving from typical 6-9% within the State to industry norms (e.g., 60-80%);
- Reduction of infrastructure call volumes and ticket resolution times as a result of the implementation of more repeatable processes associated with ITIL; and
- An overall reduction in the total cost of Infrastructure Operations Statewide from FY11 levels inclusive of hardware, software licensing, storage, networking, operations and maintenance.

Activities in this work area are designed to provide the State the requisite capabilities, processes and tools required to operate, maintain and manage IT infrastructure assets across the State. Building on the conceptual project overview described earlier in the RFP, a logical view of this work area is as follows:



8.1 Specific ITIL Processes to be Designed and Implemented

Work Area Scoping: ITIL/CoBIT v3 Processes



The State has selected a sub-set of the ITIL/CoBIT process catalog to be implemented that are **specific to infrastructure operations associated with a data center** from a design, build and operate (run) perspective. Service planning, financial management (other than that associated with the SOCC and the Scope of Work) are out of scope. As the State develops capabilities subsequent to the contracting of the Work described herein that build on the work and services described in this RFP, for example disaster recovery which would include the provision for an alternate site and application/operation level services, the applicability of ITIL may be broadened at that time and in these cases shall be addressed by a mutually agreeable change order at the time that the State determines the need for these additional related services.

The Contractor, utilizing a combination of Contractor and State Staff, must handle all incidents, problems, questions as well as provide an interface for other activities such as change requests, maintenance contracts, software licenses, Service Level Management, Configuration Management, Availability Management, Financial Management and IT Services Continuity Management.

Specifically, the Contractor must design and tailor the ITIL discipline to the State's needs, implemented over the course of the project and refined (as applicable) during Steady-State Run Operations to ensure the appropriate services support the following:

- **Service Desk:** to provide the single contact point for State Agency/Users to record their problems and requests. If there is a direct solution then the Service Desk must provide immediate resolution, if not then they must create an incident report. It is expected that incidents will initiate the appropriate chain of processes: Incident Management, Problem Management, Change Management, Release Management and Configuration Management. This chain of processes must be tracked using a Trouble Ticketing system, which must record the execution of each process, quality control point, and store the associated output documents for traceability. Implemented capabilities in this area are to include:
 - Handling incidents and requests through full life cycle management of all service requests;
 - Single Point of Contact providing a single point of entry and exit for the service process and providing an interface for 3rd parties essential to the service processes;
 - Ensuring ease of use / a good customer experience for the State Agency's/Users;
 - Maintaining infrastructure security and assuring data integrity; and
 - Providing timely and effective communication which keeps the Agency's/Users informed of progress and if appropriate advising on workarounds.
- **Incident Management** process and procedures must be in place and a process to ensure that they are continually refreshed in order to have the capability to restore a normal service operation as quickly as possible and to minimize the impact on business operations. An incident is considered to be any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. Implemented capabilities of the Incident Management process are to:
 - Restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price
 - Maintain a comprehensive inventory of 'Known Problems' (without a known root cause) or 'Known Errors' (with a root cause) under the control of Problem Management and registered in a Known Error Database (KeDB)
 - Implemented processes and procedures are to include:
 - a) Incident detection and recording
 - b) Classification and initial support
 - c) Investigation and diagnosis
 - d) Resolution and recovery
 - e) Incident closure
 - f) Incident ownership, monitoring, tracking and communication

- **Problem Management** must be in place to find and resolve the root cause of incidents to minimize the adverse impact of IT infrastructure incidents and problems on the State and to prevent recurrence of incidents related to these errors. The problem management process must:
 - Reduce the number and severity of incidents and problems on the business, and report it in documentation to be available for the Tier I and Tier II help desk.
 - Be a proactive process that identifies and resolves problems before incidents occur.
 - Supported activities are to include:
 - a) Problem identification and recording
 - b) Problem classification
 - c) Problem investigation and diagnosis
 - d) Identification of the root cause of incidents
 - e) Trend analysis
 - f) Initiation of targeted support action
 - g) Providing information to the organization
 - h) Iterative processing to diagnose known errors until they are eliminated by the successful implementation of a change under the control of the Change Management process.
- **Configuration Management** comprising of process and database tools must track all of the individual Configuration Items in the State's service catalog. Basic activities which must be enabled include:
 - *Planning*: The Configuration Management plan must cover a rolling three month period in detail, and the subsequent nine months in outline. It must be reviewed with the State at least twice a year and must include any impacts to strategy, policy, scope, objectives, roles and responsibilities, the Configuration Management processes, activities and procedures, the database, relationships with other processes and third parties, as well as tools and other resource requirements.
 - *Identification*: This must cover the recording of information including hardware and software versions, documentation, ownership and other unique identifiers. Records must be maintained in a Configuration Management Database covering the selection, identification and labeling of all configuration of every item in the Contractor provided infrastructure and systems.
 - *Control*: This must assure that only authorized and identifiable configuration items are accepted and recorded from receipt to disposal. It must also ensure that all Contractor provided infrastructure and systems are under Change Management control.
 - *Monitoring*: Accounting and reporting must provide a view regarding current and historical data (data collection begins following the Contractor implementation) concerned with each Contractor provided item throughout its life-cycle. Changes to items and tracking of their records through various statuses, e.g. ordered, received, under test, live, under repair, withdrawn or for disposal, must be provided.
 - *Verification*: Provide reviews and audits that verify the physical existence of items, and checks that they are correctly recorded in the Configuration Management Database. Verification must also include the process of validating Release Management and Change Management documentation before changes are made to the State's live environment.
- **Operations Management** must provide day-to-day technical supervision of the State's infrastructure, including: execution of documented processes and procedures, output management, job scheduling, backup and restore, network monitoring/management, system monitoring/management, storage monitoring/management. Operations must provide:
 - A stable, secure infrastructure;
 - A current, up to date Operational Documentation Library;
 - A log of all operational events;
 - Maintenance of operational monitoring and management tools;
 - Operational Scripts; and
 - Operational Procedures.

8.2 Use of State Employees for Ongoing Managed Services Operations

The State requires the Contractor to design, implement and be responsible for the ongoing operations of the SOCC in accordance with the requirements and Service Levels described herein. The State wishes to move to a model that leverages to the greatest extent possible State employees in full-lifecycle (i.e., plan, design, build and operate) activities as lead and supported by the Contractor in delivering Managed Data Center Services to the State.

The Contractor must design a high performance operation and associated organization to deliver these services. As part of Offeror responses, an organizational chart, by function must be presented that is populated with staffing, experience, skill, education, certification levels, etc. with notations as to Contractor provided or State provided Staff as proposed to successfully operate Data Center Managed Services within the prescribed Service Levels to the State.

Offerors must specify the anticipated number, experience/skill levels and other considerable factors with respect to delivering the anticipated Scope of Work within the specified Service Levels in a format similar to the following ***illustrative example***:

Service Area	Function	Expected Total Staffing Level	Expected State Provided Staff	Key Skills/Experience
Help Desk	Supervisor	4 FTE	2 FTE	<ul style="list-style-type: none"> ▪ 6 years of relevant experience ▪ ITIL Certification ▪ MCSE Certification
	Sr. Analyst	5 FTE	4 FTE	etc
	Analyst	12 FTE	9 FTE	
	Technician	8 FTE	8 FTE	
Server Administration	Technical Lead	10 FTE	2 FTE	
	Server Administrator	23 FTE	20 FTE	
	Jr. Server Administrator	15 FTE	15 FTE	
	Security Analyst	8 FTE	4 FTE	

During the initial phases of the project, and prior to the commencement of transition, the State will work with the Contractor to determine the assignment of specific personnel to the project and ongoing Managed Service.

In no way must the Contractor be expected to directly participate in employee hiring, evaluation, compensation, career counseling or other activities that are directly related to the existing relationship between the State as the employer and the State IT labor force as the employees. A possible exception to this involvement may include providing input into any skills training, certifications, qualifications and similar educational requirements as recommendations (in aggregate) to the State as it pertains to working to ensure that State employees have or acquire the requisite skills to perform the functions in such a manner as to deliver the scope of contracted Managed Service work within the specified Service Levels to the State.

State employees that are assigned to the Managed Service as provided by the Contractor must remain State employees and be afforded all of the rights, responsibilities and benefits that they would otherwise enjoy as an employee of the State.

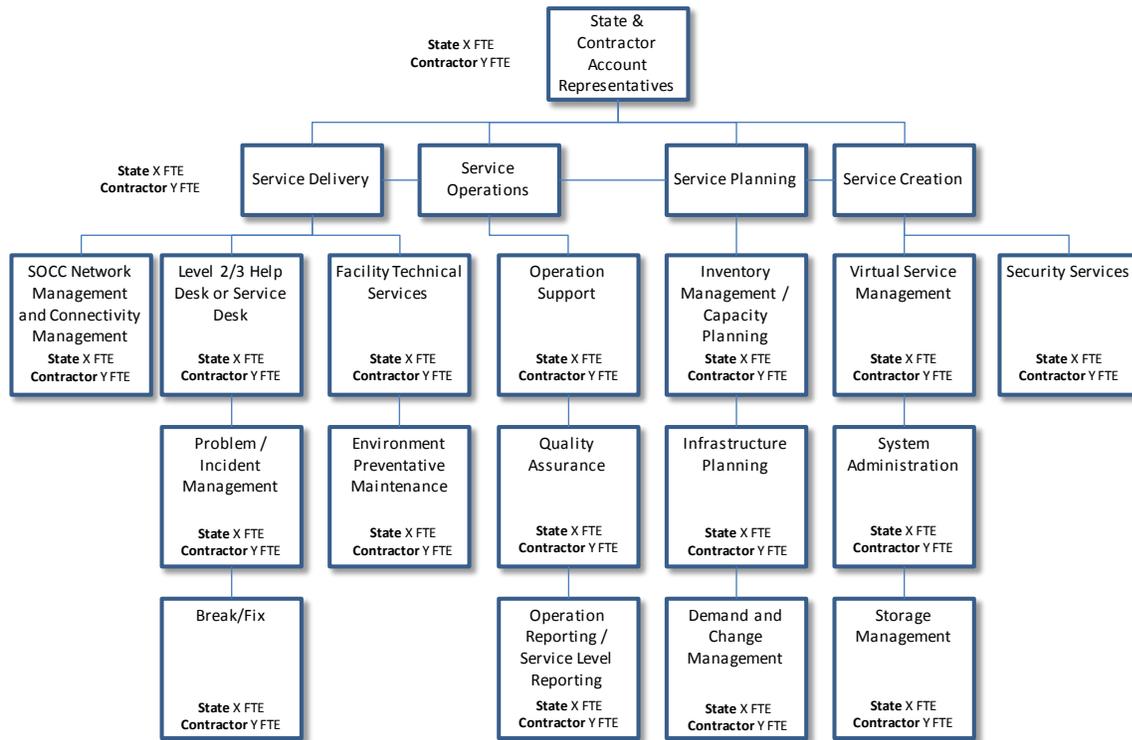
State employees must only be dedicated, while under the employ of the State, to services directly related to State business within the SOCC. State employees must not be permitted to participate in any commercial activities that are performed by the Contractor within the SOCC or outside of the SOCC for non-State approved customers of the Contractor.

8.3 Determining Specific Initial and Final Operational Roles and Responsibilities and Staffing Levels

Following an assessment of current State capabilities and in light of required operational requirements specified herein, the Contractor will propose a final Operational Roles and Responsibilities matrix that specifies the required organizational model to provide and operate the services at the required Service Levels described herein with a combination of Contractor and State personnel prior to the completion of the transition to steady-state operations.

For purposes of Offeror responses, a relative team size assessment is requested that clearly identifies State, Contractor and (if required) third party staffing, general team descriptions inclusive of roles, responsibilities and organization as follows:

Conceptual Steady-State Service Delivery Team Organization (illustrative)



Offerors are instructed to alter this illustrative organization chart as part of their responses as they see fit. Offerors should not infer any desired organization structure or staffing level from this illustration and are requested to propose ideal organizations, staffing levels, mix of Contractor/State staffing as to deliver the specified Services within the required Service Levels.

8.4 Key Contractor Personnel

During the Contract, the Contractor will designate an individual who will be primarily dedicated to the State account who (i) will be the primary contact for the State in dealing with the Contractor under the Statement(s) of Work contained herein or in effect, (ii) will have overall responsibility for managing and coordinating the delivery of the Services, (iii) will meet regularly with the State Account Representative and (iv) will have the authority to make decisions with respect to actions to be taken by the Contractor in the ordinary course of day-to-day management of the Contractor’s account in accordance with this Scope of Work (the “Contractor Account Representative”).

During the Contract, the State will designate a senior level individual and suitable alternates to perform this role in the event of vacation or absence who (i) will be the primary contact for the Contractor in dealing with the State under this Scope of Work, (ii) will have overall responsibility for managing and coordinating the receipt of the Services, (iii) will meet regularly with the Contractor Account Representative and (iv) will have the authority to make decisions with respect to actions to be taken by the State in the ordinary course of day-to-day management of this Scope of Work (the “State Account Representative”).

In an effort to develop an environment in which the Services may be provided in an effective manner, the State and Contractor may jointly designate from time to time certain key Contractor management positions, including the Contractor Account Representative (“Key Personnel”).

Key Personnel will include the following:

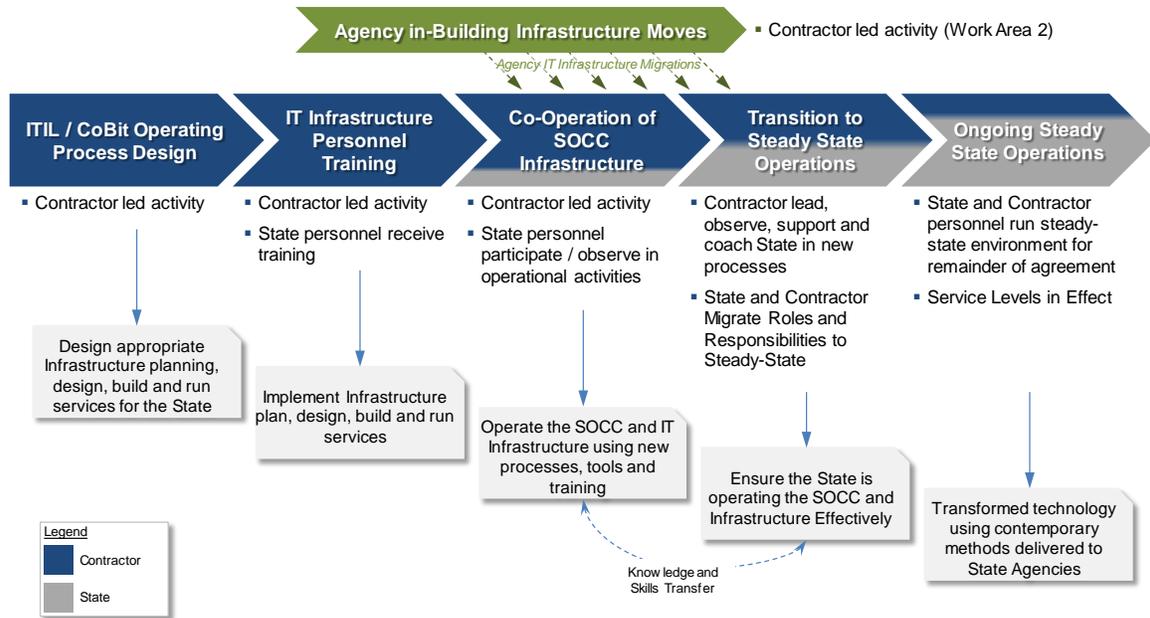
- Contractor Account Representative
- Managed Services Delivery Team (ongoing Run Services for life of Agreement)
 - ITIL Services Lead (e.g., responsible for Inventory Management, Capacity Monitoring and Planning, Financial and Operational Performance, Service Levels and Key Metrics)
 - Server/Environment Lead
 - Storage Lead
 - Networking Lead
 - Facility Technical Management Lead
- Infrastructure Services Delivery and Implementation Project Team (project inception through transition to ongoing Run service)
 - PMO Lead
 - Technical/Finance Lead
 - Training Lead
 - Managed Service Readiness and Change Lead

In the event Contractor hires an existing member of State personnel to perform work within the scope of the RFP or subsequent Contract, Contractor will adjust its fee schedule to accommodate any reductions in travel, relocation and other costs associated with such personnel's participation in delivery of the services contained within this RFP to the State. The Contractor will not be relieved of any obligations contained herein as a result of employing or utilizing existing State personnel to fulfill contract obligations.

8.5 Training Program, Knowledge Transfer, and Change Management

The overall objective of this Work Area is to design, implement and operationalize certain ITIL/CoBit processes to best position the State for the efficient and cost effective operation of IT Infrastructure. It is essential that Offerors design activities, deliverables and work products in this area to maximize operational knowledge transfer, provide opportunities to observe these new work practices, procedures and tools in a live, but controlled, situation and work to ensure that once the State resumes operational control of the IT Infrastructure Operation that the work practices, procedures and tools are fully exercised and refined to the greatest practical extent possible. Conceptually, the activities in this work area are as follows (*note: certain activities from Work Area 2 are shown for relationship purposes only*):

Conceptual ITIL / CoBit Implementation Strategy



Change management scope for the State’s IT Infrastructure Services (**Managed Service**) include stakeholder engagement, communications, training, agency readiness, SOCC readiness, all of the components of the Service Management Framework, business process reengineering, workforce transition, and the agency rollout strategy and execution.

Managed Service training is comprised of four training efforts: training for State-wide process changes, training for Managed Service employees, training for central agencies, and Contractor provided training. These four training efforts are collectively divided into the following key delivery areas:

- Training Development
- Training Delivery
- Post-Training Responsibilities

For clarity, the table below provides a high-level overview of the relative responsibilities for activities required in this Work Area. For the “Contractor Owned” activities, the State required the Contractor to take primary responsibility and drive the work effort; for the “Contractor Supported” activities, the State will take primary responsibility but will expect the Contractor to provide support in the creation and delivery of program materials; for the “State Owned” activities, the State will be primarily responsible and it is expected that the Contractor would have little to no involvement in these areas. The specific requirements of the Contractor are described in more detail in the following sections.

Contractor Owned	Contractor Supported	State Owned
------------------	----------------------	-------------

Contractor Owned	Contractor Supported	State Owned
<ul style="list-style-type: none"> ▪ Training Approach ▪ Training Logistics ▪ Training Environments ▪ Training Data Sets ▪ Training Delivery ▪ Service Management Framework ▪ Change Readiness Assessments ▪ Staffing Requirements ▪ Contractor Readiness ▪ Organization Design for the SOCC ▪ Workforce Transition Approach and Timeline ▪ Workforce Transition Plan for IT Infrastructure Services 	<ul style="list-style-type: none"> ▪ Communication Development and Deployment ▪ Communications Plan ▪ Maintenance/Updates ▪ Recruitment Interview Materials ▪ Training Material Development and Rollout ▪ Onboarding process for IT Infrastructure Management Employees ▪ Stakeholder Analysis Maintenance and Updates ▪ Agency Readiness for all Phases and Work Areas 	<ul style="list-style-type: none"> ▪ Collaborations with Individual State Employees ▪ Recruitment Interview Execution ▪ Business Process Reengineering for IT Infrastructure Workforce ▪ Agency Retained Workforce Organization Design ▪ Communication Content and Direction

The State acknowledges the Contractor has experience in this area and seeks to incorporate best practices generally available in the marketplace. This section highlights the State’s view of the minimum set of activities, deliverables and milestones required to implement the desired capabilities with respect to IT Infrastructure management. The offeror must include any additional considerations that would increase the overall probability of success and result in a high quality of delivery.

8.5.1 Training Design

End-to-end process training must incorporate all relevant Contractor and State policies, procedures and guidance as defined by a State training lead. Existing system training materials may be leveraged for many of the major processes, but it is the Contractor’s responsibility to make the necessary updates to these materials and create any additional content necessary to turn them into comprehensive end-to-end process training for the in scope processes.

It is expected that all training materials will be developed in close cooperation with the State training lead and owners and each of these deliverables will require State signoff. The deliverable descriptions provided in the next few paragraphs outline the current view of the State with respect to training and may not include all of the final requirements for the deliverable.

The Contractor will:

- Be responsible for the development of end-to-end process training materials for all processes within the scope of Managed Service, including those that impact the central agencies.
- ★ Develop training materials to support the successful transition of existing State employees and new employees into the Managed Service.
- ★ Deliver to the State training lead a comprehensive training approach and detailed timeline for the following deliverables shortly after the initiation of the Build Phase:
 - Training approach
 - Curriculum design
 - Annotated outlines
 - Course designs
 - Comprehensive training pilot
- Outline the Contractor’s governing principles and methodology for instructional design, including the methodology for determining training course delivery method(s) as well as selecting training development tools and software;
- Include the templates and style guides that will be utilized for training material development and the methodology for conducting task-to-role-to-course mapping;
- Develop curriculum designs including a course listing with course descriptions and the rationalization for the division of materials between courses;
- Develop estimates for course length and timing and a task-to-course mapping.

- Lead a comprehensive training pilot including a complete walkthrough of each training course with the State training lead, training owners and key business stakeholders. This pilot will serve as a dress rehearsal to verify all significant training issues have been identified and resolved prior to this point. The pilot must be conducted early enough in the timeline to allow the full integration of State feedback prior to train-the-trainer.
- Develop training courseware, including job aids, roles and responsibilities, common error identification and remediation, and other operational functions as required to support the Managed Service.
- Work with State resources to develop training scenarios that are “real life” and applicable to State employees to support training.
- Identify the required performance skills and any prerequisites necessary to utilize and understand the training and develop any training materials necessary to address skill gaps.
- Design and build training exercises to allow trainees to apply what they have learned.
- Revise training materials based on early experiences and feedback from training delivery personnel to enhance and streamline ongoing training materials.
- Upload and maintain all training materials on the OIT team collaboration SharePoint.

The State will:

- Develop and deliver Transition Workshop materials to educate the agencies on high-level process changes that will affect all agencies. The goal is delivery of these workshops prior to go-live for the state-wide process changes. It is expected that the State will take full responsibility for these workshops, but may contract with the Contractor for assistance.

8.5.2 Training Delivery

The Contractor may be required to lead training delivery for the Managed Service. The State will determine the extent of Contractor involvement in training delivery in addition to the minimum requirements listed below at a later date.

As part of this activity area, the Contractor will:

- Conduct detailed train-the-trainer workshops to prepare trainers for course delivery by focusing on the process and technical aspects of the training curriculum, including adult learning principles and facilitation techniques;
- Provide an end user training program that is scalable to the number and frequency of agencies and processes rolling into the Managed Service
- Design training reviews for both end user training and train-the-trainer and implement a method for evaluating the effectiveness of training that accurately measures whether or not real learning has occurred and how it can be demonstrated
- Establish a plan for tracking and reporting on training attendance and effectiveness measures for both end user training and train-the-trainer
- Perform knowledge transfer to embed the training capabilities within the Managed Service
- Develop an approach and plan for end user support after they have attended training but before go-live
- Establish a plan and build any necessary tools to manage the escalation of questions from training sessions and the communication of answers back out to trainers

To the extent that the State requires the Contractor to lead the training delivery, the Contractor will be required to provide an additional Statement of Work to be used as the basis for a formal Contract change order.

8.5.3 Post-Training Responsibilities

After the final wave of end user training is completed, the Contractor will:

- Revise all training materials in a final form to the satisfaction of the State, providing revisions do not alter the approved training design, and transition the materials to the State. Requested changes to the approved training design, would require an approved change request.
- Establish procedures and documentation for ensuring that the training team is informed of all updates to production after go-live and the training environments are included on the relevant migration paths
- Facilitate a post-training analysis to gather and document lessons learned and update communication and training plans accordingly.

8.5.4 Change Management

The State wishes to establish an organization design for the Managed Service which is deemed critical to the success of the project. The Deliverables described in this section are minimum requirements; the Contractor must work with the State to finalize the exact parameters of the Deliverables in the initial weeks of the project.

The Contractor will:

- Drive the implementation of the Managed Service organizational design;
- Lead the development and implementation of the workforce transition plan to support the State in transitioning employees into the Managed Service;
- Enable the Managed Service to focus on employee development, continuous improvement, and accountability;
- ★ Deliver a comprehensive Workforce Transition Approach that includes but is not limited to:
 - An overall high-level timeline for getting IT IS operational, including milestones/deadlines for finalizing staffing needs, identifying employees that will be transitioned, trained and on-boarded, readiness assessments for Managed Service employees, and post-go-live support
 - Best practices and tools for developing an interim staffing plan at the agencies for the time period after employees have been moved to the Managed Service but before the Managed Service is fully operational
 - Best practices and tools for conducting skills assessments, gap analyses, and creating training plans
- ★ Build on the foundational Workforce Transition Approach to create a Workforce Transition Plan that includes the following:
 - Detailed overall workplan and timeline for establishing and making operational the Managed Service
 - Detailed timeline and milestones for staffing the Managed Service
 - Detailed timeline and milestones for the Managed Service onboarding process
 - Best practices and examples for Managed Service position descriptions
 - Best practices and examples for Managed Service recruitment interview materials

Furthermore, to ensure a successful transition of existing and potentially new employees into the Managed Service and create the desired culture, the Contractor will:

- ★ Develop a plan and timeline for establishing an organization design that was completed during the Design Phase.
- Provide best practices and examples of job descriptions and staffing plans and support the State in developing - specific position descriptions.
- ★ Develop workforce transition materials including but not limited to skill and competency assessments, gap analysis tools, and supply and demand analysis tools.
- Develop a multi-faceted employee development and training program and materials that aid employees in becoming more proficient in the established competencies, skills, knowledge and experiences needed at the Managed Service (as determined by the State). Components of this program may include but not be limited to coaching, mentoring, job rotation, instructor led training, etc.
- Develop success profiles for each role within the Managed Service, to include specific competencies, skills, knowledge and experiences needed to succeed in the position.

- Develop and implement a Managed Service on-boarding program using best/leading practices to drive/reinforce the desired culture.

8.5.5 Knowledge and Skill Transfer / Validation

The Contractor must develop, review and revise with the State and implement a Knowledge Transfer and Skill Transfer / Validation program that is designed to apply and validate the effectiveness of the principles and learning's associated with new operational processes and tools to live IT Infrastructure tasks and activities. Depending on the work area, and based on the Offeror's experiences in delivering similar engagements, the approach may vary from: 1) training only; 2) training supplemented with on the job execution (with or without contractor mentoring); 3) observation and participation in Contractor's performance of tasks prior to a handoff to the State; or 4) cooperative operation of a function between the Contractor staff and State staff.

The knowledge and skill transfer /Validation approach should include:

- Identification the key knowledge owners and the knowledge to be transferred from current practices to the new service operations unit when the new personnel will be delivering the service post transition
- ★ Definition of Knowledge Transfer Plan and implementation of the plan, adjusting it as needed
- Obtaining agreement from each knowledge recipient that he or she has received the knowledge needed to function in the new organization
- ★ Development and implementation of the Knowledge and Skill Transfer approach that includes (at a minimum)
 - Purpose
 - Objectives
 - Guiding principles
 - Overall knowledge transfer approach, e.g., classroom training, job shadowing, remote knowledge transfer
 - Key activities
 - Roles and responsibilities/organization structure
 - Plan, including key activities, deliverables, and milestones
 - Tools
 - Resource requirements
 - Success criteria
 - Communications
 - Infrastructure required
 - Cost

8.6 Organization of Service Delivery Areas:

In general there are four areas under which the Contractor services will be delivered:

1. **Design Services** – those services designed to assess the current state of systems and operations sufficient to design and implement computing infrastructure operations and management services to support current and anticipated demands of the State.
2. **Migration Services** – those services designed to facilitate the successful migration from the current operations and management environment to the future state architecture designed in the Transition Services area.
3. **Steady State Run Services** – services and operations designed to support the ongoing operations of the in-scope computing environments.
4. **Infrastructure Management Services** – related services designed to administer and support a high performance, high quality and resilient computing infrastructure required by the State.

Each will be discussed in turn.

8.7 Design Services

8.7.1 Planning and Analysis Services

The tasks and activities to be performed by the Contractor as part of the planning and analyzing phase of the existing computing environment which includes the following activities and processes to be delivered by the Contractor and State to the enterprise:

- ✧ The Contractor must be responsible for managing the process of analyzing, implementing improvements to, and documenting operations, management and maintenance planning functions with the State business and technology staff. In addition, Contractor must assist in developing and refining detailed infrastructure operational and management requirements.
- ✧ Based on such requirements, Contractor must develop functional and technical operating and maintenance plans for each computing environment and prepare a scope and operations plan which will include assessing the resource requirements (e.g., hardware, software or personnel), time requirements, known impact or dependencies on other projects, and other information as required. In addition, such requirements must explore solution development or the possibility of alternative sourcing and implementation options including, where applicable, providing build versus buy analysis and support.
- Provide support to the State in the creation and evaluation of proposed strategies and standards to better coordinate and enforce information and technical architectures across the State’s business units and to develop recommendations on information and technology use within the State.
- ✧ Define high-level solution blueprints and change plan templates for each major functional and/or service domain area (a combination of “user/services type e.g., “file server”, “compute server” and “general office productivity, “engineering application”, “workflow server”, “database server” etc.).
- Conduct progress reviews with appropriate State personnel.
- Estimate the overall operational cost and schedule for the State to more optimally manage the cost of providing infrastructure services to State Agencies. As part of this process, prepare a cost and work schedule and labor for the design, development, implementation and training required for each project to be implemented by OIT for an agency. Each project plan must, at a minimum: (i) include schedules that specify a detailed level of activity, including the planned start dates, completion dates, hours and other required resources for activities to be performed by Contractor (and the State where applicable) pursuant to the project for which such project plan was developed; (ii) identify any pre-existing software components (e.g., code libraries) and tools to be used; (iii) licensing or purchase requirements of any third party components, tools or software elements including operating system software, operational tools and instrumentation, operational productivity aids and other tools required to deliver the solution to the State; (iv) include a detailed list of the deliverables and milestones (with planned delivery/completion dates) and the project management reports that will be provided; (v) describe any assumptions made in compiling the plan; and (vi) identify any State dependencies or personnel requirement assumptions.
- As a planning foundation, establish and publish baseline performance levels of applications, servers, networks, processes and other measureable elements of system performance for the current “status-quo” environment to be used as the basis for performance validation and ongoing improvements in the post Contractor transfer operational environment.
- Identify potential risks due to uncertainty with the overall infrastructure solution’s complexity and feasibility.
- Coordinate and confirm the State’s approval of project requirements, business case, and commitment to proceed with project delivery.

8.7.2 State Infrastructure Environment Design-Build Services

Contractor must design, develop and build technical and functional designs for each service domain of the computing environment. The environment design and build services must also include the following:

Design. The build designs will include, where applicable based on the size, complexity and requirements of the system(s), server(s) or application(s), design of files, databases, forms, user interfaces, reports, security, system performance and availability instrumentation, audit trails of the transactions processed, provision for parallel testing, development of fallback procedures, provision for recovery procedures from production failures, disaster recovery procedures, creation of job scheduling, and provision for on-line viewing of reports. As part of the design process the Contractor must also:

- Analyze related State servers and environments to identify any additional IT solution requirements required to deliver the services.
- Assess current IT solution gaps and/or dependencies.
- Create IT system/solution designs to support solution requirements
- Design and implement an user/agency interaction model which defines and enforces applicable standards, solution prototypes, and virtualization designs including the design and implementation of reports and forms to support these processes
- Design integrated solution components and interfaces to external systems.
- Design logical environment, data conversions, processes and procedures as agreed necessary.
- Compile and maintain solution issue lists.
- Document design specifications and create applicable acceptance criteria.
- Conduct quality and progress reviews with appropriate State personnel.
- Establish assembly, configuration, environmental, performance, and user acceptance test plans.
- Coordinate and confirm the State approval of solution design specifications and applicable acceptance criteria.
- Determine and identify relevant baseline system performance profiles or capabilities sufficient to design a robust and performance compliant solution in the Contractor environment as well as to serve as the basis for performance comparisons following migration to the Contractor's facilities and services.
- Provide the State with regular reports tracking the progress of Contractor's design work. In addition, Contractor must provide timely responses to the State requests for information and reports necessary to provide updates to the State business units and stakeholders.

Build. Contractor must be responsible for the development and implementation of operational and technical processes required to generate systems environments required to successfully support agency infrastructure platform requests. Contractor must provision for the development of operational documentation sufficient to operate the environment to support agreed upon service levels and incorporate the use of documentation standards, reviews, and audit trails, including release control. User walk-through of the systems environment will be provided upon request. Contractor's documentation will include the creation and testing of test and production procedures and job schedule, as appropriate.

- Contractor must also design and implement processes and systems to deliver the following tasks and activities in connection with building infrastructure environments:
- Perform detailed technical design as agreed appropriate.
- Build solution components to support approved design specifications
- Configure and customize solution user interfaces, process and procedures as required.
- Configure and customize solution environments including CPU, disk and memory configurations
- Configure and customize integrated solution components and interfaces to external systems.
- Coordinate with the State Infrastructure Management experts to implement other physical environmental requirements and designs.
- Wherever possible, utilize contemporary and supported third party Contractor tools to perform design, development and documentation tasks.
- Provide build, prototyping and test environments as required to perform the development work.
- Perform unit test for solution components and assess quality and completeness of results.
- Document solution and refine applicable user acceptance/validation criteria.
- Develop any applicable State-specific train-the-trainer materials, as follows:
 - Perform training needs analysis.
 - Determine the training material/method of delivery design with the State.
 - Develop the required training material to support the agreed upon approach and methods of delivery.
- Coordinate with the State Infrastructure Management experts to implement required technology environment changes as mutually agreed.

- Compile and maintain issue lists.
- Develop environments in accordance with the State strategies, principles, and standards relating to technical, data and applications architectures as set forth in Statements of Work
- Conduct Build progress reviews with appropriate State personnel.
- Coordinate and confirm the State's approval of solution components and verification of applicable acceptance criteria for transition into Test/Validation activities.
- Provide the State with reports on a weekly basis tracking the progress of Contractor's performance of build activities and deliverables. In addition, Contractor must provide timely responses to the State's requests for information and reports necessary to provide updates to the State's business units and stakeholders.
- Track and report to the State hours of labor expended on system environment development/provisioning activities. Such time reporting must be as agreed upon by the parties such that it reasonably describes the work performed.

Test/Acceptance. Each environment development project must be subject to a formal testing and acceptance process that uses objective and thorough test or validation criteria established by the OIT and an agency that will allow the parties to verify that each project meets the specified functional, technical and where appropriate, performance requirements.

- ★ The testing and acceptance process must be developed for each environment development project as soon as possible after establishing the business and user requirements. The testing and acceptance process will include an audit trail capability for tracking and correcting problems. The tasks and activities that Contractor must design and implement as part of the State's testing and acceptance process also include the following:
 - Develop and maintain test data repositories as agreed appropriate.
 - Develop test plans, scripts, cases and schedules as agreed appropriate.
 - Perform the following testing activities for solution components and assess quality and completeness of results including:
 - a) System Test / Assembly.
 - b) Product Test including integration testing and regression testing new releases of existing solutions.
 - c) Performance Test including regression testing new releases of existing solutions.
 - Provide test environments as required to perform the system and user acceptance testing work, and where appropriate performance validation testing The test environments will be designed and maintained by Contractor so that build and subsequent testing activities will be sufficient to verify that end-user perceived performance on the Contractor provided environment is consistent with the pre-transfer baseline and as to minimize issues associated with the migration of environments to the Contractor.
 - Support the following testing activities relating to a State agency's performance of user acceptance test ("UAT") for solution components as follows:
 - a) Develop with the State agreed upon UAT test plans, scripts, cases and applicable acceptance/validation criteria.
 - b) Coordinate UAT execution and acceptance procedures with the appropriate State participants.
 - c) Record and report UAT results.
 - d) Review changes, fixes and enhancements with the participants in the UAT testing.
 - e) Correct identified defects and nonconformities in accordance with the acceptance process.
 - f) Compile and maintain solution issue lists.
 - Conduct quality and progress reviews with appropriate State agency personnel.
 - Coordinate and confirm State agency approval of solution components and verification of applicable acceptance criteria for transition into deployment and production (steady state) use.
 - Provide the State with reports on a weekly basis tracking the progress of OIT's delivery of testing work, or in the case of user acceptance testing, support of the State Agencies activities. In addition, OIT must be positioned to provide timely responses to the State agency requests for information and reports necessary to provide updates to the State business units and stakeholders.

Deploy. Contractor must be responsible for designing and implementing processes that support the production deployment and roll-out of newly developed infrastructure environments. Deployment includes software environments accessible from the End User Desktop Equipment or local file Server elements (if applicable), identification of interfaces and any required data migrations, installation and testing of any required middleware products, installation of licensed software elements, and any required testing to achieve the proper roll-out of the computing environment(s).

- ★ Contractor must design and implement processes to comply with the State agency required implementation and deployment procedures as set forth in Statements of Work between OIT and the State agency. This may include, network laboratory testing, data migration procedures, the use of any pre-production or pseudo-production environment prior to production migration. OIT must be positioned to submit to the agency, for agency approval, a written deployment plan describing OIT's plan to manage each such implementation.
- The tasks and activities to be performed by Contractor as part of the deployment services design and implementation also include enabling OIT to perform the following:
 - a) Execute required data migrations.
 - b) Perform required data matching activities and error reporting.
 - c) Document data issues and provide to the agency for resolution.
 - d) Coordinate and confirm agency approval of data conversion results.
 - e) Conduct production pilot and fine tune solution as agreed appropriate.
 - f) Compile and maintain solution issue lists.
 - g) Support communication effort and identify required communication recipients and communicate deployment activities to deployment stakeholders.
 - h) Evaluate detailed communication feedback from recipients and stakeholders.
 - i) Identify the effectiveness of and need for additional communication.
 - j) Determine the requirements for, and support the State in the development of End-User training for the computing system(s) or environment(s) resulting from the each environment migration project including the roll-out of workshops, self-study guides and computer-based training and train-the trainer activities.
 - k) Support train-the-trainer activities.
 - l) Confirm timeframe, type, content, and target user audience of planned training.
 - m) Perform training with the agency trainer's audiences.
 - n) Assess the effect and value of conducted training and cooperate to resolve issues identified.
 - o) Conduct bi-weekly quality and progress reviews with appropriate agency personnel.
 - p) Develop, and thereafter maintain and make available to the agency, documentation gathered throughout the project's life and allow for re-use of such documentation for future projects.
 - q) Transition solution support responsibility to the State's steady-state operations maintenance team.
 - r) Conduct a post-implementation review process upon the completion of each infrastructure development project, and where appropriate document requirements for future enhancement of the business systems environment implemented as part of the project

8.7.3 Migration Services

Contractor must be responsible for designing and implementing processes and procedures to support the migration of systems, system components, IT infrastructure and related operational support in transitioning from the current environment to the shared and Managed environment(s) to enable the services to be provided under an agreement with a State agency to the extent defined and agreed within Statements of Work. Contractor's responsibilities with respect to Migration Services include the following tasks, activities and responsibilities:

- ★ During the period beginning on the Effective Date and ending on or before date agreed by the parties Contractor must plan, prepare for and conduct the migration of IT infrastructure systems operations (the "Migration" as described in section 6 of this RFP). Migration must include the moving of systems and related operational support from currently existing facilities/locations to the SOCC as agreed between the State and Contractor. Contractor's responsibilities with respect to the Migration include:

- Working with the State network providers, establish communications lines and network connections, and providing equipment, software, tapes, records and supplies, as made necessary by the migration;
 - Maintaining the Services and using commercially reasonable efforts to not otherwise disrupting the State’s business operations;
 - Specifying costs and effort associated with the migration, including communications lines costs (both installation and ongoing); and otherwise performing such migration tasks as are necessary to enable Contractor to provide the Services, including following the Migration.
 - Migrations must be conducted in accordance with a written plan (the “Migration Plan”) which must include the following items. The Migration Plan will be created as a Deliverable as part of section 6 of this RFP.
- ✳ Contractor must be responsible for extending the migration plan (as described in section 6) to include elements required to migrate IT infrastructure elements and services that are not currently located within the SOCC to the SOCC. Contractor must cooperate and work closely with the State in finalizing the Migration Plan (including incorporating the State’s reasonable comments) and the final Migration Plan must be subject to written approval by the State and include:
- A description of the IT operations being migrated;
 - Baseline performance attributes of the system/environment being migrated
 - A description of the methods and procedures, personnel and organization OIT will use to perform the Migration of infrastructure services to the SOCC;
 - A schedule of migration activities;
 - A detailed description of the respective roles and responsibilities of the OIT, the agency and the Contractor (if applicable);
 - Such other information and planning as are necessary to ensure that the Migration takes place on schedule and without disruption to the agency’s operations;
 - A process by which an agency may require OIT to stop proceeding with all or any part of the transition if the agency determines in good faith that such transition, or any part of such transition, poses a risk or hazard to the State’s business interests and allowing the agency to require OIT to stop proceeding with all or any part of the transition for any other reason;
 - Validation of successful migration inclusive of user acceptance and assessment of acceptable performance with respect to comparison to baseline performance attributes collected during prior phases.

No functionality of the IT operations being migrated must be disabled until the new service, process or procedure is demonstrated to conform to the requirements set forth in any related Statements of Work, operational performs and is performing conformant to agreed upon service levels, and has been authorized and accepted by State management.

8.8 Design, Implement and Provide Ongoing Steady-State Run Services

The Contractor must be responsible for designing, implementing and the ongoing operation of the State computing environment. In performing computing environment operations and maintenance activities, the Contractor must perform such activities in such a way that computing environment resources (e.g., network, hardware and associated storage) are utilized with a high degree of efficiency and in a manner as to not compromise the timely completion of such activities or service level requirements outlined in section 11.0. The Contractor’s general responsibilities with respect to Computing Environment design, build and run activities include the following tasks, activities and responsibilities listed below.

8.8.1 Steady State Operations and Maintenance Services

Steady State Operations and Maintenance Services under this Contract begin following the successful transition of a Computing Environment to the Contractor. As a prerequisite to successful transition, the Contractor must obtain

authorization from the State based on satisfying conditions of transfer, which include conforming to agreed upon service levels and completing the requirements defined throughout section 8.9.

8.9 Design and Implement Non-Discretionary Services

The Contractor must, through support and maintenance control processes, maintain support of the solutions developed by the Contractor for the duration of the Project. The following processes are to be designed and implemented at the State as part of the Project until such time as the State is reasonably capable of assuming operations for these processes. Such ongoing support and maintenance will include the following tasks and activities:

8.9.1 Level 2 and 3 Support

The Contractor must provide Level 2 and Level 3 infrastructure and facility support to the State for the scope of the services described herein. For purposes of clarity, Level 1 support refers to any application or agency specific help desk that directly interacts or interfaces with end users on matters such as simple technical requests (e.g., password resets, user id setup, general procedural questions), business process or end-user application specific questions (e.g., "how do I?"). Questions, issues, problems or incidents that are escalated to Level 2 from a Level 1 source should be assumed to be pertinent to the services contained in this RFP as they relate to IT Infrastructure Service and/or SOCC facility technical management. Additionally, the Contractor must:

- Track, monitor, respond to requests and issues, resolve issues consistent with the established service levels and refer, as appropriate, requests to Break/Fix Support resources for additional assistance when issues cannot be resolved by Level 1 Support.
- Provide documentation for the development of, or modifications to, the Service Desk to help minimize transfers to specialized support.
- Provide State Agencies with an updated list of personnel providing Level 2 Support and "on call" personnel who are responsible for Level 3 Support, including contact phone numbers.
- Work to correct environment defects or problems that require environment code or operational modifications.

8.9.2 Break/Fix Support

The Contractor must provide Break/Fix support for all in-scope environments, specifically:

- Tracking, monitoring and providing remediation for solution defects and issues requiring system configuration or in-scope environment code or configuration changes.
- Monitoring and repairing in-building connectivity, routing and redundancy for networking functions up to Telecommunications provider provided or required demarcation points inclusive of all in-building networking devices, risers, patch panels, cabling, firewalls, protocol translators, connection pooling or aggregators and other in-building networking devices;
- Identifying and implementing required system or configuration changes to address solution defects.
- Maintaining solution documentation (technical specifications and testing documentation) as well as a compendium of common problems, root causes and remedy to aid in the identification and remediation of underlying system issues.
- Testing of configuration changes to confirm resolution of defects.
- Identifying, testing, installing and implementing third party or OEM supplied patches and fixes for third party supplied packaged operational software (including Operating System, BIOS, microcode, patches, service packs and similar), as well as new releases; provided that if a new release contains new features and functionalities, the Parties will agreed to additional services required to enable or disable such features and functions (e.g., configuration, gap analysis, etc.) as part of a separate project related enhancement service.
- Contractor to comply with any State Security mandated patches or system levels to the extent and system enhancement turnaround time required given the nature of the security mandate (e.g., emergency security patches may need to be applied in hours after receiving an authorized request from the State).

8.9.3 Environment Technical Support

The Contractor must provide Environment Technical support for all in-scope environments, specifically:

- Maintaining environment performance, availability and stability of the production environments with the hardware resources.
- Understanding the issues related to in-scope environment and operational requirements from an in-scope infrastructure perspective which may require analysis of the technical components of the system, including the applications, file-systems, database storage, system software and hardware (but not database administration, debugging, tuning or maintenance activities which are out of scope).
- Conducting post-mortem reviews for corrections to technical issues with in-scope environments or operations and incorporation into ongoing continuous improvement initiatives.

The Contractor is not responsible for any application, middleware, or presentation level specific support (other than the underlying hardware, storage, network and operating systems that support these layers) as these are out of scope for this work.

8.9.4 System/Environment Administration Support

The Contractor must provide System/Environment Technical support for all in-scope environments specifically:

- Monitoring environments, applying patches, and administering the system logs.
- Monitoring and managing Storage access, capacities, I/O rates and other space, performance and availability attributes for Storage;
- Performing various technical activities such as code/object migrations, patch implementations, log administration, various data copies and exports, and general assistance in issue resolution such that migrations into production will be executed at agreed periodic intervals and other production changes will be scheduled during the maintenance window.
- If requested in writing by the State, supporting multiple release levels of environment software/hardware elements.
- Contractor to maintain an email listing for each logical server resource. When the server resource has an unscheduled outage or reduction in performance, Contractor to notify server user list based on outage/service reduction and promptly after server/service restoration.
- Contractor must make available to end users trouble ticketing system that contains all open tickets for that user, estimate to complete ticket, ticket prioritization etc. as well as all service level impacting items whether agency or OIT initiated.

8.9.5 Environment Preventive Maintenance

The Contractor must provide Preventative Maintenance Services for all in-scope environments specifically:

- Performing environment/server tuning, code restructuring, load balancing, storage administration and facility network management and provide tools and other efforts to help improve the efficiency and reliability of environments and to help reduce ongoing maintenance requirements and costs.
- Assessing, developing, and recommending opportunities to reduce (or avoid) costs associated with environment support and operations.
- Providing appropriate data for periodic agency analysis and review of resources deployed for preventive maintenance and planning preventive maintenance.
- Monitoring and analyzing trends to identify potential issues and following-up on recurring problems.
- Maintaining environments in accordance with the State's strategies, principles, and standards relating to technical, data and Applications architectures as agreed upon in Statements of Work.
- Performing: (i) adaptations to the Computing Environment as necessary to maintain the operability and full functionality of such services following new releases, enhancements and upgrades (of Systems Software or underlying operational software), and (ii) other work to implement technology changes (e.g., System Software

upgrades or new scheduling Software). Included in the scope of such adaptive development work is testing new interfaces to Applications.

8.9.6 Production Control and Scheduling

The Contractor must provide Infrastructure level Production Control Services for all in-scope environments, but exclusive of any agency applications and production schedulers specifically:

- Supporting the various service support tiers (e.g., 9x5, 16x5, 9x7, 24x7, compute processing, intermittent continuous operations on-demand) production-availability schedule as agreed with the State and authorized agency users.
- Monitoring, coordinating with designated agency production staff, and managing production schedules.
- Updating access and parameter or environment configurations contained within in-scope environments where applicable.
- Establishing a production calendar inclusive of daily and periodic maintenance activities.
- Generating and providing access to daily production control and scheduling reports, including the production of monthly summary reports that track the progress of OIT’s performance of maintenance work.
- Providing timely responses to an agency request for information and reports necessary to provide updates to the State’s business units and stakeholders.

For purposes of clarification and illustration, the following table is provided to aid Offerors in determining the scope of the requested service:

In Scope (examples)	Out of Scope (examples)
<ul style="list-style-type: none"> ▪ Contractor provided (or utilized) Job Schedulers that directly support the in-scope operations ▪ Automated operating system, BIOS, patches or other software distribution or patching Schedulers/Mechanisms ▪ Scheduled Virus/Intrusion Scans of in-scope Devices ▪ Scheduled in-scope inventory scanning, resource utilization, configuration validation processes ▪ Scheduled report generation or distribution for SOCC help desk processes 	<ul style="list-style-type: none"> ▪ Agency Specific Job Schedulers ▪ Application specific job schedulers ▪ Mainframe Job Schedulers ▪ State interfaces to outside of State job schedulers ▪ Network Data Movers/Exchanges ▪ Application Operation and Maintenance ▪ Application Break Fix ▪ Database DBA or Performance Tuning <p>However: the infrastructure elements (e.g., servers, storage, networks and the like to the operating system prompt) that support these schedulers, should they reside in the SOCC on an in-scope supported server are in scope.</p>

8.9.7 Operations Support

The Contractor must provide Operations Support Services for all in-scope environments, but exclusive of any agency applications specifically:

- Implementing and monitoring the Environment Management Services operations.
- Monitoring environment operations for correctness and adherence to agreed quality, performance and availability criteria.
- Supporting agency application production staff to create and adapt IT operational processes and procedures related to the in-scope environments.
- Communicating appropriately with the agency designees, authorized users and third party Contractors;
- Performing in-scope ad hoc operations reporting as agreed by the Parties.

- Prioritizing support functions during a crisis.
- Serving as primary point of contact and leading IT operations support for the in-scope environments.
- Acting as a resource with respect to knowledge and information sharing regarding the supported computing environment, as required by agency authorized entities and End Users. This must include providing information and consulting support with respect to: system performance, providing assistance with interface file testing, designing appropriate test environments, performing training, and maintaining system documentation.

8.9.8 Solution and Operations Reporting

The Contractor must provide Infrastructure level Operations Reporting Services for all in-scope environments, but exclusive of any agency applications specifically:

- Providing the State with summary reports on a monthly basis tracking the progress of OIT's performance of maintenance work as well as access to daily reports to confirm progress against agreed upon operational and maintenance calendars. In addition, OIT will provide timely responses to the agency requests for information and reports necessary to provide updates to the State business units and stakeholder constituencies.
- For production or customer impacting issues that result in a down system, or the unavailability of a production component, OIT must report progress based on the service level agreement until the issue is corrected and/or the agency agrees that the issue causing the unavailability situation has been corrected. In all cases, the minimum reporting standard will be dictated by the service level agreement for the impacted service.
- Tracking and reporting to the State hours of labor expended on environment software maintenance activities. Such time reporting must be as agreed upon by the parties.

8.9.9 Ad-Hoc Requests

The Contractor must support ad-hoc requests for all in-scope environments, but exclusive of any agency applications specifically, the following apply:

- Generally, Ad-Hoc requests are infrequent in nature, will require less than 1-2 hours of effort by the Contractor to fulfill or assist with and will be specific to the scope of the work contracted.
- Ad-hoc requests require no modification, configuration, or customization of the environments.
- OIT will provide service on-request to users. Requests will normally be made through the OIT Level 1 help desk to effectively track and manage demand.
- Routine tracking procedures will provide visibility of all ad-hoc requests. OIT and the agency will develop a prioritization approach for Ad-hoc requests based upon business impact.

Examples of Ad-Hoc request may include, but not be limited to:

- Participation in service review meetings with specific Agencies or on a sub-set of a meeting where Contractor expertise may be valuable to the State;
- Assisting the State in troubleshooting an application issue where the root cause is difficult to determine as an infrastructure or application issue (e.g., intermittent connectivity issue, failing storage device, re-boot of an application server);
- Generation of an ad-hoc report based on in-scope data (e.g., server inventory, help desk call volume) to support State decision making; and
- Supporting the State in prospective conversations or capability demonstrations with Agencies that are not currently in the SOCC to migrate to the SOCC.

8.9.10 Minor Infrastructure Enhancements

The Contractor must provide minor Infrastructure Enhancement Services for all in-scope, but exclusive of any agency applications specifically:

- Release upgrades for packaged infrastructure software are initiated through periodic releases by OIT scheduled releases including operating systems, patches, service packs, microcode, BIOS updates, virtualization software, virus scanners, network operating systems and file servers.
- Minor enhancements are initiated when an agency identifies a functional, technical, legal, quality or external requirement that is driving a minor change to the in-scope environment(s).
- Release upgrades and minor enhancements are generally limited (in aggregate) to 10 work-hours or less of total effort for each such project.
- Minor Enhancements will be performed in accordance with the appropriate requesting State agency.

8.9.11 Data Center and Infrastructure Management Services

The Contractor must provide Infrastructure Management Services for all in-scope environments, but exclusive of any agency applications specifically:

- Oversight and management of data center facility as well as the capabilities within the data center itself including air conditioning, power and cleaning as provided by contracted services.
- Supporting data center redundancy approach as agreed to help prevent loss of system availability.
- Supporting physical site planning.
- As a future consideration that is currently out of scope, providing an interface with management at each hosting location (primarily the SOCC), including details on access, site security, environments hosted at site, and other infrastructure specific requirements.
- Supporting media management including maintaining, tracking, and offsite storage of media used by storage devices on standard schedules.
- Providing remote management infrastructure to support the physical needs of environment including changing media, system start up and shut down, as well as physical inspection and mediation of the systems.
- Supporting agency disaster recovery testing activities as they pertain to support in-scope failover or recovery operations, but exclusive of application or presentation level disaster recovery functions.
- Supporting service levels as agreed in accordance with section 11
- Supporting the following system instances to as required to provide environment management services for agency environments including (but not limited to) the following high-level environment classes at a minimum:
 - Development
 - System Testing
 - User Acceptance
 - Production
 - Training/Demonstration

8.9.12 Systems Management and Administration

The Contractor must provide Systems Management and Administration Services for all in-scope environments, but exclusive of any agency applications specifically:

- Coordinating the installation, testing, operating, troubleshooting and maintaining of the operating system.
- Identifying, testing, packaging patches and other updates associated with supported operating systems, as well as supporting additional security-related fixes associated with the operating systems.
- Managing the security functions related to the operating system including administrative access and passwords and the related security controls to maintain the integrity of the operating system, based on State standard service center security processes.
- Configuring and maintaining systems that are being managed by the State for network and remote access.
- Supporting the anti-virus and end-point protection suite solutions for the systems that are being managed by the State.
- Ensuring that, unless otherwise requested by the State under an approved exception request, solution delivery elements including but not limited to: software, microcode, patches, operating systems, connectivity software

are maintained in accordance with the State policies in effect at the time and have a currency level no older than current major release (X) or immediate prior major release (X-1), and in all cases are supported by the 3rd party software or hardware vendor.

- The Contractor must strive to accommodate the agency testing, review and approval processes prior to the installation of these elements in a production environment.
- Providing management services to support the following scope of infrastructure services and roles including (but not limited to):
 - Server administration, set-up and configuration
 - Performance validation and tuning
 - Infrastructure upgrades
 - Infrastructure capacity planning
 - Backup and system restore

8.9.13 Security Services

State Agencies are responsible for Application Layer (and higher) system services and functions that build upon the in-scope infrastructure environment elements, the Contractor shall not be responsible for the implementation of Security Services of these systems as these shall be retained by the State.

The Contractor must be responsible for maintaining the security of information in environment elements under management and in accordance with the State Security Policy. The Contractor will implement information security policies and capabilities as set forth in Statements of Work and, upon review and agreement by the State, based on the Contractors standard service center security processes as they satisfy the State's requirements contained herein. The Contractor's responsibilities with respect to security services must also include the following:

- Support intrusion detection & prevention including prompt agency notification of such events, reporting, monitoring and assessing security events.
- Provide vulnerability management services including supporting remediation for identified vulnerabilities as agreed.
- Support the State IT Security Policy which includes the development, maintenance, updates, and implementation of security procedures with the agency's review and approval, including physical access strategies and standards, ID approval procedures and a breach of security action plan.
- Support OIT in the implementation, maintenance and updating of statewide data security policies, including the State information risk policies, standards and procedures.
- Managing and administering access to the systems, networks, Operating Software, systems files and the State Data.
- Supporting Agencies in implementation of programs to raise the awareness of End Users and staff personnel as to the existence and importance of security policy compliance.
- Installing and updating State provided or approved system security Software, assigning and resetting passwords per established procedures, providing the agency access to create user ID's, suspend and delete inactive logon IDs, research system security problems, maintain network access authority, assisting processing the agency requested security requests, performing security audits to confirm that adequate security procedures are in place on an ongoing basis, with the agency's assistance providing incident investigation support, and providing environment and server security support and technical advice.
- Developing, implementing, and maintaining a set of automated and manual processes so that the State data access rules, as they are made known to OIT, are not compromised.
- Performing physical security functions (e.g., identification badge controls, alarm responses) at the facilities under OIT control.
- Where the Contractor identifies a potential issue in maintaining an "as provided" State infrastructure element with the more stringent of an agency security policy (which may be Federally mandated or otherwise required by law), identifying to Agencies the nature of the issue, and if possible, potential remedies for consideration by the State agency.

The State shall be responsible for conducting periodic security and privacy audits and generally utilizes members of the OIT Chief Information Security Officer and Privacy teams, the OBM Office of Internal Audit and the Auditor of State, depending on the focus area of an audit. Should an audit issue be discovered the following resolution path shall apply:

- If a security or privacy issue is determined to be pre-existing to this agreement, the State will have responsibility to address or resolve the issue. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor;
- If over the course of delivering services to the State under this Statement of Work for in-scope environments the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams the Contractor is to notify the State within 6 hours. This notification shall not minimize the more stringent Service Level Agreements pertaining to security scans and breaches contained herein, which due to the nature of an active breach shall take precedence over this notification. Dependent on the nature of the issue the State may elect to contract with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor;
- If over the course of the agreement a security or privacy issue arises, whether detected by the State, a State auditor or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of ongoing run services associated with this agreement, the Contractor shall: i) notify the State of the issue or acknowledge receipt of the issue within 24 hours; ii) within 48 hours from the initial detection or communication of the issue from the State, present an potential exposure or issue assessment document to the State Account Representative and the State Chief Information Security Officer with a high level assessment as to resolution actions and a plan; iii) within 4 calendar days, and upon direction from the State, implement to the extent commercially reasonable measures to minimize the State's exposure to security or privacy until such time as the issue is resolved; and iv) upon approval from the State implement a permanent repair to the identified issue at the Contractor's cost; and
- For in-scope environments and services, all new systems implemented or deployed by the Contractor shall comply with State security and privacy policies.

8.9.14 IT Network Connectivity & Monitoring Services

The Contractor must be responsible for Network connectivity and operations. Contractor responsibilities with respect to Network connectivity and operations must include the following:

- Establishing secure channels between the SOCC and agency, within in-scope environment elements only, to deliver managed infrastructure services-- using managed, end-to-end IP Security (IPSec) encrypted VPNs or hardware-based stateful inspection firewalls.
- Maintaining contractual responsibilities for Contractor managed network capabilities.
- Maintaining network failover capabilities in the event of loss of connectivity.
- Providing bandwidth sufficient to perform the environment management services at agreed upon service levels and availability.
- Event management and continuous monitoring of systems based on pre-defined parameters and thresholds and feeding of events into fault management tools.
- Systems monitoring across system components including identifying unauthorized to the network, and reporting outages via the management tool set.
- Event correlation for fault managed devices and mapping of the relationship for multiple identified events.
- Engineering support at agreed levels for addressing, mediating and managing critical hardware and software issues.
- Maintaining and providing network documentation for the Contractor's areas of responsibility and participating with the agency in maintaining overall network documentation.
- Maintaining and supporting network components within the Contractor's areas of responsibility, including:

- a) Supporting network and server software required and provided protocols and security techniques as well as standard data access and transport techniques
 - b) Providing hardware maintenance for environment servers, remote routers, operating system, database, middleware and application software products and ancillary components as required to operate the systems
 - c) Tracking, managing, communicating and supporting resolution of network exceptions.
 - d) Evaluating and testing, in advance, network, hardware, and interface equipment including the configuration and installation of equipment that will be attached to, and will communicate over, the State network.
- Upon the agency review and approval, supporting the provision of connectivity to the Contractor Services and third party agency facilities and systems or other external networks.
 - Developing acceptance procedures for installation and changes to the network, and for verifying restoration of availability following problems with network circuits or equipment.
 - In consultation with an agency, and as set forth in Statements of Work, developing and providing reports on the status of the Network.

8.10 Solution Documentation

- ★ The contractor will be responsible for the initial documentation the solutions developed or modified by the Contractor in accordance with established methods, processes, and procedures such that, at a minimum the State or a competent third party service provider can subsequently provide the same scope of services following a reasonable period of transition services.
- Developing and maintaining, as agreed appropriate, the documentation on in-scope environments. Where it is determined that documentation is inaccurate (for example, due to demonstrated errors or obsolescence), and such inaccuracy may negatively affect the Services, Contractor will correct such Documentation as part of normal day-to-day operational support.
- Updating programmer, end-user and operational reference materials.

8.11 Quality Assurance

- ★ The Contractor will be responsible for developing and documenting quality assurance processes and procedures for the delivery of Services by the Contractor to the State including:
 - Confirming compliance with agreed upon quality assurance procedures.
 - Conducting quality and progress reviews with appropriate agency personnel.
 - Systematically documenting and incorporating preferred experiences from related projects and activities into future work.
 - Reviewing project performance and outcomes relative to documented business and financial goals/expectations as requested by the agency based on mutually agreed business case, project rationale, goals and objectives and/or other relevant measures of success based on the State's overall goals.

8.12 Service Desk Design and Implementation

The State maintains a variety of Service Desk tools that may or may not be applicable to supporting the design, implementation and operation of a contemporary Service Desk. Offerors are to review the software elements provided in this section based on the requirements of the State and their proposed solution.

As the State has a variety of licensing mechanisms in place for these software packages that were contracted by agencies over time, it would be prohibitive to include the commercial details (e.g., licensing schemes, pricing, maintenance agreements and the like) for each, therefore offerors may assume that: (i) the current licensing framework for each is acceptable to the State; (ii) there are no preclusions that the offeror needs to be aware of that would limit the onward use of the software package for statewide use within the SOCC (i.e., the State will resolve these issues with the software vendors independent of the Contractor); (iii) all packages are under current, maintenance and support agreements that are acceptable to the State; (iv) the incremental use of the State-provided software package for Contractor use in the SOCC shall not factor in consideration of the offeror Cost Proposal (i.e., be offeror cost neutral), except for the case where the offeror proposes a software package that is not included on the list below, in which case the Costs of the proposed offeror Solution must be included in the offeror Cost Proposal.

- ★ The Contractor will be responsible for the selection, design and implementation of a Statewide Infrastructure Services service desk including associated functions and processes areas described in this section. Offerors are to note that the State maintains working systems in several large Agencies currently located at the SOCC as follows:

Large SOCC Agency	Implemented Service Desk and Infrastructure Management Platforms / Software
Bureau of Workers Compensation	<ul style="list-style-type: none"> ▪ Remedy ▪ Site-Server ▪ BMC Patrol ▪ BRIO Query Tools ▪ NuMega Suites ▪ CISCO Web Collaboration ▪ MText ▪ AutoCoder ▪ Finalist
Ohio Department of Job and Family Services (ODJFS)	<ul style="list-style-type: none"> ▪ Dimensions – Enterprise Asset & Change Management ▪ Microsoft Operations Manager ▪ NetIQ – Network Monitoring ▪ Remedy Action Request System
Department of Health	<ul style="list-style-type: none"> ▪ Serena, PVCS / Version Manager – software version management
DAS OIT	<ul style="list-style-type: none"> ▪ PeopleSoft CRM (OAKS Level 1 help desk) ▪ HP Openview – Device Monitoring ▪ HP Openview Service Desk – Trouble Ticketing ▪ IBM Tivoli – Unix Systems Management ▪ ITS Help Desk System (Custom help desk software) ▪ Outage Database (Custom database for Unix/Linux outage management) ▪ System Center Configuration Manager (SCCM) – Windows Server Management ▪ System Center Operations Manager (SCOM) – Windows Server Monitoring ▪ WSS Server Database – Custom Application to manage server configurations
Ohio Department of Transportation (TAX)	<ul style="list-style-type: none"> ▪ Tivoli Problem Management TPM – Centralized help desk software

8.12.1 Sizing Considerations: Infrastructure Services Division (ISD) Call Center

A snapshot (January 2012) of Infrastructure help desk incident volumes, types and element areas is provided for sizing purposes only. Statistics may vary seasonally both in number and nature of incidents but are provided to aid offerors in “rough order of magnitude” system selection and sizing considerations.

Customer Service Center Ticket Summary Metrics for January 2012

Call Type	Network	Server	Storage	Security	Other	Total
Incidents Opened	156	11	-	8	225	400
Incidents Closed	157	13	-	11	127	308

Service Requests Opened	638	368	3	-	1,272	2,281
Service Requests Closed	613	360	5	-	1,160	2,138
Portal Live Chat Sessions	-	-	-	-	773	-
<i>Total</i>	<u>1,564</u>	<u>752</u>	<u>8</u>	<u>19</u>	<u>3,557</u>	<u>5,127</u>

Which is based on the following support profile:

Number of Entities (Agencies, Boards, Commissions) with Tickets in January 2012	64
Mainframe Devices	7,000
Network Nodes (routers, switches, etc.)	889
Network Interfaces	25,300
Physical Servers	308
Virtual Servers	594
Storage Devices	23

It is the State's desire to leverage historical investments in service desk software, supporting infrastructure and personnel training investments while providing high levels of service and responsiveness to agency support needs. Therefore, the Contractor, in consideration of best practices in delivering these infrastructure services is to select one of the State's implemented service desk platforms to serve as the standard for the State. The Contractor must perform an analysis inclusive of functionality, technical attributes, relative implementation costs, data and agency data conversions (active cases only and selected historical data to serve as the basis for a knowledge base) and recommend to the State the preferred service desk platform on which to implement these services. In the event that one of the State's platforms is deemed deficient by an offeror, offerors are instructed to provide the rationale for deficiency as well as include software licensing, maintenance and infrastructure costs to implement their recommended solution.

★ The Contractor designed and implemented solution must support:

8.12.2 Problem Management

- Provide a single point of IT contact for supporting agency needs.
- Tracking and managing issues, including by employing procedures for proactive monitoring, logging, tracking, escalation, review, and reporting (historical and predictive) for issues.
- Implementing a process that establishes, to the extent reasonably possible, end-to-end responsibility and ownership of issues in a manner that helps reduce redundant contacts and helps eliminate the need for the users to describe the issue multiple times to different Contractor personnel.
- Categorizing and documenting the relative importance of each issue according to the severity levels as agreed.
- Monitoring and managing each issue, including issues associated with changes, and reporting on the status of resolution efforts until it is corrected or resolved and an agency authorized user confirms such resolution.
- Assisting with the prioritization and maintenance of outstanding work logs.

8.12.3 Additional Services

- To the extent an issue is due to errors or bugs in an in-scope environment, server or in-scope software element licensed by a third party to the State, assist the State by referring such issue to the appropriate third party entity for resolution and coordinating with third party vendors as appropriate to help minimize the State's role in problem management.
- Performing trend analyses at the State's request, and no less frequently on a quarterly basis when not otherwise requested, on the volume and nature of issues in order to identify possible areas for improvement.
- Implementing measures to help avoid unnecessary recurrence of issues, by performing root cause analysis and event correlation.

8.12.4 Service Desk Tools

- Utilizing State owned or Contractor licensed tools, and enhancing processes, to proactively perform problem management, with the objectives of automating the problem management process.
- Granting the agencies access to the problem tracking system via the web from all facilities where the Services are performed and where an agency has access to the Web, and allowing the agency to monitor and view the ticket status on an ongoing basis.

8.13 IT Infrastructure Management Services

The State wishes to analyze trends and initiate a continuous improvement process striving to enhance its operations and identifying continuous improvement ideas while sharing applicable best practices and that may improve the State’s overall IT processes and usage of enabling technologies. Therefore the State wishes to design and implement processes to conducting periodic knowledge exchanges between the Statewide Infrastructure Management team and Statewide Agencies. Specific capabilities to be designed and implemented by the Contractor are as follows:

8.13.1 Capacity Planning

- Review the State’s growth plans during regular service review meetings, and if requested due to an unforeseen requirement, participate in ad-hoc reviews coincident with these new requirements and infrastructure needs to correctly plan for capacity – periodic capacity increases as well as “on-demand” needs as a result of unanticipated business needs.
- Monitor system use/capacity, forecast capacity and review with the State Infrastructure Management on a regular basis

8.13.2 Continuous Improvement

Contractor responsibilities with respect to the continuous improvements with the agreement of the State’s Infrastructure Management must include the following:

- Generate and receive (from agency customers or internal staff) improvement ideas, and agree an annual server consolidation targets to reduce less physical devices for initially transferred services (rebalancing, replacement, planned obsolescence, virtualization, re-hosting, decommissioning)
- Setting of annual and quarterly aggregate processing capability increases without corresponding uplift in fees for services

8.13.3 IT Infrastructure Provisioning

- Contractor responsibilities with respect to the provisioning services must include the following:
 - Physical and Virtual machine provisioning.
 - Internal Data Center Network design, specification, implementation and migration to operations;
 - Perform all associated setup, configuration and maintenance per manufacturer or best practices specifications including standard configuration physical machines, cabinet (rack, Power, UPS), Hardware (CPU/Servers, Disk Arrays, Monitors), Networking Equipment (Switches, Routers, Firewall) and other supporting infrastructure elements.
 - Network device assignment, configuration and security design, implementation and validation of effectiveness in compliance with established State security policies and practices.

8.13.4 Disaster Recovery (DR) and Business Continuity (BC) Support Processes

Based on the current capabilities of the State, the overall complexity of the State’s computing applications and services portfolio, and existing agency provisions for DR/BC, the Contractor’s responsibilities shall in general: i) apply to in-scope environments located in the SOCC; ii) the SOCC itself in consideration of existing capabilities and, following implementation, Contractor improvements to the facility; iii) existing implemented methods to support agency specified DR/BC for agency applications and systems; iv) not apply to middleware, application software, application presentation or any agency supported applications, customizations or extensions and be limited to in-scope environment elements.

Contractor responsibilities with respect to the DR/BC services must include the following:

- Except as otherwise provided, State Agencies will retain sole responsibility for overall business continuity plans, application and network recovery, and recovery process management activities.
- The Contractor must support business continuity plans as they relate to in-scope environment elements (i.e., in-scope infrastructure and facility elements only) as specified by an agency and participate in and support the regular testing and improvement of the business continuity plans.
- To the extent agreed appropriate, support OIT and upon request participate in planning sessions, testing review sessions and other meeting activities between OIT and a participating agency for in-scope environment elements.
- Support implementation of business continuity plans as agreed in Statements of Work between OIT and an agency for in-scope environments as they pertain to the support of the implementation, testing and remediation of agency DR/BC plans for in-scope environment elements;
- Support State activities, processes and procedures for in-scope work and environments to support agency disaster recovery capabilities.
- Support the State's potential future specification, design and implementation of infrastructure disaster recovery plans for in-scope environments and environment elements, but exclusive of middleware, application or presentation software as agreed based upon the following principles:
 - a) Leverage a State provided offsite and geographically diverse alternate disaster recovery site that has sufficient computing and network capabilities which are adequate to process the State's transactions and to provide systems access to end-user personnel during an outage period
 - b) Document requirements and support design reviews to facilitate transfer of operations to disaster site for in-scope environment elements to occur within 48 hours of failure of primary site
 - c) Document procedures to restore primary operations for in-scope environment site operations (once available) within 24 hours
 - d) Identification of redundant processing environment requirements to ensure 24x7 operations for State critical infrastructure components
 - e) Specification of redundant power requirements to ensure 24x7 operations for State critical infrastructure components
 - f) Specification of redundant networking requirements (network devices and telecommunications access) to ensure 24X7 operations for State critical infrastructure components
 - g) Specification of fire detection and suppression requirements to comport with service levels contained elsewhere in this document with regard to systems availability, failover and service levels as agreed for in-scope environment elements.
- Testing
 - Support OIT in establishing joint test objectives with an agency designed to verify that the in-scope environment elements will be available within the agreed upon timeframes contained in an agency business continuity plan as they pertain to in-scope environment elements.
 - Support OIT in scheduling and testing in scope environment elements of the disaster recovery and business continuity plans relating to in-scope environment elements at least annually in support of the agency, its designees, any testing and recovery providers, and relevant State third party Contractors.
 - Continuing to operate and manage the in-scope environment elements during periodic disaster recovery tests
- Communications
 - Notifying impacted Agencies as soon as practicable upon becoming aware of a disaster or outage affecting the contracted Services.
 - Supporting with the State to support an agency disaster recovery and business continuity plan. In such regard, the Contractor will:

- a) Perform necessary migrations of the software code and data as defined in the agency disaster recovery plan to reinstate the in-scope environment elements so that they are functional at a backup location designated by an agency in accordance with the established procedures.
- b) Coordinate with the agency to support the reinstatement of the in-scope Environment(s) at such backup location for in-scope environments.
- c) Maintain provision and ongoing operation of the Services for unaffected areas.
- d) Following any disaster, at the agency's request, the Contractor will support OIT and the agency in the reinstallation any in-scope environment elements affected by such disaster in accordance with the process for such re-installation set forth in an agency disaster recovery plan and business continuity plan.
- e) Following any disaster, conducting a post-disaster meeting with the State for the purpose of developing or enhancing plans to mitigate the adverse impact of future occurrences as they relate to in-scope environment elements.
- f) To the extent applicable to the in scope environment elements, maintain compliance with agency documented disaster recovery policies, standards, and procedures contained in a provided disaster recovery and business continuity plan.
- g) Support an annual test, documented results and feedback procedures contained a the agency provided disaster recovery and business continuity plan for in-scope Infrastructure environment elements.

The Contractor shall not be responsible for, or quote or specify services associated with:

- a) Providing alternate data processing facilities or capabilities to the State inclusive of data centers, networking, redundant or failover equipment and associated software; ands
- b) Develop detailed disaster recovery or business continuity plans for State applications; these plans shall remain the sole responsibility of the State agency that maintains the application.

9.0 Ongoing Facility Technical Management Services

The State desires to contract with a professional data center management company to operate the technical aspects of the SOCC for the State. The selected Contractor will be responsible for the management of all phases of the building technical operations and must provide services to support limited general construction for the building's tenants at the direction of OIT.

9.1 Overview

The SOCC is dedicated to provide continuous uptime for the sophisticated systems and tenants. These systems include computers, battery and generator backup power feeds, dual communication feeds and redundant components in all critical systems, such as air conditioning, electrical distribution, fire protection (standpipe, pre-action sprinkler and halon 1301), UPS systems and a building management system (BMS).

The important priority under this Contract must be the continuous operation and security of the computer and telecommunications equipment installed within the SOCC. Services provided by the various SOCC tenants' computer systems are essential to the support of critical missions to the State of Ohio. The facility must continuously operate 24 hours each day, 365 days a year, without interruption for weekends or holidays. The largest portion of staff is on-site Monday through Friday, 8:00 a.m. to 5:00 p.m. Shift changes vary by tenant, but normally occur at 7:00 a.m., 4:00 p.m. and midnight.

At a minimum the offeror must propose a property technical manager ("Property Technical Manager"), a building engineer ("Building Engineer"), a cabling designer ("Cabling Designer") and two building electricians ("Building Electricians"). The offeror must propose any additional staff required for continuous SOCC operations.

9.2 Document Library

In addition to the contents of this RFP, the State has a library of materials that are related to the Project. The library contains materials that are relevant to the Project but are not practical to include as part of this RFP. The document library contains the documents listed in Part Three of this RFP. Only Qualified Offerors, which may include the proposed subcontractor(s), will have access to the information, which will allow for review of the equipment inventory and equipment history reports during the RFP process.

See Part 3: General Instructions of the RFP for guidance on scheduling appointments to review the contents of the Document Library.

9.3 Work Requirements

The Contractor will be responsible for performing all of the work necessary to design, repair, manage, maintain and provide data center services at the SOCC. All operating expenses associated with the management, maintenance and tenant services including without limitation the Contractor's monthly service fee, on-site salaries, wages, prevailing wages, payroll taxes, benefits, materials, equipment, tools, parts, supplies, subcontractors, preventative and remedial maintenance contracts and insurance must be included in the Contractor's cost summary.

The SOCC must be managed and maintained in accordance with all current industry standards and regulations and those designated in this RFP, including but not limited to the following:

- Contractor must be responsible for managing and maintaining all building systems to the manufacturer's specifications and recommendations.
- The systems/equipment identified in this RFP (regardless of those provided by the State or the Contractor) must be maintained utilizing factory authorized service contracts.
- Contractor must maintain current licenses and permits required by administrative rules, statutes, or other legal authorities.
- Contractor must maintain and update operating manuals and blueprints for the State.

- Contractor must have standard programs for in-house training of Contractor's personnel in safety and environmental issues concerning the work place. Contractor must be responsible for calling such issues to the attention of the SOCC DAS Facilities Manager.
- Contractor will be responsible for scheduling and setting up all conference rooms.
- Contractor must provide a documented thermographic study of all electrical distribution systems once a year through the life of the Contract.
- Contractor must conduct quarterly tenant meetings.
- Contractor must prepare and submit a Standard Operating Procedures (SOP) manual describing the policies and procedures for the Contractor to use in operating the SOCC. This manual must be submitted to the SOCC DAS Facilities Manager for review and approval within 60 calendar days of award of the Contract. Contractor must provide an electronic copy to the SOCC DAS Facilities Manager. Contractor will update and keep the manual current through the life of the Contract.
- Contractor must utilize the existing SOCC Tenant Handbook describing the services available to tenants, the building rules and regulations and a listing of building contacts and telephone numbers.
- Contractor assures throughout the contract term that all tenants have a copy of the SOCC Tenant Handbook. Contractor will update and keep the Handbook current through the life of the Contract.
- Contractor will operate the existing Data Stream response system for acting upon or resolving tenant complaints and requests for service, scheduling and performing equipment preventative maintenance on all building systems.
- The Contractor will prepare and submit for the State's approval, within 30 days of award of the Contract, finalized operating budget based upon the Proposal and will submit subsequent annual operating budgets at times and in formats agreeable to the State.
- The Contractor will provide the State with monthly operating statements showing performance to budget, accompanied by a variance analysis explaining significant variances from budget. These reports are to be received by the State no more than 15 calendar days following the close of each successive month.

9.4 Interior Air Quality Test

Within one hundred and eighty (180) days after the effective date of the Contract, the State's management firm will perform or cause to be performed an interior air quality test. Tests results are to be turned over to the State's SOCC OIT Data Center Manager.

Eighteen (18) sample locations must be selected by the owners to ascertain the quality of interior air. The purpose is to gain an average air quality measurement throughout the facility and to locate any unusual conditions. The testing must consist of recording the following:

- Temperature and humidity
- Carbon dioxide
- Carbon monoxide
- Ozone
- Formaldehyde
- Quantify airborne dust in ug/m3
- Bacteria counts in CFU/m3
- Mold counts in CFU/m3

Any deviations from established standards are to be noted, and recommendations for corrective action and/or further testing should be provided.

9.5 Wiring Maintenance Plan

The SOCC Technical Manager will be responsible for installing, maintaining, inventorying and documenting under floor cabling systems including:

- Design and coordinate installation of data and voice cabling with tenants, contractors, Unified Network Service Provider and OIT Data Center Manager.
- Design and coordinate direct installation of horizontal cable tray throughout facility for new tenant areas not included in capital construction project.
- Maintain up to date inventory of all vertical risers through use of “DOC-IT” inventory software provided by the State of Ohio.
- Maintain voice and data cross connections schedules via “DOC-IT” for main cross-cut equipment and distribution points throughout the facility.
- Responsible for operation of CAD/D system (Contractor supplied and maintained) to build and maintain database of drawings indicating all furniture systems, equipment, electrical circuits and power distribution unit panel schedules.
- Design and coordinate with building engineer the installation of electrical circuits throughout facility, for work performed by in-house electricians.
- Act as liaison between the Unified Network Service Provider and building engineer to determine new cabling requirements for tenant build out and remodel.

9.6 Facility Technical System Maintenance

The Contractor must manage and maintain the systems and services listed below:

- Uninterrupted Power Source (UPS);
- Stand-by Battery Systems;
- Emergency Generator Systems;
- Emergency Power Off (EPO) System;
- Electronic Control Systems;
- Building Mechanical System;
- Building Electrical System;
- Building Plumbing System;
- Water Treatment System;
- Fire Protection System;
- Security and Closed Circuit TV Systems;
- Site Scan System;
- Heating/Ventilation/Air Conditioning (HVAC);
- Elevators;
- Automated Safety Halon system;
- Pop Up Bollard (Crash Barrier) (estimated installation date 09/01/05);
- Lighting System (Interior);
- Lighting System (Exterior);
- Under floor Structured Cabling System; and
- Any other building technical system not listed here.

The Contractor must assure all replacement parts used will be the same kind or equivalent to existing parts and must not violate any manufacturer warranties.

The Contractor will be integrated into a team to coordinate and discuss day-to-day issues related to property management, security and janitorial services. This team will meet as required to provide information exchange between the contractors and to provide a brief status of current issues. The current contract for security is with Goodwill Rehabilitation Center (GRC). The current contract for vending is currently with Sanese Services. The current contract for janitorial services is with OIH, Inc.

The Contractor must maintain and supply to the State all records as required by Chapter 4115 of the Ohio Revised Code, the Prevailing Wage Law, for both the Contractor and its subcontractors.

9.7 Excluded Services

The Contractor will **not** be responsible for managing and maintaining the systems and services listed below:

- Window Cleaning (Interior);
- Window Cleaning (Exterior);
- Pest and Rodent Control (Interior);
- Pest and Rodent Control (Exterior);
- Snow and Ice Removal;
- Refuse Removal;
- Painting (Interior);
- Painting (Exterior);
- Landscaping (Interior);
- Landscaping (Exterior) including ground maintenance;
- Irrigation System;
- Seasonal Planting;
- Parking Lot Resealing and Striping; and
- Guard Shacks (2).

9.8 HVAC Operation and Maintenance

HVAC operations and maintenance must include all in-house and contract personnel that operate and maintain the central HVAC plant and associated equipment, chillers, ice tanks, cooling tower, various pumps and motors, boilers, Leibert units, air handlers and central systems.

- The Contractor will utilize the current Data Stream preventive maintenance system for the property's equipment and systems. This system is capable of scheduling preventative maintenance work and tracking work progress. The system can generate status reports that can be used for the State's reports as well as in-house job control. The preventive maintenance program must be capable of maintaining complete record histories on all included equipment. The schedules tasks must meet manufacturer's recommendations and/or industry standards.
- Contractor must have predictive maintenance functions included in the preventive maintenance program. These functions must include but not limited to oil, vibration, corrosion, and electrical analysis. Trend logs must be recorded for each of these functions.
- Contractor must maintain comprehensive daily operating logs for the facility.
- The Contractor must ensure that all property library and drawing files are kept current and secure. Contractor will obtain or create all required documentation of building equipment and systems installation. Library files must include a complete building mechanical equipment inventory and sequence of operations.
- The Contractor must provide a method of energy accounting of the building's utility expenses. This system must be capable of providing energy use and variance reports. The Contractor must use this information to make appropriate utilities conservation recommendations to the State for both management and occupant participation.
- The Contractor must maintain the mechanical equipment and surrounding areas in clean condition with their own in-house staff. The Contractor must ensure that mechanical equipment rooms are painted in a manner acceptable to the State.
- The Contractor must provide oversight of the subcontractor's work in building or space renovation services as requested by the State within the capability of the in-house workforce and oversee the efforts of such subcontractors as may be employed in this respect by agreement with the State.

9.9 Limited General Construction

Contractor must be responsible for providing engineering design, obtaining competitive estimates and contracting for limited construction services as required for tenants. The Contractor must seek at least three (3) bids when contracting any work and for the purchase of all commodities and services. The State reserves the right to participate in the evaluation of such bids.

The Contractor must be responsible for ensuring that all required permits and inspections are obtained and that "as built" drawings are provided to the State. The Contractor must require any company providing limited general construction services to provide a performance bond in the full amount of the contract for the benefit of the State, to pay the applicable prevailing wage rates and to submit certified payroll reports.

Limited general construction services must not exceed \$750,000 per Contract year and must be approved in writing by the SOCC OIT Data Center Manager. Such services will primarily include:

- Procurement and oversight of the engineering design;
- Plumbing and maintenance;
- Wall construction; and
- Electrical work.

These services must be billed to the SOCC tenant requiring the services. The Contractor will begin work only upon receipt of a purchase order. The Contractor and subcontractors must pay prevailing wage as applicable to such work.

9.10 Staffing Requirements

At a minimum the Offeror must propose a Technical Manager, a Building Engineer, a Registered Communications Cabling Designer and a Building Electrician. The Offeror must propose any additional staff required for continuous SOCC operations. The Contractor must notify the State of vacations and other absences for key personnel. At its option, the State may require the Contractor to provide comparable replacement personnel during vacations and other absences.

- Contractor must provide a fully trained and qualified Property Manager who must be on-site at the SOCC during regular business hours (8:00 a.m. – 5:00 p.m. Monday through Friday, excluding State holidays). The Property Manager must remain on-call 24 hours a day, 365 days a year. Employees of Contractor will observe the holiday schedule published annually for State employees while maintaining uninterrupted performance of services.
- The Technical Manager must be responsible for the day-to-day management of the technical aspects of the building that directly support continuous Data Center Operations in accordance with the operating principles and procedures that have been reviewed and approved by the State. The Technical Manager must immediately inform the SOCC OIT Data Center Manager of any significant problem or decision that would affect tenant security, safety and service and must follow all emergency escalation of evacuation procedures.
- The Building Engineer must be responsible for the day-to-day operations of the building in accordance with operating principles and procedures that have been reviewed and approved by the State. The building Engineer must immediately inform the Contractor Technical Manager of any significant problem or decision that would affect tenant security, safety and service and must follow all emergency escalation procedures.
- The Contractor must provide two (2) Building Electricians, for a minimum of 40 man hours per week each, to do base building and tenant electrical work. All electricians must be certified by the state of Ohio as an electrical journey person. If the Contractor determines that electrical work requires staff beyond the full time electricians, the Contractor must furnish the State with documentation to support the use of outside electrical services.

9.10.1 Technical Manager (on-site):

The Technical Manager will be in charge of the delivery and management of technical services for the duration of the Contract. The offeror must propose a candidate that can perform the responsibilities specified below:

- Support of mission critical or business critical data center operations;
- Property management a Tier II or greater data center of 85,000 square feet or larger;
- Supervising the implementation and control of preventative maintenance systems, life safety and environment management systems and building energy management in support of a Tier II or greater Data Center;
- Recommend, approve and oversee data center capital improvements in excess of \$5,000, as well as completing life-cycle cost analysis or feasibility studies of these improvements as appropriate;
- Handling of day-to-day operations of a Tier II or greater data center, including control or supervision of technical staff, job assignment, contract administration and inspection; and
- Capable of contracting and supervising Tier II data center improvement work; and
- Experience handling or coordinating outside or in-house consulting services of architects, engineers and other professionals on technical issues.

9.10.2 Building Engineer

The Building Engineer will be in charge of the building operations for the duration of the Contract. The Offeror must propose a candidate that can perform the responsibilities specified below:

- Operation of a Tier II or greater data center supporting mission critical or business critical operations;
- Performing routine building operations functions for a multiple floor data center of 85,000 square feet or larger.
- Supervise the implementation and associated controls for facility preventative maintenance systems, life safety and environmental management systems and energy management systems for a multiple floor data center;
- Needs identification and recommendation of capital improvements in excess of \$5,000, as well as completing life cycle cost analysis or feasibility studies of these improvements as appropriate;
- Handle day-to-day operations of a Tier II or greater data center, including control or supervision of building maintenance staff, job assignment, contract administration and inspection;
- Management and oversight of base building and tenant improvement work; and
- Management and coordination of outside or in-house consulting services of architects, engineers and other professionals on technical and construction issues.

9.10.3 Registered Communications and Cabling Designer

The building Cabling Designer will be in charge of all communications and data service delivery infrastructure, the cabling itself. The offeror must propose a candidate that is capable of providing the following work requirements:

- Design and coordinate installation of data and voice cabling with tenants, contractors, and telecommunications/networking providers and the OIT SOCC Data Center Manager.
- Design and coordinate direct installation of horizontal cable trays or similar throughout facility for tenant areas not included in capital construction projects.
- Maintain up to date inventory of all vertical risers through use of inventory software provided by the State of Ohio.
- Maintain voice and data cross connections schedules via for main cross-cut equipment and distribution points throughout the facility.
- Responsible for operation of CAD/D system (Contractor supplied and maintained) to build and maintain database of drawings indicating all furniture systems, equipment, electrical circuits and power distribution unit panel schedules.
- Design and coordinate with building engineer the installation of electrical circuits throughout facility, for work performed by in-house electricians.
- Act as liaison between a telecommunications/network service provider and building engineer(s) to determine new cabling requirements for tenant build out and remodel.
- Assist in the development of SOCC communications and data disaster recovery.

9.10.4 Building Electricians

The Building Electricians will be in charge of all electrical work for the duration of the Contract. The offeror must propose candidates that are State of Ohio certified electrical journey persons that are capable of performing the minimum responsibilities specified below:

- Perform electrical work in buildings supporting mission critical or business critical operations, 365 days per year, 7 days per week and 24 hours per day; and
- Perform electrical work in a multiple floor building 85,000 square feet or larger.

9.11 Drug Testing

The Contractor must submit results from an alcohol and drug abuse test for every employee, including subcontractor personnel, prior to that individual's access to the SOCC. The Contractor will also be expected to perform random testing for the duration of the Contract. The State may request additional testing at any time for reasonable suspicion. All testing must be performed at the expense of the Contractor.

9.12 Exclusions

The Contractor is not responsible for the following in State-occupied space:

- Negotiating and executing the janitorial contract and purchasing related janitorial supplies.
- Negotiating and executing the food service contract and purchasing related food service supplies.
- Negotiating and executing the security contract and purchasing related security supplies.
- Payment of utility bills.
- Payment of diesel fuel bills.
- Capital expenditures as required by the State.
- Major equipment or system repairs exceeding \$5,000.00 for any State-owned asset.

9.13 Transition Period

The Contractor will be required to bring in their transition team 30 calendar days prior to the effective date of this portion of the Contract (targeted no later than July 1, 2013). At a minimum, the Contractor transition team will include the Technical Manager, Building Manager, Registered Communications and Cabling Designer and Building Electricians. The Contractor transition team must be on site and must work with the State and the existing Contractor to transition all responsibilities for each of the three shifts. In addition the Contractor will be responsible for verifying the existing supply inventory during this period. The Contractor must provide a transition report no later than six (6) weeks of the effective date of the Contract. The transition report must include an overall assessment of the building, systems, responsibilities and identified issues.

9.14 Building Operation Plan

The Contractor must employ effective techniques, strategies and approaches for maintaining and operating the building.

The offeror must provide Building Operation Plan that includes the techniques, strategies and approaches for maintaining and operating the building and a complete detailed description of their proposed staffing levels for each of the three (3) shifts. The plan must clearly indicate the tasks and services that will normally be performed on each shift.

The offeror must also address potential problem areas, recommended solutions to the problem areas, and any assumptions used in developing the Building Operation Plan.

The offeror must provide a detailed description of any computer systems or applications that will be used on a day-to-day basis for managing, tracking and reporting any SOCC property issues. This description must also include a discussion of the tracking systems proposed to track and manage tenant work.

9.15 Systems Maintenance Plan

Within 30 days of the initial baselined Project Plan the Contractor must submit a detailed plan for warranty and non-warranty maintenance on all equipment and systems located at the SOCC and included in the specifications of this RFP. This plan must also indicate the response time for remedial maintenance of vital systems to ensure continuous operation of computer systems running in the building. This plan must also address the 24-hour per day emergency services included in the Proposal. Telephone support and maintenance escalation procedures must also be described in this section.

The Systems Maintenance Plan must contain a detailed description of the proposed maintenance for each system contained in the table found below. This section must include the frequency of preventative maintenance proposed. The Contractor must provide a table in their plan that provides the following requested information.

System Maintenance	Name of Responsible Party (Indicate the name of the Contractor, subcontractor or 3rd party responsible for maintenance)	Description of frequency and type of scheduled preventative maintenance to be performed
Uninterrupted Power Systems (UPS)		
Stand-by Battery Systems		
Emergency Generator Systems		
Emergency Power Off (EPO) System		
Electronic Control Systems		
Building Mechanical System		
Building Electrical System		
Building Plumbing System		
Water Treatment System		
Fire Protection System		
Security and Closed Circuit TV Systems		
Site Scan System		
Heating/Ventilation/Air Conditioning (HVAC)		
Elevators		
Automated Safety Halon System		
Lighting System (Interior)		
Lighting System (Exterior)		
Under floor Structured Cabling System		
Any other building system not listed here		

9.16 Property Management Approach

The Contractor must employ effective techniques, strategies and approaches to ensure continuous uptime, effective budgeting and cost control, which are vital to successfully delivering property management services.

The evaluation committee is particularly interested in the offeror's approach to the property management services at this facility. A brief description of the offeror's approach to property management and, in particular, the methods to be utilized for this project must be provided.

Continuous uptime, effective budgeting and cost control are vital to the success of delivery of these services to the State. A brief description of the offeror's ability and experience in these areas and any consultants or additional resources that the offeror intends to engage in these areas must be provided.

9.17 Tenant Complaint Resolution Plan

Within 90 days of the effective date of Contract award, the Contractor must implement an effective response system for acting upon and resolving tenant complaints. This system must be automated and clearly indicate who is responsible for ensuring that tenant complaints are resolved quickly and effectively.

The offeror must submit a detailed plan for operating an effective response system for acting upon and resolving tenant complaints. This plan must be automated and clearly indicate who is responsible for ensuring that tenant complaints are resolved quickly and effectively.

9.18 Quarterly Tenant Meetings

The contractor awarded this Contract will be responsible for conducting a quarterly tenant meeting. The Contractor will schedule the quarterly meetings in July, November, February and May of each year of the life of the Contract. These meetings can only be cancelled and/or rescheduled with the State's approval. The Contractor, in a timely manner, must track and address all questions and issues raised during the quarterly tenant meetings and communicate the solutions to all questions and issues to the State.

The offeror must provide a detailed description of the proposed format of the tenant meeting. The offeror must provide a description of how questions and issues raised during the tenant meeting will be tracked and addressed in a timely manner. The offeror must also describe how the solution to outstanding issues or answers to outstanding questions will be communicated to the State.

9.19 Site Disaster Recovery Plan

The Contractor must develop a Site Disaster Recovery Plan for the SOCC and the tenants. The Contractor will be required to customize a Site Disaster Recovery Plan within 90 calendar days after award of the Contract. This plan is subject to approval by the State. The Contractor must revise their Site Disaster Recovery Plan annually for the life of the Contract. Each revision will be subject to approval by the State.

The offeror must provide an outline of their basic Site Disaster Recovery Plan with the Proposal.

9.20 Transition Plan

The Contractor must develop a Transition Plan for assuming total responsibility of the SOCC property management. The Contractor awarded this Contract will be required to provide a transition report within 14 calendar days of the effective date of the Contract.

The offeror must provide a proposed transition plan in this section of their proposal. The transition plan must include in their proposal a basic outline of the topics to be included on the transition report.

9.21 Support Requirements

The Contractor will maintain a professional office environment, including office equipment and furniture. The Contractor is required to utilize the State's current e-mail system (Microsoft Exchange) for communication. The State currently provides six (6) digital phones, four (4) personal computers (PCs), two (2) printers, network connections and five (5) password sign-ons. The Contractor is responsible for all telecommunication charges and any additional equipment or furniture required to maintain the Contractor's office space.

10.0 Work Area 4: SOCC and Service Governance Implementation

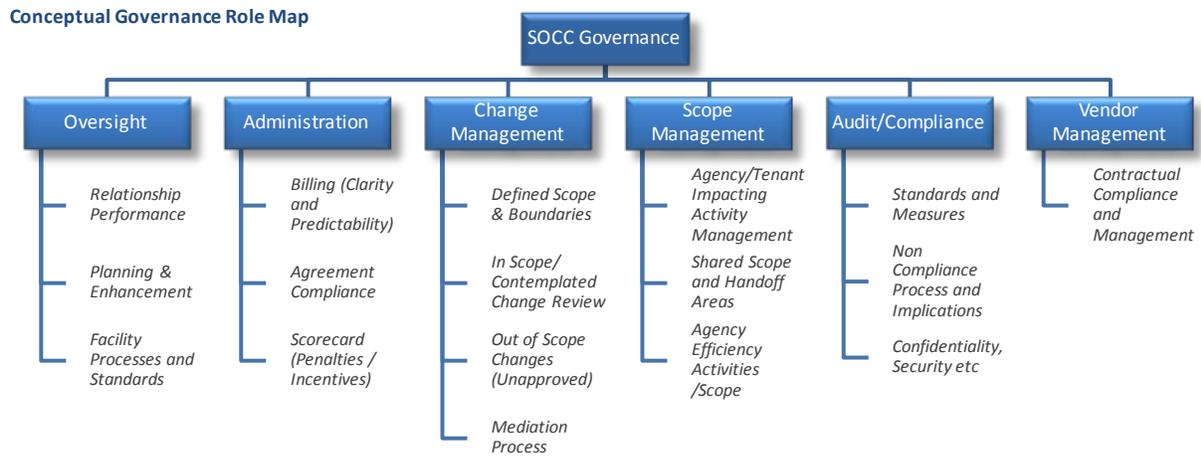
Historically, the SOCC has been managed as a facility through two divisions of the Department of Administrative Services (DAS): The Office of Information Technology (OIT) and the General Services Division (GSD). At a high level, current agency tenants of the facility work with both GSD and OIT to coordinate access, location, building services, IT services, physical security, technical and telecommunications, mainframe and other services. A “rent and chargeback” type model has historically been employed that factors space and utility (power) usage, work requests, special projects and the like. Both GSD and OIT offer services in response to agency requests through a variety of methods including State employees, contracted on-site services, 3rd party maintenance services and usage of a variety of contractors (e.g., electrical, plumbing, wiring etc.) to fulfill these requests.

In general, the current operating model for the SOCC is as follows:

Entity	Current High Level Responsibilities Pertinent to the SOCC
DAS (as a whole)	<ul style="list-style-type: none"> ▪ Ensure that centralized services are aligned with the State’s Technology strategy and that facility, technology and Agency/Tenant requirements are harmonized
OIT	<ul style="list-style-type: none"> ▪ Enterprise Infrastructure & Services Strategy & Architecture ▪ Standard Product and Services Definition ▪ Functional team management & co-ordination ▪ Central Financial Management (Aligned with OBM for budget/forecast, actual, product pricing) ▪ Procurement management liaison (standard frameworks/contracts, preferred contractors)
GSD	<ul style="list-style-type: none"> ▪ Facilities Management ▪ Facility Vendor Management ▪ Facility Performance Management ▪ Verification of Facilities Management contractual obligations and commitments
ISD (a section of OIT)	<ul style="list-style-type: none"> ▪ Standard Configuration, Implementation and Operation of Technical Solutions (defined products and central shared services) ▪ Architecture and Solution design ▪ Standards, Policies, Guidelines ▪ Operational Infrastructure (Process, Procedure & Tools) ▪ Major Problem Management ▪ Release & Upgrade Control and Management
Agency / Tenants	<ul style="list-style-type: none"> ▪ Day to Day Service Delivery of Agency Services ▪ Procurement of hardware, software & services ▪ I/M/A/C, Service introduction of Approved Services and Products ▪ Participation in Standards and Policy Development Activities ▪ Agency Cost & Budget Management ▪ Computing Environment Performance Management ▪ Application and User Interaction layers of IT Solutions

As the State moves to centralize the design, provision, operation and maintenance of core IT Infrastructure services using the SOCC as the central consolidation point, it is important that a clear governance model be identified and implemented to best leverage the State’s investment in the SOCC, maximize the return on this project, and work to ensure that ongoing stewardship of the facility is maintained and that the SOCC be contemporary with current and future IT operating models for the State.

Conceptually, the activities pertaining to the implementation of governance for the SOCC can be viewed as follows:



In consideration of the facility improvements (work area 1), computing infrastructure consolidation (work area 2) and enhancements to operating processes (work area 3), Governance is an essential mechanism that is designed to allow the State to best manage the facility and the services offered from the facility to Statewide Agencies.

The key goals and objectives of the State’s implementation of governance for IT Infrastructure services (and the SOCC) include:

SOCC Governance High Level Objectives

- Measurably improve the efficiency and effectiveness of IT Infrastructure Service Delivery
- Better align the SOCC (and other central data processing facilities) with agency needs
- Provide transparency: clear commitments, clear costs, clear results
- Resolve issues and make decisions impacting Agency/Tenant Service Delivery

SOCC Governance Goals

- Increased Capacity, Technology Improvement
- Increased protection of State data and critical systems
- Minimizing on boarding disruption(s), timing and cost
- Phased reengineering (virtualization, opportunity farming and migration to next generation services)
- Continuous Improvement that leverage fact based models
- Increased visibility to Agency/Tenant needs

10.1 Scope of Governance to be Implemented

In general, the scope of governance must pertain to three primary parties involved in the use of the SOCC:

1. A State Agency or Tenant of the Facility (currently 15 Agencies outside of OIT)
2. The Office of Information Technology (part of DAS)
3. The General Services Division (part of DAS)

The specific scope of services to be considered to be part of the Governance process is:

Area	High Level Description	Governance Role / Ownership
Financial Management	<ul style="list-style-type: none"> Ensure the overall “profitability”, costs, rates and other financial impacts of services offerings are in line with expectations 	DAS/OIT
Customer Management	<ul style="list-style-type: none"> Design service offerings meet or exceed customer requirements and are updated based on future needs 	OIT/LMC/MAC
Service Management	<ul style="list-style-type: none"> Drive the scope of work and service levels of the Data Center to align with customer requirements 	OIT/ISD
Applications Management	<ul style="list-style-type: none"> Manage full IT lifecycle (design, build, run, maintain) for certain applications 	Agency Retained
Operations Management	<ul style="list-style-type: none"> Manage the overall availability and reliability of scheduled operations and routine/scheduled functions 	Agency (App) OIT (Infrastructure)
Server & Storage Management	<ul style="list-style-type: none"> Provide the underlying computing and storage infrastructure for client, server and storage based infrastructure assets 	OIT & Contractor
Infrastructure Management	<ul style="list-style-type: none"> Provide the underlying networking, connectivity, power distribution and security functions for the Data Center 	OIT & Contractor
Facilities Management	<ul style="list-style-type: none"> Provide the physical facility and facility-specific considerations including power, cooling & physical security 	OIT & Contractor

10.2 Implementing Roles & Responsibilities for SOCC Services

The Contractor must review the current operating model at the SOCC and, using a combination of industry best practices, Contractor experiences and standard industry models that are compatible with ITIL/CoBiT, design and propose a Governance model for the State’s use of the SOCC and provision of centrally offered IT Infrastructure Services from the SOCC.

Specific contractor activities and deliverables in this area will include (at a minimum):

- ✧ Creation of a critical services inventory that span “from the basement of the facility” to “the operating system prompt” and include:
 - Physical Plant
 - Internal Facility Operations
 - Physical Facility Security
 - Administrative Personnel Access
 - On-Boarding of New Projects or Equipment
 - Design, Layout and Provisioning of New Projects or Equipment
 - Moves, Adds, Changes and Deletes of Existing Equipment or Devices
 - Off-boarding of agency/tenants or agency/tenant Equipment
 - Building Monitoring, Administration and Billing
 - All ITIL/CoBiT Processes Implemented in Work Area 2 pertinent to building wide operations and planning functions
 - Policy Enforcement and Compliance
 - Other identified areas as mutually agreed
- ✧ For the above critical services inventory, identify the best State provider of these services and determine the relevant operating, decision making and Executive escalation personnel within the State.
- As part of this assessment develop methods to implement these services in a manner as to maximize responsibility, empowerment and agility (as a service to agency / tenants) and minimize disputes, gaps in

accountability or create “loopholes” that allow activities to occur in an unstructured or less than optimally executed manner.

10.3 Establishment of Service Management Oversight Committee

The Contractor will work with the State to establish a Service Management Oversight Committee, made up of a number of key representatives and executives from each participating agency (e.g., OIT, GSD, agency Tenants and potentially other State Agency CIOs), which will meet at a minimum on a quarterly basis, and at such time as its members or the Parties deem appropriate to:

- Review and analyze the monthly performance reports for the preceding period, including any actual or anticipated budget or schedule overruns, service level attainment of targets, any issues or outages that result in the creation of a service credit and the Parties’ overall performance under the scope of services;
- Review progress projects and on the resolution of issues;
- Provide a strategic outlook for the State requirements;
- Review any planned change orders or statements of work outside of the scope of the deployed services; and
- Attempt to resolve, or designate individuals to attempt to resolve, any disputes or disagreements arising within the scope of IT Infrastructure Services provision and consolidation activities.

Additionally, and pertinent to longer-term planning, the Management Oversight Committee may elect to address business requirements, technology alignment, Contract performance, Performance Standards, continuous improvement, service performance and cost benchmarking, quality assurance and escalated issues and disputes.

10.4 Creation of a Dispute Resolution Capability

The parties will make efforts to first resolve internally any dispute, by escalating it to higher levels of management. If the disputed matter has not been resolved by the identified responsible party (or organization) as defined in section 8.2, the disputed matter will be reviewed by the Service Management Oversight Committee within a commercially reasonable period of the delivery of a written notice by one Party to another.

10.5 Other Governance Processes to be implemented

10.5.1 Remediation Project Communications and Oversight

- Oversee the SOCC remediation progress that will implement recommendations to better align the facility to the State’s strategic technologies and standards.
- Collaborate with existing State Agencies to implement and refine as appropriate.

10.5.2 Change and Scope Management/Audit Compliance

- End to end process management for areas that affect all Agencies/Tenants.
- Work to ensure consistency with standard architectures and processes.

10.5.3 Efficiency Oversight and Optimization

- Defining specific Scope of Services for the facility that include service level agreements based on established operating, cost and efficiency standards that reward efficiency and dis-incent waste.
- Review of agency/tenant consumption profiles for space, power and cooling in consideration of system’s needs (critical, essential, deferrable and utility) in light of near and longer term agency/tenant roadmaps and Facility profile

10.5.4 Administration

- Consideration and review of an objective set of standards and targets for the measurement of space, power and cooling consumption in light of State facility goals and actual cost recovery that provide transparency: clear commitments, clear costs, clear results.

- Ensure facility maintenance and operations contracts meet expectations and are regularly reviewed for compliance and cost-effectiveness.
- Oversee and manage building construction activities including changes to space, power and cooling distribution and other changes to the physical plant.

10.5.5 Audit and Enforcement

- Review agency/tenant usage for overall compliance with established standards as well as regular review of operational considerations including cost, service levels, efficiency and consumption and adherence to policies and standards.

10.5.6 Policy and Standards

- Development of pragmatic standards for the facility that incorporate ongoing increases to rack, device, power and cooling densities.
- Drive standards to better align with industry norms while reducing the overall cost and increasing the efficiency of the facility.
- Liaise with agency/tenants to ensure that ongoing requirements and needs are understood and incorporated into OIT products and services.

11.0 Service Levels and Standards

The State wishes to design, deploy and operate IT infrastructure services in a manner that is consistent with contemporary standards in the commercial marketplace. As IT Infrastructure services are the fundamental building block for the support of applications and solutions that support the operation of the State and the State's services to constituents in the State of Ohio, it is critical that IT Infrastructure Services are delivered in a fashion as to:

- Have high degrees of reliability, availability, redundancy and performance;
- Be designed, provisioned and deployed in an agile manner that is flexible to accommodate changing business needs;
- Be delivered, from an agency perspective, as a seamless and predictable fashion as an enabler to projects, applications and services;
- Be a clear step up in service quality from those services that an agency could otherwise provide for themselves;
- Be delivered at a cost point that is commercially viable (aligned with market norms), attractive (a fraction of current infrastructure operating costs), future facing (an enabler of new computing models and a foundation for consolidation) and flexible (an enabler as opposed to an impediment for business opportunities).

Therefore a comprehensive set of service level targets have been selected to deliver these IT Infrastructure services and serve as design targets for: 1) the implementation of improvements to the SOCC (work area 1); consolidation of IT infrastructure Statewide (work area 2) implementation of contemporary Infrastructure Management processes, practices and tools (work area 3).

Following the completion of work areas 1-3 and coincident with the migration to Steady State Operations as provided by the Contractor as a Managed Service to the State, the following Service Levels must be in effect and be pertinent to the Managed Services portion of this agreement.

11.1 Service Levels as a Result of "Co-Managed" Services

The State requires a Steady State Run operation that is comprised of a combination of Contractor and State resources as described in the Managed Services and Technical Facilities Management sections (8 and 9) of this RFP. Resolving the degree, nature and accountability of a service level failure as a result of this Co-Managed service will adhere to the following conventions:

- For items that cause a Service Level to be in less than a green (as specified) state, a root cause analysis will be developed following closure of an incident by the Contractor and presented at the end of a calendar month, usually co-incident with Contractor invoicing processes, to the State for discussion. The root cause analysis shall reference the then current Operating Procedures or Process Interface Manual to aid the State and Contractor in determining the contracted responsibility pertaining to the incident.
- For purposes of reporting and resolution between the State and the Contractor, an Incident as recorded in the incident management system of record shall be the lowest level of granularity in assessing a Service Level failure. In the absence of a presented root-cause analysis report to the State, the default presumption of the State shall be that the Contractor is at fault for the Service Level failure.

Therefore the State and Contractor will work under the following Determination of Service Level Fault framework to clarify to the extent possible, and in consideration of the facts of a root cause analysis associated with an incident.

11.1.1 Determination of Service Level Fault

The following items shall be considered **Contractor Fault** with respect to Service Level failures and shall apply to Performance Credits and Overall Contract Performance considerations discussed later in this section:

- Failures that are exclusively in the Contractor responsibility area, or that are exclusively staffed or performed by Contractor provided personnel;

- Failures where Managed Services personnel (Contractor or State) are following established Contractor processes where as a result of issues, defects, omissions or inconsistencies in these designed and provided processes are shown to be the primary source of the failure;
- Failures where Managed Services personnel (Contractor or State) are not provided processes that are required by this RFP for the Contractor to design, develop, implement or document;
- Failures where Contractor provided Managed Services personnel has an exclusive role or responsibility and is not dependent on State resources to complete the tasks associated with the failure;
- Failures arising where Managed Services personnel (Contractor or State) are following the direction of a Contractor resource where that direction is inconsistent with established policies and procedures;
- Failures arising where a State resource is performing a role, responsibility or task that is outside of the established State's responsibility but within the Contractor's responsibility area on an adhoc or temporary basis in lieu of a Contractor resource at the request of the Contractor;
- Any failure arising as a result of Managed Services personnel (Contractor or State) not following established State Security, Privacy or IT Policies, excepting those incidents that arise as a result of a State system being non-compliant with these Policies prior to the Steady State Run in-service date; and
- Any failure resulting from a sub-contractor or small-dollar contractor working for, or at the direction of the Contractor; and
- Failures arising from Contractor owned equipment or computing devices coincident with providing the in-scope services.

The following items **not be considered Contractor Fault** with respect to Service level failures and therefore not apply to any Contractor Performance Credits or Overall Contract Performance considerations discussed later in this section:

- Failures outside of the scope of the Contractor responsibilities or failure of an out-of-scope State element that directly impacts an in-scope State or Contractor element;
- Failures arising from State provided equipment that is not under warranty or otherwise covered by a maintenance agreement with a 3rd party such as the OEM or a reseller;
- A pre-existing or undocumented deficiency in a State provided computing element as they pertain to adhering to State Policies and Standards. In this case, upon identification the Contractor is to promptly identify the State of the identified deficiency following the procedure described in Section 8.9.13 of this RFP.
- A deficiency in the skill, experience level or certification of a State provided resource that directly causes the Failure as a result of the resources deficiency;
- Failure of a State resource to follow and comply with Contractor provided processes and procedures except where: (i) State Policies and Contractor policies are in conflict in which case the State resource shall follow State Policies and notify the Contractor of the conflict or; (ii) in cases of emergency that would place the State resource at physical peril or harm;
- Failure of a State provided third party warranty or maintenance agreement to deliver Services to the Contractor for in-scope services and infrastructure elements within the required or contracted third party service repair/resolution/replacement times;
- The period of time associated with an Incident where a State contracted third party service, repair or replacement service renders an in-scope infrastructure element unusable by the Contractor to provide the Contracted Services shall be reduced from the overall duration timing of an incident.

In the cases where a State resource is not performing to the level as required to support the Work at levels required by the Service Level Agreements, the Contractor is to notify the State of the Contractor perceived deficiency and allow the State (at the State's discretion) to remedy the situation via change in personnel, training or other development activities. Until such time as the resource can comply with the established roles and responsibilities the Contractor shall be exempt from fault pertaining to similar failures originating from the identified resource;

11.1.2 Other SLA Principles Pertinent to Determination of Fault and Credits

It is the State’s goal to provide a contemporary managed infrastructure service from a delivery, availability and cost perspective to Statewide Agencies. Additionally, for the State to derive value from the Contracted Services as a result of its relationship with the Contractor, these Service Levels are important to the State to effectively deliver these services.

However, it is not the goal of the State to create a Service Level environment that is overly complex or burdensome for the State or Contractor to administer with respect to determining fault as this relates to a particular incident.

The State and Contractor shall review service levels based on their importance to the State (e.g., driving business value, reducing costs, increasing efficiency) and real cost to the Contractor and in the case of Service violations, the goal of the State is to promptly address an issue and revise or enhance procedures to minimize the probability recurrence of the issue.

To drive a cost effective and equitable resolution to those issues that, after consideration by the State and Contractor of the facts contained in the root cause analysis, and based on a nominal total value not to exceed two percent (2%) of the Contractor’s monthly fees, shall be split evenly between the State and the Contractor under the spirit of partnership and moving beyond the dispute as expeditiously as possible and restoring the performance to a compliant level without undue commercial cost or debate. By example:

Contractor Monthly Managed Service Fees:	\$290,000
Maximum Monthly Fees at Risk %:	12%
Maximum Monthly Fees at Risk:	\$34,800
Assuming three SLAs in “red” State	
Comprising of:	
Contractor at Fault Items	\$4,930 service credit to State
Contractor not at Fault Items	\$0 service credit to State
Items where a clear determination of Fault cannot be mutually made or items remaining in joint dispute following review by the State and Contractor:	Not to exceed 2% of \$290,000: \$5,800 Maximum monthly credit to State of \$2,900 or one half (½) of the disputed Fault amount, whichever is lower.

Items that remain disputed in consideration of SLA Faults following this process or as a result of the frequency, repetition or other factors shall be addressed via Informal and formal dispute resolution processes described elsewhere in this RFP.

11.2 Service Level Framework

This section sets forth the functional and technical specifications for the Service Level Agreements (SLA) and Service Level Objectives (SLO) to be established between Contractor and the State. This section contains the tables and descriptions that provide the State framework and expectations relating to service level commitments, and the implications of meeting versus failing to meet the requirements and objectives, as applicable. This document defines the State detailed performance, management, and reporting requirements for all Contractor Service Delivery Center Services.

Both the State and Contractor recognize and agree that new categories of Service Levels and Performance Specifications may be added during the term of the Contract as business, organizational objectives and technological changes permit and require.

The method set out herein will be implemented to manage Contractor’s performance against each Service Level, in order to monitor the overall performance of Contractor.

Contractor will be required to comply with the following performance management and reporting mechanisms for all Services within the scope of Managed Services SOW, Section 8, procured by the State:

- **Service Level Specific Performance** – Agreed upon specific Service Level Agreements to measure the performance of specific Services or Service Elements. The individual Service Level Agreements are linked to Performance Credits to incent Contractor performance
- **Overall Contract Performance** – An overall performance score of Contractor across all Service Levels (i.e., SLA and SLO). The overall performance score is linked to governance and escalation processes as needed to initiate corrective actions and remedial processes

11.3 Service Level Specific Performance Credits

Each Service Level (SL) will be measured using a “Green-Yellow-Red” (GYR) traffic light mechanism (the “Individual SL GYR State”), with “Green” representing the highest level of performance and “Red” representing the lowest level of performance. A financial credit will be due to the State (a “Performance Credit”) in the event a specific Individual SLA GYR State falls in the “Yellow” or “Red” State. The amount of the Performance Credit for each SLA will be based on the Individual SLA GYR State. Further, the amounts of the Performance Credits will, in certain cases, increase where they are imposed in consecutive months. No Service Level Performance Credit will be payable for Contractor’s failure to meet a Service Level Objective.

Set forth below is a table summarizing the monthly Performance Credits for each SLA. All amounts set forth below that are contained in a row pertaining to the “Yellow” or “Red” GYR State, represent Performance Credit amounts. Except as explicitly stated in the Consecutive Months Credit table below, where a larger percentage may be at risk, Contractor agrees that in each month of the Agreement, up to 12% of the monthly recurring charges (MRC) associated with the Managed Services portion of this RFP (“Fees at Risk”). The Fees at Risk will pertain to failure to meet the Service Levels set forth in the Agreement. Contractor will not be required to provide Performance Credits for multiple Performance Specifications for the same event, with the highest Performance Credit available to the State for that particular event to be applicable.

On a quarterly basis, there will be a “true-up” at which time the total amount of the Performance Credits will be calculated (the “Net Amount”), and such Net Amount will be set off against any fees owed by the State to Contractor, unless the State requests a payment in cash.

Moreover, in the event of consecutive failures to meet the Service Levels, the Contractor will be required to pay the State the maximum Credit under the terms of this document.

Contractor will not be liable for any Service Level caused by circumstances beyond its control, and that could not be avoided or mitigated through the exercise of prudence and ordinary care, provided that Contractor takes all steps to minimize the effect of such circumstances and to resume its performance of the Services in accordance with the SLAs as soon as possible.

Consecutive Months Credit Table (SLA Performance Credits)												
Individual SL GYR State	1 st Month	2 nd Month	3 rd Month	4 th Month	5 th Month	6 th Month	7 th Month	8 th Month	9 th Month	10 th Month	11 th Month	12 th Month
Red	A =1.71% of MRC	A + 50% of A	A + 100% of A	A + 150% of A	A + 200% of A	A + 250% of A	A + 300% of A	A + 350% of A	A + 400% of A	A + 450% of A	A + 500% of A	A + 550% of A
Yellow	B = 0.855% of MRC	B + 50% of B	B + 100% of B	B + 150% of B	B + 200% of B	B + 250% of B	B + 300% of B	B + 350% of B	B + 400% of B	B + 450% of B	B + 500% of B	B + 550% of B
Green	None	None	None									

For example, if an Individual SL GYR State is Yellow in the first Measurement Period, Red in the second Measurement Period and back to Yellow in the third Measurement Period for an SLA then the Performance Credit due to the State will be the sum of Yellow Month 1 (B) for the first Measurement Period, Red Month 2 (A + 50% of A) for the second Measurement period, and Yellow Month 3 (B + 100% of B) for the third Measurement period, provided (1) such Performance Credit does not exceed 12% of the aggregate Monthly Recurring Charge (the At-Risk Amount); and, (2) no single Service Level Credit will exceed 20% of the total At-Risk Amount, as stated below:

- Service Level Credit payable to the State = (B) + (A + 50% A) + (B + 100% B), based on an illustrative Monthly Recurring Charge of \$290,000.

SLA Calculation EXAMPLE						
Monthly Recurring Charge (MRC) = \$290,000.00						
Monthly At Risk Amount = 12% of MRC = \$34,800						
Maximum for any one SLA = 20% of At Risk Amount = \$6,960						
GYR State	1 st Month		2 nd Month		3 rd Month	
Red	0	\$	0	\$ 7,438.50	0	
Yellow	1	\$ 2,479.50	1		1	\$ 4,959.00
Green	6	\$	6		6	
Totals	7	\$ 2,479.50	7	\$ 7,438.50	7	\$ 4,959.00
Adjusted Totals by At Risk Amount and 20% per individual SLA Limitations	(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - Yes \$ 2,479.50		(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - No \$ 6,960.00		(Is monthly total of all Service Level Credits equal to or less than \$34,800?) - Yes (Is monthly amount for any one Service Level Credit equal to or less than \$ 6,960?) - Yes \$ 4,959.00	
Total Quarterly Credit:	\$ 2,479.50		+ \$ 6,960.00		+ \$ 4,959.00	
Total Quarterly Credit: \$ 14,398.50						

11.4 Service Level Exclusions and Other Considerations

SLA/SLOs shall not apply to out of scope equipment repairs (generally those exceeding \$5,000 or those otherwise covered by a maintenance contract or third party warranty that are not provided by the Contractor) that are out of the scope of the managed service or otherwise the sole responsibility of the State.

To further clarify, the Performance Credits available to the State under the terms of this document will not constitute the State exclusive remedy to resolving issues related to Contractor’s performance.

Service Levels will not apply during the Transition period, but will commence with the Contractor’s assumption of services in the production Steady State environment for all migrated elements in part or in full.

Should, for any reason, not all Service levels be in effect for any reporting period, the weighting of the remaining Service Levels that are in effect for the period must be adjusted to compensate for the absence of Service Levels not in effect for that period. As an example, if there are twelve service levels specified to in effect in a given month, and assuming 12% fees at risk, each SL when weighted equally would equate to 1% of the fees at risk. If, due to timing or other reasons only 9 SLs are in effect for a month, each one would represent approximately 1.33% of the fees at risk total.

The total of any weighting factors may not exceed 100% of the total At-Risk Amount.

The following calculation must apply to periods when all SLs are not in effect:

Total Number of Service Levels	X	Fees at Risk	=	Individual SL
Total Service Levels in Effect for Reporting Period	Times	(12%)	equals	Weighting for Period

11.5 Treatment of Federal, State, and Local Fines Related to Service Disruption

Above and beyond the Service Levels discussed above, should any failure to deliver services by the Contractor result in a mandated regulatory fine associated with late, incomplete, or incorrect filings as a **direct result** of Contractor’s inability to deliver services under the defined Statement(s) of Work, production schedules, reporting

and filing obligations, the requirements and Service Levels contained herein , the Contractor will be obligated to issue a credit to the State equal to the amount of the fine.

11.6 Overall Contract Performance

In addition to the service specific performance credits, on a monthly basis, an overall SL score (the “Overall SL Score”) will be determined, by assigning points to each SL based on its Individual SL GYR State. The matrix set forth below describes the methodology for computing the Overall SL Score:

Individual SLAs and SLOs GYR State	Performance Multiple
Green	0
Yellow	1
Red	4

The Overall SL score is calculated by multiplying the number of SLAs and SLOs in each GYR State by the Performance Multiples above. For example, if all SLAs and SLOs are Green except for two SLAs in a Red GYR State, the Overall SL Score would be the equivalent of 8 (4 x 2 Red SLAs).

Based on the Overall SL Score thresholds value exceeding a threshold of 26 then executive escalation procedures as agreed to by the parties will be initiated to restore acceptable Service Levels. The State may terminate the Contract for cause if:

- The overall SL score reaches a threshold level of 44 per month over a period of 3 consecutive months (equivalent to 50% of the service levels in a red State); or
- Contractor fails to cure the affected Service Levels within 60 calendar days of receipt of the State written notice of intent to terminate; or
- The State exercises its right to terminate for exceeding the threshold level of 88 per month (i.e., all Service Levels not met) within five calendar days of receipt of Contractor’s third monthly SLA status report.

Should the State terminate the Contract for cause, for the Contractor exceeding the threshold level of 88 per month (i.e., all Service Levels not met), it will pay to Contractor actual and agreed wind down expenses only, and no other Termination Charges.

The Overall Contract Performance under the terms of this document will not constitute the State exclusive remedy to resolving issues related to Contractor’s performance.

The State retains the right to terminate for Overall Contract Performance under the terms of this Contract will apply only to this Scope of Work.

11.7 Monthly Service Level Report

On a the State accounting monthly basis, Contractor will provide a written report to the State which includes the following information (the “Monthly Service Level Report”): (i) Contractor’ quantitative performance for each Service Level; (ii) each Individual SL GYR State and the Overall SL Score; (iii) the amount of any monthly Performance Credit for each Service Level (iv) the year-to-date total Performance Credit balance (i.e., credits owed the State by the Contractor) for each Service Level and all the Service Levels (i.e., SLO and SLA results to date); (v) a “Root-Cause Analysis” and corrective action plan with respect to any Service Levels where the Individual SL GYR State was not “Green” during the preceding month; and (vi) trend or statistical analysis with respect to each Service Level as requested by the State . The Monthly Service Level Report will be due no later than the tenth (10th) accounting day of the following month.

11.8 Critical and Non-Critical Applications

The State acknowledges that its application environment requirements fall into two major categories: 1) critical applications – those that are required to perform day-to-day state functions in production or support the SDLC

requirements for major infrastructure investments for major initiatives where significant funds are devoted to providing environments to development teams; and 2) non-critical application environments – which are defined as items that do not have a significant impact on day-to day operations, are used in a non-production capacity, which may not adversely impact the productivity of State development efforts or are otherwise used to support non-commercial activities. The Contractor must deliver Service Levels in keeping with the criticality levels as described below.

11.9 Period Service Level in Full Effect and In-Progress Service Levels

Service levels specified herein must be in full effect no later than ninety (90) days following the completion of migration of the current services and environments to the Contractor’s service delivery centers. During the phases in which the Contractor is performing Transition/Migration Services and while the State still retains operational responsibility of the application environments, and no longer than 180 calendar days following the execution of an agreement between the State and the Contractor, the Contractor will not be subject to financial penalties associated with the Service levels described herein. During the period in which the State no longer has substantive operational responsibilities pertaining to the application environments, and the Contractor is operating application environments on the State’s premise, or a combination of State and Contractor premises the Contractor agrees to:

- Perform services in keeping with the described Service Levels contained herein;
- Promptly report any Service Level violations in accordance with the Service Level reporting requirements contained herein;
- Work in good faith and using commercially reasonable efforts to address and otherwise resolve service level violations that arise;
- Provide a level of service in keeping with levels performed by State personnel and otherwise aligned with commercial best practices prior to the operational transfer; and
- Not be subject to any financial penalties associated with Service Level violations.

11.10 Service Level Review and Continual Improvement

11.10.1 Service Level Agreement Review and Change Process

The State believes that in order to ensure that IT Infrastructure Services are delivered at levels relevant to agency needs, that Service Levels should be subject to review on the following occasions throughout the Term via established governance as outlined in section 12.

Offerors are directed to include processes within the completion of governance activities as they pertain to reviewing and adjusting SLAs as follows:

- **Initial Review:** Within six months of an Agency Service Commencement Date or completion of Migration as outlined in the Statement of Work, whichever is sooner, the Parties will meet to review the Service Levels and the Contractor’s performance and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be only as agreed upon in writing by the Parties.
- **Six Month Review:** Within six months of an Agency Service Commencement Date or completion of Migration as outlined in the Statement of Work, and every six months thereafter, the Parties will meet to review the Service Levels and the Contractor’s performance in the period of time since the prior review, and discuss possible modifications to the Service Levels. Any changes to the Service Levels will be only as agreed upon in writing by the Parties.
- **Ongoing Annual Reviews:** The Contractor and the State must set a mutually agreed date to conduct annual reviews of the Service Levels and the Contractor’s performance with respect to the Service Levels. At a minimum, the annual review must include:
 - Comprehensive review of the previous year’s performance including fault, impact time and duration and a root cause analysis;
 - Compendium of remedial actions, operational or process enhancements, system hardware or software enhancements implemented to address any deficiencies with regard to delivering the Service Levels; and
 - Revision of the Service Levels, if any, based upon mutual written agreement

11.10.2 Continuous Improvement

Continual Improvement: Twelve months after the completion of Transition as outlined in the SOW, the Parties will meet to review the Service Levels and Contractor’s performance in the period of time since the prior review. For each SLA and SLO, the performance during the six highest performing months will be averaged and this performance, if in consideration of the prevailing charges, actual delivered service levels if higher than the current SLA/SLO, State may opt for SLA/SLO modification and or a reduced fee structure associated with a lower, but agreeable level going forward.

Ongoing Annual Reviews: Contractor and the State will set a mutually agreed date to conduct annual reviews of the Service Levels and Contractor’s performance with respect to the Service Levels. At a minimum, the annual review must include:

- Comprehensive review of the previous year’s performance including fault, impact time and duration and a root cause analysis;
- Compendium of remedial actions, operational or process enhancements, system hardware or software enhancements implemented to address any deficiencies with regard to delivering the Service Levels; and
- Revision of the Service Levels, if any, based upon mutual written agreement.

11.11 Monthly Service Level Report

- ★ As part of this project, the Contractor must develop a written automated report to the State which includes the following information (the “Monthly Service Level Report”):
 - Quantitative performance for each Service Level;
 - Each Individual Service Level’s “green, yellow and red” State;
 - A year-to-date total trend for each Service Level and all the Service Levels;
 - A “Root-Cause Analysis” and corrective action plan with respect to any Service Levels where the Individual SL state was not “Green” during the preceding month;

Over the course of the project, the Contractor will assist the State in the creation, refinement and operationalizing of this report so that it can be produced by the State on an ongoing basis as an indication of the overall “health” of the IT Infrastructure services.

11.12 Service Level Scope

A selection of Service Levels has been chosen to align IT Infrastructure services to the State’s goals for these services as follows:

Category	Nº	Service Level	Type
Agency Experience	1	Incident Resolution – Mean Time to Repair (Priority 1 Outages)	SLA
	2	Incident Resolution – Mean Time to Repair (Priority 2 Outages)	SLA
	3	Incident Resolution – Mean Time to Repair (Priority 3 Outages)	Objective
	4	Incident Resolution - Incident Triage, Closure and Recidivist Rate	SLA
	5	Service Availability – Non-Critical Infrastructure Availability	Objective
	6	Service Availability - Virtual Server High Availability	SLA
	7	Service Availability – Data Center LAN Availability	SLA
Predictable Operations	8	Capacity Monitoring & Planning – Capacity Utilization Target	Objective
	9	Scheduled Provisioning – Virtual Machines	SLA
	10	Scheduled Provisioning – Physical Machines	SLA
	11	User Interaction – Administrative User Deletes	SLA
	12	User Interaction –Administrative User Adds and Changes	SLA
Security	13	Security - Security Compliance	Objective
	14	Security – Annual Security Review	Objective
	15	Monitoring & Auditing – Security Breach Detection	Objective
Resource Management	16	Asset Management & Refresh - Asset Inventory Element Accuracy	Objective
	17	Capacity Monitoring and Usage Report	Objective
Change	18	Operational Process Control & Repeatability – Changes to Production Environments	Objective

Category	N°	Service Level	Type
Management	19	Service Availability – Nightly Batch Processing	Objective
	20	Service Quality – System Changes	SLA
	21	Service Timeliness – System Changes	SLA
	22	Service Quality & Timeliness – Delivery Date Compliance	SLA

11.13 Service Level Targets

N°	Service Level	Green	Yellow	Red	Unit / Measure
1	Incident Resolution – Mean Time to Repair (Priority 1 Outages)	<=2	2-6	>6	hours
2	Incident Resolution – Mean Time to Repair (Priority 2 Outages)	<=6	6-12	>12	hours
3	Incident Resolution – Mean Time to Repair (Priority 3 Outages)	<=24	24-36	>36	hours
4	Incident Resolution - Incident Triage, Closure and Recidivist Rate	99%	99%-95%	<95%	kpis met
5	Service Availability – Non Critical Infrastructure	99.5%+	99.5%-99.0%	<99%	9x7 extended business hours uptime
6	Service Availability - Virtual Server High Availability	99.7%+	99.7%-99.9%	<99.7%	uptime
7	Service Availability – Data Center LAN Availability	99.7%+	99.7%-99.9%	<99.7%	uptime
8	Capacity Monitoring & Planning – Capacity Utilization Target	>80%	70-80%	<70%	resource utilization
9	Scheduled Provisioning – Virtual Machines	>90%	80-90%	<80%	% provisioned in <8 hours
10	Scheduled Provisioning – Physical Machines	>90%	80-90%	<80%	% provisioned in <24 hours
11	User Interaction – Administrative User Deletes	>95%	90-95%	<90%	% provisioned in <8 hours
12	User Interaction –Administrative User Adds and Changes	>97%	95-97%	<95%	% provisioned in <4 hours
13	Security - Security Compliance	100%	-	<100%	% Compliance with State Security Policies
14	Security – Annual Security Review	>99%	95%-99%	<95%	KPIs met
15	Monitoring & Auditing – Security Breach Detection	0	-	>0	Security breaches not detected/reported
16	Asset Management & Refresh - Asset Inventory Element Accuracy	>95%	92-95%	<92%	% devices reported in inventory database
17	Capacity Monitoring and Usage Report	>95%	90-95%	<90%	accuracy of capacity usage report for managed devices
18	Operational Process Control & Repeatability – Changes to Production Environments	>99%	95%-99%	<95%	% changes to production that follow plan
19	Service Availability – Nightly Batch Processing	>99%	95-99%	<95%	% jobs initiated/complete on schedule
20	Service Quality – System Changes	>99%	95-99%	<95%	% changes implemented correctly first time
21	Service Timeliness – System Changes	>99%	95-99%	<95%	% changes implemented correctly on schedule
22	Service Quality & Timeliness – Delivery Date Compliance	>99%	95-99%	<95%	% contracted tasks that complete per schedule

11.14 Service Level Specifications

11.14.1 Incident Resolution – Mean Time to Repair (Priority 1 Outages)

Specification: Incident Resolution – Mean Time to Repair (Priority 1 Outages)

Definition: Mean Time to Repair (Priority 1 Outages) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Priority 1 Outage Service Requests for in-scope Services in the Contract Month. “Time to Repair” is measured from time Service Request is received at the Level 2 Service Desk to point in time when the incident is resolved or workaround is in place and the Contractor submits the resolved Service Request to the State for confirmation of resolution.

“Priority 1 Outage Service Request” is defined as :

An Incident must be categorized as a “Severity 1 Incident” if the Incident is characterized by the following attributes: the Incident (a) renders a business critical System, Service, Software, Equipment or network component un-Available, substantially un-Available or seriously impacts normal business operations, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

This Service Level begins upon completion of agreed production acceptance criteria and a measurement period as documented in the transition to production plan. The initial service level shown for this SLA will be 99.0%, and will be validated during a measurement period. Following the measurement period, the initial Service Level will be adjusted to 99.5%. The measurement period will be as mutually agreed by the Parties, not to exceed six months.

Formula:
$$\text{Mean Time to Repair (Priority 1 Outages)} = \frac{\text{(Total elapsed time it takes to repair Priority 1 Outage Service Requests)}}{\text{(Total Priority 1 Outage Service Requests)}}$$

Measurement Period: Accounting Month

Data Source: Monthly Service Report

Frequency of Collection: Per incident

11.14.2 Incident Resolution – Mean Time to Repair (Priority 2 Outages)

Specification: Incident Resolution – Mean Time to Repair (Priority 2 Outages)

Definition: Mean Time to Repair (Priority 2 Outages) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Priority 2 Outage Service Requests for in-scope Services in the Contract Month. “Time to Repair” is measured from time Service Request is received at the Level 2 Service Desk to point in time when the incident is resolved or workaround is in place and the Contractor submits the resolved Service Request to the State for confirmation of resolution.

“Priority 2 Outage Service Request” is defined as :

An Incident must be categorized as a “Severity 2 Incident” if the Incident is characterized by the following attributes: the Incident (a) does not render a business critical System, Service, Software, Equipment or network component un-Available or substantially un-Available, but a function or functions are not Available, substantially Available or functioning as they should, in each case prohibiting the execution of productive work, and (b) affects either (i) a group or groups of people, or (ii) a single individual performing a critical business function.

This Service Level begins upon completion of agreed production acceptance criteria and a measurement period as documented in the transition to production plan. The initial Service Level shown for this SLA will be 99.0% and will be validated during the measurement period. Following the measurement period, the initial Service Level will be adjusted to 99.5%. The measurement period will be as mutually agreed by the Parties, not to exceed six months.

In the event of “go live” of new functionality, an Upgrade, or significant change in the architecture of the Application environment, this Service Level will be suspended temporarily from the time the “go live” of the applicable Change through two (2) business days following completion of stabilization criteria in accordance with the transition to production plan.

Formula:
$$\text{Mean Time to Repair (Priority 2 Outages)} = \frac{\text{(Total elapsed time it takes to repair Priority 2 Outage Service Requests)}}{\text{(Total Priority 2 Outage Service Requests)}}$$

Measurement Period: Accounting Month

Data Source: Monthly Service Report

Frequency of Collection: Per incident

11.14.3 Incident Resolution – Mean Time to Repair (Priority 3 Outages)

Specification: Incident Resolution – Mean Time to Repair (Priority 3 Outages)

Definition: Mean Time to Repair (Priority 3 Outages) will be determined by determining the elapsed time (stated in hours and minutes) representing the statistical mean for all Priority 3 Outage Service Requests in the Contract Month.

“Time to Repair” is measured from time a Service Request for in-scope Services is received at the Level 3 Service Desk to point in time when the incident is resolved or workaround is in place and the Contractor submits the resolved Service Request to the State for confirmation of resolution.

“Priority 3 Outage Service Request” Is defined as :

An Incident must be categorized as a “Severity 3 Incident” if the Incident is characterized by the following attributes: the Incident causes a group or individual to experience a Incident with accessing or using a System, Service, Software, Equipment or network component or a key feature thereof and a reasonable workaround is not available, but does not prohibit the execution of productive work.

This Service Level begins upon completion of agreed production acceptance criteria and a measurement period as documented in the stabilization and transition to production plan. The initial Service Level shown for this SLO will be 99% and validated during the measurement period. Following the measurement period, the initial Service Level will be adjusted to 99.5%. The measurement period will be as mutually agreed by the Parties, not to exceed six months.

Formula: Mean Time to Repair (Priority 3 Outages) = $\frac{\text{(Total elapsed time it takes to repair Priority 3 Outage Service Requests)}}{\text{(Total Priority 3 Outage Service Requests)}}$

Measurement Period: Accounting Month

Data Source: Monthly Service Report

Frequency of Collection: Per incident

11.14.4 Incident Resolution - Issue Triage, Closure and Recidivist Rate

Specification: Incident Resolution - Incident Triage, Closure and Recidivist Rate

Definition: Incident Triage, Closure and Recidivist Rate will be determined by monitoring compliance with the following four key performance indicators (KPI):

Incident Triage: Contractor to indicate high-level diagnosis and estimate to remedy to the State within 30 minutes of acknowledgement

Incident Closure: Incident to be documented with root cause remedy, (where root cause is within Contractor's control), and procedures to eliminate repeat of incident within 24 hours of incident close

Incident Recidivist Rate: Closed incidents not to reappear across all in scope Services no more than 2 times following incident closure.

Incident means any Priority 1 incident where the Services for which Contractor is responsible under the SOW are unavailable.

Formula: Issue Triage, Closure and Recidivist Rate
$$= \frac{(\text{Total Priority 1 Incidents for which Contractor is responsible under the SOW, where solution Services are unavailable}) - (\text{Number of Incidents where the KPI was not in compliance})}{(\text{Total Priority 1 Incidents where Services for which Contractor is responsible under the SOW are unavailable})} \times 100$$

Measurement Period: Half year

Data Source: Incident Management System

Frequency of Collection: Per six month review cycle

11.14.5 Service Availability – Non Critical Infrastructure Availability

Specification: Service Availability – Non Critical Infrastructure Availability

Definition: Infrastructure Component Availability for each in-scope Platform that the State identifies as “non-critical” or non-production environments supporting routine system development and maintenance activities, training, demonstration or supporting non-commercial use application usage.

Infrastructure Component Availability means access to the underlying system is enabled; operating system log-in permitted from the user workstation and business transactions can be executed. While it is dependent on hardware, system software and Third Party software and network availability the expectation is that the Contractor will implement monitoring instrumentation that validates availability to the point of presence within the Service Delivery Center.

Scheduled Business hours are 9 hours per day, 7 days a week, commencing at 8am local time

Formula:
$$\text{Non-Critical Infrastructure Availability} = \frac{(\text{Total application business hours uptime minus total application unscheduled business hours downtime})}{(\text{Total application scheduled business hours uptime})} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Continuous (24 hours a day, 7 days a week)

11.14.6 Service Availability – Virtual Server Availability

Specification: Service Availability – Virtual Server Availability

Definition: Virtual Server Availability for each in-scope Platform that the State identifies as “critical” or -production environments supporting production applications, agency functions, other normal business functions, or commercial use application usage.

Virtual Server Availability means access to the underlying system is enabled; operating system log-in permitted from the user workstation and business transactions can be executed. While it is dependent on hardware, system software and Third Party software and network availability the expectation is that the Contractor will implement monitoring instrumentation that validates availability to the point of presence within the Service Delivery Center.

Scheduled Business hours are 24 hours per day, 7 days a week

Formula: Server Availability =
$$\frac{(\text{Total server uptime minus total server hours downtime})}{(\text{Total server hours uptime})} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Continuous (24 hours a day, 7 days a week)

11.14.7 Service Availability – Data Center LAN Availability

Specification: Service Availability – Data Center LAN Availability

Definition: LAN Availability for each in-scope Platform,

LAN Availability means LAN access to the production system is enabled; log-in permitted from the local LAN and business transactions can be executed. While it is dependent on hardware, system software and Third Party software availability the expectation is that the Contractor will implement LAN monitoring instrumentation that validates availability to the point of presence within the Service Delivery Center.

This Service Level begins upon completion of stabilization criteria as documented in the stabilization and transition to production plan. In the event of “go live” of new functionality, an upgrade, or significant change in the architecture of the LAN Environment, this Service Level will be suspended temporarily from the time the “go live” of the applicable Change through two (2) business days following completion of stabilization criteria in accordance with the stabilization and transition to production plan Scheduled

Availability hours are 24 hours per day, 7 days a week

Formula:
$$\text{LAN Availability} = \frac{\text{Total LAN Device scheduled uptime minus total LAN Device unscheduled downtime,}}{\text{(Total LAN Device scheduled uptime)}} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Continuous (24 hours a day, 7 days a week)

11.14.8 Capacity Monitoring & Planning – Capacity Utilization

Specification: Capacity Monitoring & Planning – Capacity Utilization

Definition: Capacity Monitoring & Planning – Capacity Utilization Flag will be determined by monitoring compliance with the following five key performance indicators (KPI):

Contractor Service Delivery Center CPU capacity not to exceed 95% aggregate sustained utilization by Supported server class (compute, file, web etc.) for a period of 4 hours or 80% aggregate sustained utilization for a period of 8 hours. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents.

Contractor Service Delivery Center disk capacity (online) not to exceed 80% utilization as measured by both available disk space and available I/O by server class for period of 5 days. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents.

Contractor Service Delivery Center memory usage not to exceed 95% aggregate sustained utilization by server class for period of 4 hours. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents.

Data center LAN and Wide Area connectivity elements not to exceed 90% aggregate sustained utilization on primary network backbone. If this performance indicator has not been met then Contractor has notified the State and provided a remediation/enhancement plan as set forth in the Process Interface Manual or other supporting documents.

Flag, for the purposes of this Service Level, means a Contractor notification to the State as set forth in the Process Interface Manual or other supporting documents.

Formula: Capacity Utilization = (Number of instances where individual KPI's were not in compliance)

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per monthly reporting cycle

11.14.9 Scheduled Provisioning – Virtual Machines

Specification: Scheduled Provisioning – Virtual Machine environments

Definition: Scheduled provisioning of virtual machine environments is defined as the planning, management and configuration of the host server and their connectivity to networks and data storage devices to accommodate new requests for service.

Time measurement is from receipt of the provisioning request in the Contractors Service Desk through to visibility of the provisioned machine on the network.

Formula:
$$\frac{\text{Scheduled Provisioning Virtual Machines} \times 100 - (\text{Total number of virtual machine scheduled provisioning requests}) \text{ minus } (\text{number of scheduled virtual machines provisioned in greater than 8 hours})}{(\text{Total number of virtual machine scheduled provisioning requests})}$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per provisioning request

11.14.10 Scheduled Provisioning – Physical Machines

Specification: Scheduled Provisioning – Physical Machines

Definition: Scheduled provisioning of physical machines is defined as the sourcing, procurement and planning tasks necessary to procure, set up and configure additional Service Delivery Center hardware required by the State, provided that such hardware is available at Contractor’s Service Delivery Center. Set of representative hardware includes:

- i. Cabinet (e.g., Rack, Power, UPS, KVM)
- ii. Hardware (e.g., CPU/servers, Disk Arrays, Monitors)
- iii. Networking Equipment (e.g., Switches)

Time measurement is from receipt of the provisioning request in the Contractors Service Desk through to visibility of the provisioned machine on the network.

Formula:
$$\frac{\text{Provisioning Physical Machines} \times 100}{\text{(Total number of scheduled physical machine provisioning requests) - (number of scheduled physical machines provisioned in greater than 2 business days of initial contact with Service)}} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per provisioning request

11.14.11 User Interaction - Completion of Administrative User Deletes

Specification: User Interaction - Completion of Administrative User Deletes

Definition: Administrative Users are defined as any user who maintains “administrator”, “super-user” or “root” equivalent access to operating systems, devices and networking equipment. Administrative Users do not include end-users or users otherwise managed by an agency Application.

Completion of Deletes defines the timeliness of both emergency and scheduled User Deletes.

Late Emergency User Deletes are defined as anything greater than 1 business hour

Late Scheduled User Deletes are defined as anything greater than 4 business hours

Formula:

$$\begin{array}{l} \text{Completion} \\ \text{of} \\ \text{Administrativ} \\ \text{e User} \\ \text{Deletes} \end{array} = \frac{((\text{Total Emergency User Deletes}) - (\text{Late Emergency User Deletes})) + ((\text{Total Scheduled User Deletes}) - (\text{Late Scheduled User Deletes}))}{(\text{Total Emergency User Deletes}) + (\text{Total Scheduled User Deletes})} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per Administrative user delete

11.14.12 User Interaction - Completion of Administrative User Adds & Changes

Specification: User Interaction - Completion of User Adds & Changes

Definition: Administrative Users are defined as any user who maintains “administrator”, “super-user” or “root” equivalent access to operating systems, devices and networking equipment.

Completion of User Adds & Changes defines the timeliness of the creation of new users and the implementation of changes to existing users

Computation of time to complete begins when the identification validation is completed and a ticket is entered into Contractor’s Service Desk, and excludes technical corrections required as stated in the Process Interface Manual or other supporting documentation.

Late User Adds and Changes are defined as anything beyond 4 business hours

Formula:

$$\frac{\text{Completion of Administrative User Adds \& Changes} - (\text{Total number of requests for Administrative User Adds \& Changes}) - (\text{Number of Late User Adds \& Changes})}{(\text{Total Number of requests for Administrative User Adds \& Changes})} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per user add and change request

11.14.13 Security – Security Compliance

Specification: Security – Security Compliance

Definition: Security Compliance will be determined by monitoring compliance with the following five key performance indicators (KPI):

Material compliance with the State IT security policies listed in Supplement Seven

Update of antivirus signatures with most current version every 12 hours

100% of environments (inclusive of memory, disk and other file structures) to be actively scanned for viruses, trojan horses, rootkits and other malware every 24 hours

100% LAN devices actively scanned for open ports, forwarded ports or configurations not in keeping with adherence to the State security policies every 24 hours

100% of environments to be reviewed for inactive/suspended user accounts every 30 days

Formula: Security Compliance Flag

$$\frac{(\text{Total number of individual KPI's performed per month}) - (\text{Total number of individual KPI's performed per month that were not in})}{(\text{Total number of individual KPI's performed per month})} \times 100$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per monthly reporting cycle

11.14.14 Security – Annual Security Review

Specification: Security – Annual Security Review

Definition: Annual Security Review completion will be determined by monitoring compliance with the following three key performance indicators (KPI):

Contractor to provide a non-The State specific audit of the Contractor facilities providing the Services every 12 months through an Contractor SSAE 16 Type 2 report as stated in the SOW.

Contractor to provide the right for a Third Party or the State security personnel to perform an annual security reviews at the Contractors facilities used to provide the Services. Contractor will assist and cooperate with this effort by providing Third Party or the State security personnel with appropriate access to Contractor’s facilities and personnel as required to conduct these reviews.

This Service Level begins upon completion of Transition; and for the SSAE 16 Type 2 report, upon the first SSAE 16 Type 2 report prepared by Contractor’s external reviewer after completion of Transition as stated in the SOW.

Formula: Annual Security Review (Number of instances where individual KPI’s were not in compliance)

Measurement Period: Twelve months

Data Source: Annual SLA Review Report

Frequency of Collection: Per twelve month audit cycle or following any audit

11.14.15 Monitoring & Auditing – Security Breach Detection

Specification: Monitoring & Auditing – Physical, Network, System Security Breach Detection

Definition: Physical, Network, System Security Breach Detection will be determined by monitoring compliance with the following two key performance indicators (KPI):

Physical, Network, System security breach success notification due within 30 minutes of physical intrusion detection of Contractor’s Service Delivery Center area containing Contractor’s Machines. Notification will be as set forth in the Process Interface Manual or other supporting documents.

Physical, Network, System security breach (attempt, failure) notification due within 1 hour of such physical intrusion detection. Notification will be as set forth in the Process Interface Manual or other supporting documents.

Formula: Security Breach Detection (Number of instances where individual KPI’s were not in compliance)

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Continuous (24 hours a day, 7 days a week)

11.14.16 Asset Management & Refresh – Asset Inventory Element Accuracy

Specification: Asset Management & Refresh – Asset Inventory Element Accuracy

Definition: Asset Inventory Element Accuracy will be determined by comparing the Contractor provided and maintained Asset Management Tracking system records against the State system generated record of Asset Inventory Elements. The scope of this comparison is all hardware (physical and virtual) including equipment and software procured, operated and supported by the Contractor for use by the State, as set forth in the SOW. Contractor will not be responsible for accuracy errors that are not caused by Contractor.

Formula:
$$\text{Asset Element Accuracy} = \frac{(\text{Total Asset Inventory Elements}) - (\text{Total Inaccurate Asset Inventory Elements})}{(\text{Total Asset Inventory Elements})}$$

Measurement Period: Accounting Month

Data Source: Asset Inventory Management System

Frequency of Collection: Per monthly reporting cycle

11.14.17 Capacity Monitoring and Usage Report

Specification: Capacity Monitoring and Usage Report

Definition: The Capacity monitoring and usage measure is determined by monitoring compliance with the following key performance indicator:

Capacity monitoring and usage report distributed electronically to the State in less than or equal to 7 days following the State accounting period month end.

Formula: Capacity Usage & Planning (Number of instances where individual KPI's were not in compliance)

Measurement Period: Monthly

Data Source: Monthly Capacity Monitoring and Report

Frequency of Collection: Per monthly review cycle

11.14.18 Operational Process Control & Repeatability – Changes to Production environments

Specification: Operational Process Control & Repeatability – Changes to Production environments

Definition: The changes to production environment measure is determined by monitoring compliance with the following two key performance indicator:

All changes to production environments have an authorization from an approved State employee

Corresponding updates to the Process Interface Manual or other supporting documents are completed within three business days of receiving and implementing minor approved change request(s)

Formula:
$$\frac{\text{Changes to Production environments} \times 100}{\text{(Total number of changes and updates where individual KPI's were not in compliance for the month)}}{\text{(Total number of changes and updates for the month)}}$$

Measurement Period: Monthly

Data Source: Monthly Service Level Report

Frequency of Collection: Per monthly review cycle

11.14.19 System Performance & Responsiveness

Specification: System Performance & Responsiveness

Definition: System Performance & Responsiveness will be based on the following:

Upon service transition and acceptance, Contractor will perform end-to-end service class performance baselining (e.g., network time, application/session response time, system time, and network return time) for key service elements as mutually agreed.

Formula:
$$\text{System Performance \& Responsiveness} = \frac{\text{Total service elements that do not meet the baseline requirements}}{\text{Total service elements}}$$

Measurement Period: Monthly

Data Source: Monthly Service Level Report

Frequency of Collection: Monthly

11.14.20 **Service Quality – System Changes**

Specification: Service Quality – System Changes

Definition: The Service Quality & Timeliness System Changes measure is determined by monitoring compliance with the following four key performance indicators (KPI):

99% of system changes or updates (i.e., break fix, configuration, and patches) in planned releases are implemented correctly the first time (OS, Router, BIOS, Microcode and other in-scope code and Applications)

99% of system changes (i.e., break fix, configuration, and patches) in planned releases that do not cause other problems

95% of system changes or updates (i.e., break fix, configuration, and patches) in emergency releases are implemented correctly the first time (OS, Router, BIOS, Microcode and other in-scope code)

95% of system changes (i.e., break fix, configuration, and patches) emergency releases that do not cause other problems

Formula:

Service Quality System Changes	(Number of instances where individual KPI's were not in compliance) <hr style="width: 100%;"/> (Number of total KPIs)
--------------------------------------	---

Measurement Period: Monthly

Data Source: Monthly Service Level Report

Frequency of Collection: Per monthly review cycle

11.14.21 Service Timeliness – System Changes

Specification: Service Timeliness – System Changes

Definition: The Service Timeliness System Changes measure is determined by monitoring compliance with the following three key performance indicators (KPI):

Emergency system changes or updates (i.e., break fix, configuration, and patches) to operating systems on Contractor’s Machines to be initiated within 24 hours of the State approved request form and Change Management Process and to be reported complete within 1 hour of completion

Non-emergency system changes or updates (i.e., break fix, configuration, and patches) to operating systems on Contractor’s Machines to be initiated in accordance with the State policies as stated in the SOW and reported within 2 days of post implementation certification

Emergency system changes or updates (i.e., break fix, configuration, and patches) will be defined as set forth in the Process Interface Manual or other supporting documents.

Formula:

$$\frac{\text{Service Timeliness System Changes (Total Number of system changes where individual KPI's were not in compliance per month)}}{\text{(Total number of system changes per month)}}$$

Measurement Period: Monthly

Data Source: Monthly Service Level Report

Frequency of Collection: Per monthly review cycle

11.14.22 **Service Levels – Delivery Date Compliance**

Specification: Delivery Date Compliance

Definition: For service requests activities related to code changes that Contractor commits to a mutually agreed upon delivery date, the percent of resolutions that are completed by the delivery date

Formula: Delivery Date Compliance
$$\frac{(\text{Total Number of Code Changes}) - (\text{Number of Code Changes failing to meet agreed Delivery Date})}{(\text{Total Number of Code Changes})}$$

Measurement Period: Accounting Month

Data Source: Monthly Service Level Report

Frequency of Collection: Per monthly reporting cycle

12.0 Contract Governance and Changes

12.1 Regular Meetings and Conference Calls

Within thirty (30) days after the Effective Date of the commencement of the Managed Service, the Parties will determine an appropriate set of scheduled periodic monthly meetings or telephone conference calls to be held between representatives of the State and the Contractor. At either Party's request, the other Party will publish its proposed agenda for any meeting sufficiently in advance of the meeting to allow meeting participants an opportunity to prepare. All meetings will be held in such location as mutually agreed by the Parties. The Parties contemplate that such meetings will include the following:

- A monthly meeting among the State Account Representative, the Contractor Account Representative and any other appropriate operational personnel to discuss daily performance and planned or anticipated activities that may adversely affect performance or any contract changes;
- A quarterly management meeting of the Service Management Steering Committee; and
- An annual senior management meeting to review relevant performance and other issues.

12.2 System Changes

The Contractor will comply with the following control procedures for any changes to the in-scope environments or supporting production infrastructure ("System Environment Changes"):

- The Contractor will schedule its implementation of System Environment Changes so as not to unreasonably interrupt State business operations.
- The Contractor will make no System Environment Changes that would alter the functionality of the systems used to provide the Services to an agency or degrade the performance beyond established baselines for online transactions, or from established agency run-look batch processing cycle times and schedules or SLAs as established of the Services, without first obtaining State approval.
- In the case of an emergency, and in keeping with State security policies in effect, the Contractor may make temporary System Environment Changes at any time and without State approval, to the extent such System Changes are necessary, in the Contractor's judgment, (i) to maintain the continuity of the Services, (ii) to correct an event or occurrence that would substantially prevent, hinder or delay the operation of State critical business functions; and (iii) to prevent damage to the Contractor's network or equipment. The Contractor will promptly notify the State of all such temporary System Environment Changes. At the conclusion of the emergency the Contractor will restore any System Environment Changes to the pre-emergency state, and if the change is deemed necessary for normal operation of the system, a corresponding change request will be initiated for State review and approval.
- The Contractor will review, and perform a root-cause analysis of any deviation from scheduled System Environment Changes and failed System Environment Changes.
- Prior to using any software or equipment to provide the Services, the Contractor must perform agreed upon testing with the exception of User Acceptance or Validation testing which will be performed by the State. During User Acceptance or Validation testing the State will verify that the item has been properly installed, is operating substantially in conformance to its specifications, and is performing its intended functions in a reliable manner in keeping with the defined Service Levels in effect at the time of the change.
- The Contractor will follow a mutually agreed, formalized and published methodology in migrating systems, environments, configurations and Contractor supplied programs from development and testing environments into production environments.

12.3 Extraordinary Events

If an Extraordinary Event occurs, the Parties will meet within three (3) business days to discuss and review the potential impact, including the impact on Contractor's charges and resources (including base charges and rates as appropriate). The Parties will work to agree on equitable adjustments, if required, to then-current resources, service levels, and pricing. If the Parties are unable to reach a mutual agreement on such equitable adjustments,

the Parties will follow the internal escalation procedures. As part of a mutually agreed upon resolution to any Extraordinary Events, the Parties may agree: (i) to add to, or eliminate from, the provision of Services, certain Contractor Personnel providing the Services, as the case may be); or, (ii) to modify as appropriate the costs (including appropriate indirect and overhead costs) as part of any targeted resource additions or targeted resource reductions.

Any such changes to the Services will be documented in a mutually agreed upon Change Order. In the event the Parties so agree, Contractor will promptly enact the targeted resource additions or targeted resource reductions, but in no event will such targeted resource additions or targeted resource reductions take more than three (3) months from the effective date of any related Change Order.

12.4 Dispute Resolution

12.4.1 Informal Dispute Resolution

Prior to the initiation of formal dispute resolution procedures as to any dispute (other than those arising out of the breach of a Party's obligations), the Parties will first attempt to resolve each dispute informally, as follows:

- If the Parties are unable to resolve a dispute in an amount of time that either Party deems required under the circumstances, such Party may refer the dispute to the State CIO or designee by delivering a written notice of such referral to the other Party.
- Within five (5) Business Days of the delivery of a notice referring a dispute to the State CIO or designee, each Party will prepare and submit to the Managed Services Oversight Council a detailed summary of the dispute, the underlying facts, supporting information and documentation and their respective positions, together with any supporting documentation.
- The State CIO or designee will address the dispute at its next regularly scheduled meeting or, at the request of either Party, will conduct a special meeting within ten (10) Business Days to address such dispute. The State CIO or designee will address the dispute in an effort to resolve such dispute without the necessity of any formal proceeding.
- The State CIO or designee will address the dispute at the next regularly scheduled meeting between the Contractor and the State or, at the request of either Party, will conduct a special meeting within twenty (20) Business Days to address such dispute. The State CIO or designee will address the dispute in an effort to resolve such dispute without the necessity of any formal proceeding.
- If the State CIO or designee is unable to resolve a dispute within thirty (30) days of the first regular meeting between the State and Contractor addressing such dispute (or such longer period of time as the Parties may agree upon), either Party may refer the dispute to internal escalation by delivering written notice of such referral to the other Party.

12.4.2 Internal Escalation.

If for whatever reason the Contractor and the State cannot resolve a dispute via the above escalation processes and procedures, the Contractor and the State agree to choose a mutually agreeable neutral third party who will mediate the dispute between the parties. The mediator chosen must be an experienced mediator and must not be: a current or former employee of either party or associated with any aspect of the Government of the State of Ohio; associated with any equipment or software supplier; or associated with the Contractor or the State. As to each prohibition this means either directly or indirectly or by virtue of any material financial interests, directly or indirectly, or by virtue of any family members, close friendships or in any way that would have the reasonable appearance of either conflict or potential for bias. If the parties are unable to agree on a qualified person, the mediator will be appointed by the American Arbitration Association.

The mediation must be non-binding and must be confidential to the extent permitted by law. Each party must be represented in the mediation by a person with authority to settle the dispute. The parties must participate in good faith in accordance with the recommendations of the mediator and must follow procedures for mediation as suggested by the mediator. All mediation expenses, except expenses of the individual parties, must be shared equally by the parties. The parties must refrain from court proceedings during the mediation process insofar as they can do so without prejudicing their legal rights.

If the disputed matter has not been resolved within thirty (30) days thereafter, or such longer period as agreed to in writing by the Parties, each Party will have the right to commence any legal proceeding as permitted by law.

12.4.3 Escalation for Repetitive Service Level Failures

Although it is the State's intent to escalate service level failures to the Contractor Account Representative, the State may decide to escalate to other levels within the Contractor's corporate structure deemed appropriate to resolve repetitive service failures.

12.4.4 No Termination or Suspension of Services.

While any dispute is pending, the Contractor must continue its obligations under the Contract and not take any action that intentionally obstructs, delays, or reduces in any way the performance of such obligations.

12.5 Billing, Invoicing and Reporting

12.5.1 Billing Format and Timing

The Contractor must provide electronic billing by the first business day of each month for the Monthly Recurring Charge, and by the tenth day of each month for the preceding month's additional or reduced charges.

12.5.2 Billing Detail

In support of the monthly electronic billing feed, the Contractor must include sufficient detail as to uniquely identify key billable items including, but not limited to, the following: quantity of items, service types/description, resource units, and prices on a monthly basis with sufficient granularity to link to the State cost centers.

The monthly billed amount will include the Monthly Recurring Charge adjusted by any additional or reduced charges (which may include Performance Credits to the State) during the preceding financial cycle (usually one month), plus any additional amended services incurred during the month. The annual billed amount is equal to the total of the Monthly Recurring Charge, adjusted by additional or reduced charges, plus any additional amended services for a given invoice period.

12.5.3 Invoicing

The Contractor agrees to meet with the State, after award of the Contract, to formalize the invoice requirements, including, but not limited to format, content, back up information, review processes, approval and timing considerations.

12.5.4 Reporting

The Contractor will implement and utilize measurement and monitoring tools and metrics as well as standard reporting procedures to measure, monitor and report the Contractor's performance of the Services against the applicable Service Level Specific Performance plus the Overall Performance Score and provide any other reports required under the Contract. The Contractor will provide the State with access to the Contractor's asset management reports used in performing the services, and to on-line databases containing up-to-date information regarding the status of service problems, service requests and user inquiries. The Contractor also must provide the State with information and access to the measurement and monitoring reports and procedures utilized by the Contractor for purposes of audit verification. The State will not be required to pay for such measurement and monitoring tools or the resource utilization associated with their use.

Prior to the Commencement of the Managed Service, the Contractor must provide the proposed report formats to the State for approval. In addition, from time to time, the State may identify a number of additional reports to be generated by the Contractor and delivered to the State on an ad hoc or periodic basis. Generally, the Contractor tools provide a number of standard reports and capability to provide real-time ad hoc queries by the State. A number of additional or other periodic reports (i.e., those other than the standard ones included in the tools) mean a number that can be provided incidentally without major commitment of resources or disruption of the efficient performance of the services. Such additional reports will be electronically generated by the Contractor,

provided as part of the Services and at no additional charge to the State. To the extent possible, all reports will be provided to the State on-line in web-enabled format and the information contained therein will be capable of being displayed graphically.

At a minimum, the reports to be provided by the Contractor must include:

- Monthly Service Level report(s) documenting the Contractor's performance with respect to Service Level Agreements;
- Monthly report(s) describing the State utilization of each particular type of Resource Unit, and comparing such utilization to then applicable baseline for each Resource Unit;
- A number of other periodic reports requested by the State which the State reasonably determines are necessary and related to its use and understanding of the Services; and,
- Reports that contain resource unit utilization data at a level of detail, and any other similar and related information that the State reasonably determines is necessary, to enable the State to verify and allocate accurately the Contractor's Charges under this Scope of Work to the various business units and divisions of the State and the other Eligible Recipients.

12.5.5 Back-Up Documentation

As part of the Services, the Contractor will provide the State with such documentation and other information available to the Contractor as may be reasonably requested by the State from time to time in order to verify the accuracy of the reports provided by the Contractor. In addition, the Contractor will provide the State with all documentation and other information reasonably requested by the State from time to time to verify that the Contractor's performance of the Services is in compliance with the Service Levels and this Scope of Work.

12.5.6 Correction of Errors

As part of the Services and at no additional charge to the State, the Contractor will promptly correct any errors or inaccuracies in or with respect to the reports, the date or other Deliverables caused by the Contractor or its agents, subcontractors or Third Party product or service providers.

12.5.7 Cost of Living Adjustments

The pricing in the Cost Summary Form and in any SOW as applicable for Contractor resources (excluding fixed fee SOW pricing) shall be adjusted on July 1 of each year following the third (3rd) full year of the Contract during the Term to reflect the effects of cost of living and inflation. The pricing and rates will be adjusted using the relative change in the Employment Cost Index (ECI) as published by the Bureau of Labor Statistics of the U.S. Department of Labor. Should a cost adjustment, either an increase or decrease, be required as per a fluctuation of ECI, the Contractor and State will meet, no less than ninety (90) days to the effective date of the increase or decrease prior, to review the change and work to ensure that the required purchase orders, invoices, reporting and other billing artifacts are adjusted in advance to help ensure an orderly move to the new pricing. Should the proposed pricing adjustment based on ECI vary in either direction (i.e., up or down) by more than 5% in a given year, the State and Contractor will meet, no less than ninety (90) days prior to the effective change, to review alternative methods as to how best to address this fluctuation in a mutually agreeable manner, which could include service scope or service level reductions or increases. In no case shall an automatic annual cost increase or decrease exceeding 5% of the prior year's fees be permitted.

12.6 Benchmarking

12.6.1 General

The State may request the services of an qualified independent Third Party (a "Benchmarker") to compare the quality and price of the Services against the quality and price of well-managed operations performing services of a similar nature. The State uses the Benchmarker to validate that it is obtaining pricing and levels of service that are competitive with market rates, prices and service levels, given the nature, volume and type of Services provided by the Contractor hereunder ("Benchmarking").

12.6.2 Frequency & Designation of Benchmarker

- The State may request Benchmarks during the term of the Contract at any time after completion of Transition; no more frequently than every two years.
- For purposes of performing Benchmarking services, the Parties will designate a nationally recognized Benchmarker as mutually agreeable as the Third Party Benchmarker.
- The Benchmarker will execute a tripartite agreement with the State and the Contractor, which will at a minimum reflect the requirements set forth in this section.
- The Benchmarker will not be compensated on a contingency fee or incentive basis.
- The State and the Contractor will share equally the fees and expenses the Benchmarker charges in conducting the Benchmark.

12.6.3 Methodology

The State, the Contractor, and the Benchmarker will conduct the Benchmark in accordance with the following Benchmark process:

- The Benchmarker will conduct the Benchmark using a Representative Sample.
- Prior to performing the comparison, the Benchmarker will provide and review the Benchmark methodology with the State and the Contractor and will explain how each Comparator in the Representative Sample compares to the relevant normalization factors and the normalization approach that will be applied.
- The State and the Contractor will mutually agree to the Benchmark methodology and any appropriate adjustments necessitated by differences in the Services provided to the State and the services provided to the Comparators in the Representative Sample.
- Normalization is used by the Benchmarker to ensure appropriate adjustments are made to all data relating to each of the Comparators in the Representative Sample to account for any differences between the Services provided to the State and the services provided to the respective Comparator that may impede a true “like-for-like” comparison. These normalization factors may include:
 - Scope and nature of services;
 - Respective services environments;
 - The hardware or software used or required to provide the services;
 - Geographic disparity of services delivery and recipient locations;
 - Industry differences affecting information technology costs;
 - Economies of scale;
 - Size of investment;
 - Volume of services being provided;
 - Duration of the contractual commitment;
 - Service levels;
 - Complexity factors (including operating environment);
 - Contractor contract considerations and constraints;
 - Degree of standardization;
 - Financial engineering and allocations;
 - Financing provided by the Contractor;
 - Any additional or value added services performed by the Contractor and not received by the Comparator(s);
 - The State or the Comparators’ unique requirements or limitations;
 - Terms and conditions under which the State received services;
 - Terms and conditions under which the Comparators received services; and
 - Any other relevant factors.
- The Benchmarker will meet with the State and the Contractor to explain how the normalization was performed on each Comparator in the Representative Sample and will provide the State and the Contractor the pre adjustment and post adjustment Comparator data, while preserving the confidentiality of the Comparator.

- Neither the State nor the Contractor will be required to disclose to the Benchmarking actual performance against Service Levels or other actual performance comparison.
- The Representative Sample used by the Benchmarking for the Benchmark will be reasonably current (i.e., based on services provided to the State and the Comparators no more than 12 months prior to the start of the Benchmark).
- During the 30 day period after the Benchmarking completes the data gathering, but before the Benchmarking has concluded the Benchmark analysis, the State and the Contractor will have an opportunity to verify the Benchmark conformed to the agreed Benchmark process.
- The State and the Contractor agree to participate jointly in all discussions with the Benchmarking and to cooperate reasonably with the Benchmarking in the Benchmark activities; provided, however, in no event will the Contractor be required to provide the Benchmarking with the Contractor cost data or data from other Contractor customers.
- The State and the Contractor agree that all information provided to or obtained from the Benchmarking will be provided to both the State and the Contractor, unless otherwise agreed.
- The State and the Contractor agree that the Benchmark will be conducted in a manner that will not unreasonably disrupt either Party's performance or utilization of the Services.
- Any Benchmarking engaged by the State will not be a Direct Contractor Competitor and will agree in writing to be bound by the confidentiality and security provisions specified in this Scope of Work and specify that the data provided by the State and the Contractor may not be used for any purpose other than conducting the Benchmark of the Services. The Contractor will cooperate fully with the State and the Benchmarking and will provide access to the Benchmarking during such effort, at the Contractor's cost and expense.

12.6.4 Standard

The Benchmark Level will be the highest price of the total charges attributable to the Benchmarked Services areas within the top quartile among the Comparators comprising the Representative Sample. The Benchmarking will calculate the range of the first quartile using the Excel spreadsheet macro for quartile calculations.

12.6.5 Adjustments

(a) If the Benchmark determines that the Charges paid by the State for all Services or for any Functional Services Area are less favorable to the State and the charges for the Benchmarked Services Area is in the aggregate equal to or less than the established 10 % dead band, then there will be no adjustment to such charges. If the Benchmark determines that the charges are in the aggregate higher than the Benchmark Level for such Services Area and the difference between the Benchmark Level and the charges for the Benchmarked Services Area is in the aggregate equal to or less than the established 10% dead band, then there will be no adjustment to such charges.

(b) If the Benchmark determines that the charges for any Benchmarked Functional Service Area are in the aggregate higher than the Benchmark Level for such Services Area and the difference between the Benchmark Level and the charges for the Benchmarked Services Area is in the aggregate greater than the established 10% dead band of the charges for such Services Area, then:

(c) Based on consultation with the State, and the State's consent, the Contractor will either reduce such charges for that year, or increase areas of service to be commensurate with the fees being charged to bring the charges for the Benchmarked Services Area within the established 10% dead band, provided that such reduction will be limited to no more than 5% of the current year's Charges, as measured against the originally anticipated revenue for such year. As part of the current year's benchmark, future year's Charges or Services will be adjusted so that they are no greater than the current year's adjusted Charges; provided that the cumulative adjustments made to future year's charges must be no more than 5% of that year's Charges; or

(d) If the Contractor is unwilling to bring the charges for the Benchmarked Services Area within the established 10% dead band as described above, then the State may exercise its right to terminate for convenience the affected Benchmarked Services Area, but the State will be obligated to pay the Contractor's actual Wind-Down Expenses and unamortized investments in lieu of the Termination Charges.

(e) Any changes made to the charges pursuant to a Benchmark will take effect on a prospective basis 30 days following the Benchmarker's delivery of the final Benchmark Results.

12.6.6 Disputes

The State and the Contractor will resolve any disagreement related to the Benchmark using the Dispute Resolution Process.

12.6.7 Charges Review

If the State elects not to conduct a Benchmark in any calendar year, the Parties must meet to review the charges and discuss potential equitable adjustments to the charges. Although any equitable adjustments should be mutual, the Parties are required to review the charges in light of the services provided in the event a Benchmark is not provided. Should the Parties agree to such an equitable adjustment, the Parties will execute an appropriate amendment to this Contract.

12.7 Contractor Best Practices

The Contractor acknowledges that the quality of the Services provided in certain Service areas can and will be improved during the Term and agrees that the Service Levels in such Service areas will be enhanced periodically in recognition of the anticipated improvement in service quality. The Contractor will improve the quality of the Services provided in such areas to meet or exceed the enhanced Service Levels and will do so at no additional charge to the State. The Contractor will implement best practices including but not limited to items included in this RFP, ITIL tools and process compliance, COBIT, CMM development and testing and other practices based on the Contractor's eminence and experience in operating systems of a similar scope and complexity.

12.8 Meetings

In conjunction with regularly scheduled operational meetings with State Personnel or a meeting of the Service Management Steering Committee, and in conjunction with continuous improvement requirements of this Contract, the Contractor may elect to sponsor a meeting to review recent or anticipated industry trends, emerging technologies, technology advancements, alternative processing approaches, new tools, methodologies or business processes (collectively "best practices") that, at the State choosing, could alter the cost, efficiency, computing capacity, server density or otherwise drive efficiencies for both the State and the Contractor.

12.9 Obligations

The Contractor will perform its obligation, including its obligations with respect to continuous improvement, in accordance with the common Six Sigma Quality Improvement Methodology (or similar quality management methodologies that the Contractor may utilize). The State is under no obligation to accept or implement these "best practices", and absent a formal approval to implement these changes with a corresponding change order, the Contractor is under no obligation to implement these "best practices".

12.10 SSAE 16 Type 2 Reporting

In the fourth quarter of every calendar year, the Contractor will be responsible for an independent third party SSAE 16 audit (Statements on Standards for Attestation Engagements No. 16, which superseded SAS-70 in June of 2011). The independent third party must be a nationally recognized firm qualified to perform such audits. The SSAE 16 audit must cover at least the preceding six month period for the Contractor service locations or service types for which the Contractor, in its normal course of business, has conducted SSAE 16 Service Organization Control (SOC) 1 Type 2 report audits and to the extent such reports are pertinent to the Services. The audit will be a multi-customer SSAE 16 SOC 1 Type 2 covering the common processes controlled and performed by the Contractor at primary Contractor shared service locations in administering customer accounts. In the year Transition occurs, a SSAE 16 audit will be required only if Transition is completed in sufficient time to allow six months of Contractor performance prior to September 30 of the first full year of service. A copy of each of the resulting audit reports will be delivered to the State during the last quarter of each calendar year, no less than 45 days following the conclusion of the SSAE 16 audit.

The scope of the Contractor SSAE 16 Type 2 audits must include the elements of service including the hardware, software and services as relevant supporting the Services environment.

It is the sole obligation of the Contractor to remedy any written issues, material weaknesses, or other items arising from these audits as they pertain to services or capabilities provided by the Contractor to the State in conjunction with the Statement(s) of Work in effect at the time of the Audit. The Contractor must remedy these issues at no cost to the State. For items that arise as a result of State policies, procedures and activities, after mutual agreement on the underlying cause, remedial activity requirements and plan, State agrees to work, and under agreed terms, to effect the required changes to the Services delivery model to remediate issues discovered under a SSAE 16 Type 2 audit.

12.11 Audit

12.11.1 Onsite Operational and Financial Examinations

To assist the State in its activities related to oversight of Contractor in the performance of the Contract, in addition to the examinations that occurred prior to the execution of this Contract, subsequent to the Effective Date of this Contract, the State, or its agent, may conduct onsite operational and financial examinations of Contractor.

The onsite examinations may include, without limitation, verification that business is conducted as represented by Contractor at all sites where it performs Managed Services or Disaster Recovery for the State; Contractor's facilities are adequate to support claims of staffing, services performed and inventory housed; and the facilities provide adequate security for staff, functions performed and services rendered. This examination may include verification that Contractor has adequate information security compliance policies and procedures.

The financial examination may include, without limitation, a review of Contractor's current balance sheet; its most recent annual report; up to three (3) years of third party audits; tax returns for the previous three (3) years; and all documentation supporting employee bonds and insurance policies of Contractor.

12.11.2 Consent to Examinations

By execution of this Contract, the Contractor consents to the examinations described in these provisions and the provisions of Attachment Four of the RFP and consents to such examinations being conducted by the State or its agent.

The State may conduct such examinations from time to time during the Term of this Agreement and the consent to the examinations provided by Contractor must be a continuing consent to conduct the examinations periodically in the State's discretion during the Term of this Contract.

12.11.3 Right to Terminate as a Result of Audit Findings

In the event the State determines that the results of any examination of the Contractor is unsatisfactory per the requirements of the Contract and not remedied within a 90 day period following written notice from the State, the State may terminate this Agreement, in part or in full.

If the Contractor fails to satisfy the requirements of the State with regard to security of information, or if an examination reveals information that would result in a continuing contractual relationship that causes the State to be in violation of any law, the State may terminate this Contract immediately without notice.

If the Contractor fails to satisfy the requirements of the State with regard to matters not related to items contained in the preceding two (2) paragraphs, the State will provide Contractor with notice and an opportunity to cure the failure within forty-five (45) days. If the failure is not cured by Contractor within such forty-five (45) day period, the State may terminate this Contract without further notice.

12.12 Criminal Background Check of Personnel

The Contractor agrees that (1) it will conduct third-party criminal background checks on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no Ineligible Personnel will perform Sensitive Services under this Agreement. "Ineligible Personnel" means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, or money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (b) has been convicted of a felony. "Sensitive Services" means those services that (i) require access to Customer/Consumer Information, (ii) relate to the State's computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities ("Sensitive Services"). Upon request, the Contractor will provide written evidence that all of the Contractor's personnel providing Sensitive Services have undergone a criminal background check and are eligible to provide Sensitive Services. In the event that the Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

12.13 Confidentiality

The State may disclose to the Contractor written material or oral or other information that the State treats as confidential ("Confidential Information"). Title to the Confidential Information and all related materials and documentation the State delivers to the Contractor will remain with the State. The Contractor must treat such Confidential Information as secret if it is so marked, otherwise identified as such, or when, by its very nature, it deals with matters that, if generally known, would be damaging to the best interests of the public, other contractors or potential contractors with the State, or individuals or organizations about whom the State keeps information. The Contractor may not disclose any Confidential Information to third parties and must use it solely to perform under this Contract.

If any Deliverables contain data, documentation, or other written information that is confidential in nature and properly labeled as such, then it also will be Confidential Information for purposes of this section. The State will keep all such Confidential Information in confidence and will not use it other than as authorized under this Contract. Nor will the State disclose any such Confidential Information to any third party without first obligating the third party to maintain the secrecy of the Confidential Information.

If one party discloses Confidential Information ("Disclosing Party") to the other party to this Contract ("Receiving Party"), the Receiving Party's obligation to maintain the confidentiality of the Confidential Information will not apply where such:

- (1) Was already in the possession of the Receiving Party without an obligation of confidence;
- (2) Is independently developed by the Receiving Party, provided documentary evidence exists to support the independent development;
- (3) Except as provided in the next paragraph, is or becomes publicly available without a breach of this Contract;
- (4) Is rightfully received by the Receiving Party from a third party without an obligation of confidence;
- (5) Is disclosed by the Receiving Party with the written consent of the Disclosing Party; or
- (6) Is released under a valid order of a court or governmental agency, provided that the Receiving Party:
 - (a) Notifies the Disclosing Party of the order immediately upon receipt of it; and
 - (b) Makes a reasonable effort to obtain a protective order from the issuing court or agency limiting the disclosure and use of the Confidential Information solely for the purposes intended to be served by the original order of production.

Information that may be available publicly through other sources about people that is personal in nature, such as medical records, addresses, phone numbers, social security numbers, and similar things are nevertheless sensitive in nature and may not be disclosed or used in any manner except as expressly authorized in this Contract. Therefore, item (3) in the preceding paragraph does not apply, and the Contractor must treat such information as Confidential Information whether it is available elsewhere or not.

Except for Confidential Information that the Contractor delivers to the State and that is part of a Deliverable or necessary for the proper use or maintenance of a Deliverable, the Receiving Party must return all originals of any Confidential Information and destroy any copies it has made on termination or expiration of this Contract.

The disclosure of the Confidential Information of the Disclosing Party in a manner inconsistent with the terms of this provision may cause the Disclosing Party irreparable damage for which remedies other than injunctive relief may be inadequate, and each Receiving Party agrees that in the event of a breach of the Receiving Party's obligations hereunder, the Disclosing Party will be entitled to temporary and permanent injunctive relief to enforce the provisions of this Contract without the necessity of proving actual damages. However, provision does not diminish or alter any right to claim and recover damages.

12.14 Handling the State's Data

The Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State data are secure and to protect that data from unauthorized disclosure, modification, or destruction. The State's minimum standard is the NIST 800-53 moderate baseline. To accomplish this, the Contractor must:

- (1) Apply appropriate risk management techniques to ensure security for all sensitive data, including but not limited to any data identified as Confidential Information elsewhere in this Contract.
- (2) Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability.
- (3) Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as and detect and respond to those threats and vulnerabilities.
- (4) Maintain appropriate identification and authentication process for information systems and services associated with State data.
- (5) Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State data.
- (6) Implement and manage security audit logging on information systems, including computers and network devices.

The Contractor must maintain a robust boundary security capacity that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State data, limiting access to only these points, and disable all others. To do this, the Contractor must use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available. The Contractor must use two-factor authentication to limit access to systems that contain particularly sensitive State data, such as personally identifiable data.

Unless the State instructs the Contractor otherwise in writing, the Contractor must assume all State data is both confidential and critical for State operations, and the Contractor's security policies, plans, and procedure for the handling, storage, backup, access, and, if appropriate, destruction of that data must be commensurate to this level of sensitivity. As part of the Contractor's protection and control of access to and use of data, the Contractor must employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access the State's data, as well as attacks on the Contractor's infrastructure associated with the State's data. Further, the Contractor must monitor and appropriately address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State's data.

The Contractor must use appropriate measures to ensure that State's data is secure before transferring control of any systems or media on which State data is stored. The method of securing the data must be appropriate to the situation and may include erasure, destruction, or encryption of the data before transfer of control. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this Contract.

The Contractor must have a business continuity plan in place. The Contractor must test and update the IT disaster recovery portion of its business continuity plan at least annually. The plan must address procedures for response to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains the State's data in case of loss of that data at the primary site. The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State's data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the State's data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

The Contractor may not allow the State's data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this Contract properly and approved by the State's Chief Information Security Officer. Even then, the Contractor may permit such only if adequate security measures are in place to ensure the integrity and security of the data. Those measures must include a policy on physical security for such devices to minimize the risks of theft and unauthorized access that includes a prohibition against viewing sensitive or confidential data in public or common areas. At a minimum, portable computing devices must have anti-virus software, personal firewalls, and system password protection. In addition, the State's data must be encrypted when stored on any portable computing or storage device or media or when transmitted from them across any data network. The Contractor also must maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

Any encryption requirement identified in this provision must meet the Ohio standard as defined in Ohio IT standard ITS-SEC-01, "Data Encryption and Cryptography".

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State data and must report any loss or theft of such to the State in writing as quickly as reasonably possible. The Contractor also must maintain an incident response capability for all security breaches involving State data whether involving mobile devices or media or not. The Contractor must detail this capability in a written policy that defines procedures for how the Contractor will detect, evaluate, and respond to adverse events that may indicate a breach or attempt to attack or access State data or the infrastructure associated with State data.

In case of an actual security breach that may have compromised State data, including but not loss or theft of devices or media, the Contractor must notify the State in writing of the breach, or the suspicion of a breach, no more than within 24 hours of the Contractor becoming aware of the breach, and fully cooperate with the State to mitigate the consequences of such a breach. This includes any use or disclosure of the State data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this Contract by an employee, agent, or subcontractor of the Contractor.

The Contractor must give the State full access to the details of the breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate. The Contractor must document all such incidents, including its response to them, and make that documentation available to the State on request. In addition to any other liability under this Contract related to the Contractor's improper disclosure of State data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity whose personally identifiable information is compromised while it is in the Contractor's possession. Such identity theft protection must be reasonably acceptable to the State.

All State Data will remain the property of the State. The Contractor must ensure that the State retains access and download capability for purposes of retrieving its data for research, investigation, transfer, or migration to others systems.

12.14.1 Return of State Data

The Contractor may use Confidential Information only as necessary for Contractor's performance under or pursuant to rights granted in this Agreement and for no other purpose. The Contractor's limited right to use Confidential Information expires upon expiration or termination of this Agreement for any reason. The Contractor's obligations of confidentiality and non-disclosure survive termination or expiration for any reason of this Agreement.

12.14.2 Confidentiality Agreements

When the Contractor performs services under this Contract that require the Contractor's and its subcontractors' personnel to access facilities, data, or systems that the State, in its sole discretion, deems sensitive, the State may require the Contractor's and its subcontractors' personnel with such access to sign an individual acknowledgement of data handling responsibilities, and have a background check performed before accessing those facilities, data, or systems. Each State agency, board, and commission may require a different confidentiality agreement or acknowledgement, and the Contractor's and its subcontractors' personnel may be required to sign a different confidentiality agreement or acknowledgement for each agency. The Contractor must immediately replace any of its or its subcontractors' personnel who refuse to sign a required confidentiality agreement or acknowledgment or have a background check performed.

Supplement 3

Cloud Computing Guidelines Document

Supplement 4

SOCC Policy Receipt Acknowledgement

State of Ohio Computing Center
Policy Receipt Acknowledgement

I, _____, acknowledge that on _____ I received
(printed name) (date)
the following policies, standards and IT Bulletins. All State of Ohio Enterprise policies, standards and bulletins are available online at:

<http://das.ohio.gov/Divisions/InformationTechnology/StateofOhioITPolicies/tabid/107/Default.aspx>

Department of Administrative Services (DAS) policies are available at
<http://das.ohio.gov/Divisions/DirectorsOffice/EmployeeServices/DASpolicies/tabid/463/Default.aspx>

Any questions relating to these policies should be directed to the OIT Security Operations Team:

**Enterprise Policies, Standards and
Bulletins: Policy No.**

Policy Name

ITB-2007.02	Data Encryption and Securing Sensitive Data Bulletin
ITB-2007.01	Electronic Communication and Public Records
ITS-SEC-01	Data Encryption and Cryptography Standard
ITS-SEC-02	Enterprise Security Controls Framework
ITP-A.26	Software Licensing
ITP-E.1	Disposal, Servicing and Transfer of IT Equipment
ITP-E.8	Use of Internet, E-mail and Other IT Resources
ITP-E.30	Electronic Records
ETP-H.2	Use of State Telephones