

State of Texas

Department of Information Resources



Attachment 1.1

Deliverables

Security Operations Services

DIR-SECOPS-MSA-434

September 4, 2020

Overview	
This document includes all Deliverables required throughout the RFO and Respondent response, including any and all Transition Deliverables with verifiable criteria for acceptance.	
Definitions of Fields	
Reference Number	Unique identifier
Name	Name of the Deliverable
Source	Note the document and document section
Description	Description of the activities comprising the Deliverable
Minimum Acceptance Criteria	Description of Acceptance Criteria that will indicate completion of the milestone or Deliverable.
Critical (C) or Payment (P)	As outlined in Exhibit 1, Table 1 Terms and Definitions
Due Date (mm/dd/yy)	Date when the Deliverable will be completed in mm/dd/yy format.

Change Log			
CCR/CN	Amendment	Date	Description
CCR 382	N/A	3/31/2020	Date revisions, acceptance criteria reference clarifications and administrative changes for One-time deliverables
CCR 413	N/A	8/14/2020	"One-Time Deliverables" tab: due date revision for "Phase 2 Transition Milestones complete"
CCR XXX	N/A	9/4/2020	"Recurring Deliverables" tab: added language for Financial Forecast “, or as other such time as mutually agreed to.” to update Due Date for Financial Forecast, Deliverable ID# FF-SECOPS-001, from 10/1/2020 to 12/1/2020, to align with revised due date for the MSI Contract parent deliverable to allow for additional data to be incorporated due to the Next Generation DCS contracts commencing on September 1, 2020.

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)	Proposed # of deliverable reviews
1.1	Transition Project Plan	The document will include the SR's transition tasks and activities necessary to successfully migrate all applicable Services from the current Contract.	<p>The Transition Project Plan must include a detailed task/activity level for the planned Transition period, inclusive of activities and named resources engaged by the Successful Respondent and all roles with effort hours required for DIR and/or current SCP(s). The Transition Project Plan must also propose for DIR consideration, a proposed schedule of regular status meetings with DIR to ensure DIR remains informed on the status of all Transition activities. DIR may also request additional status updates outside of the regularly scheduled meetings at their discretion. The Transition Project Plan must be maintained by the Successful Respondent on an ongoing basis through Transition and made available on a DIR-provided document collaboration site to all DCS stakeholders associated with the Transition of the Service. The Transition Project Plan must include an updated Staffing Plan (for the Successful Respondent's resources and MSI, SCPs, and DIR resources that are required to participate in the work including Successful Respondent-related activities). The Staffing Plan must include the number of resources by role for the high-level tasks. Additionally, the Successful Respondent must also provide an inventory of required DIR resources needed by task and role. The Detailed Transition Project Plan (for both the Response and Critical Deliverable) must also include at a minimum the following:</p> <ol style="list-style-type: none"> 1. Project Integration – among DIR, reliant or dependent DCS SCPs, and DCS Customers; 2. Stakeholder goals and expectations; 3. Project Scope; 4. Project Time; 5. Project Schedule Management Plan; 6. Project Change Management; 7. Project Quality Measures and Management Plan; 8. Project Staffing; 9. Project Communications; 10. Plan for validating inventory, and implementing automated discovery tools for tracking and reporting on all operational hardware, software, appliances, etc., on supported Service elements and devices; 11. Plan and associated timelines for developing Application Programming Interfaces (APIs) and other system integrations to support automated reporting, data feeds, etc., into the MSI tools, including any know interdependencies or resource requirements for MSI, DIR, or other SCPs; 12. A description of the documentation, methods and procedures, personnel and organization the Successful Respondent will use to perform the Transition; 13. Any other information and planning artifacts as are necessary such that the Transition takes place on schedule and without disruption to DCS Customer operations; 14. A definition of completion criteria for each phase of the Transition Plan, with required specificity such that all Parties may 	Yes	Yes	Effective Date +35 Days	3
1.2	Operational Readiness Assessment	The SR will provide documentation to support its readiness to operate and maintain the functionality deployed and recommend strategies to ensure DIR, DIR customers, and DCS SCPs are prepared to support any new system functionality	<p>Confirmation of integration with MSI and other SCPs as required Documentation of required 4 reviews conducted with DIR prior to final submission. Confirmation of alignment with MSI processes/procedures in the SMMs and identification of any critical gaps in documentation or processes Updated Key Personnel contact information and staff employment status Documented operational processes/procedures needed to deliver Services and status of publication on the MSI portal Status of Software license transfers or purchases Status of hardware transfers or purchases Status of lease transfers Billing process including detail for invoices Status of operating agreements between the Successful Respondent and the MSI and Service Component Providers (SCPs) Confirmation of successful testing of network Knowledge transfer programs</p>	Yes	Yes	Commencement Date -30 Days	4

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)	Proposed # of deliverable reviews
1.3.1	SMM Documentation Phase I	The SR will document appropriate policies, processes, and procedures for inclusion in the SMM.	<p>Publication of a .doc document that describes how the SMM requirements will be satisfied:</p> <ul style="list-style-type: none"> - Structure and hierarchy - Document templates - Descriptions of contents for SMM implementation phases I-III <p>Documentation of required 1 review conducted with DIR prior to final submission.</p> <p>Publication of required Phase I SMM sections as defined in Attachment 4 SMM Content and Organization</p> <ul style="list-style-type: none"> • SMM content aligned with SMM Phase I contents and structure • Processes reflect the requirements of the Agreement • Detailed descriptions of policies, processes, and procedures are documented in the manual. • Roles and responsibilities are defined for Respondent, MSI, DIR, other SCPs, and/or DIR Customers as appropriate. • Dependencies and relationships are documented. • Risks associated with procedures are identified and mitigation strategies documented for each risk. • The policies and procedures are consistent with the proposed project approach 	Yes	yes	Effective Date +35 Days	2
1.3.2	SMM Documentation Phase II	The SR will document appropriate policies, processes, and procedures for inclusion in the SMM.	<p>Publication of a .doc document that details the processes support the SMM requirements:</p> <ul style="list-style-type: none"> - Roles and responsibilities - Inputs and outputs - Navvia tool in place with Service Management SMMs loaded - Published UAT results confirm SMM is performing as expected, in accordance with the SMM requirements, and contains the expected content <p>Documentation of required 2 reviews conducted with DIR prior to final submission.</p> <p>Publication of required Phase II SMM sections as defined in Attachment 4 SMM Content and Organization</p> <ul style="list-style-type: none"> • SMM content aligned with SMM Phase II contents and structure • Processes reflect the requirements of the Agreement • Detailed descriptions of policies, processes, and procedures are documented in the manual. • Roles and responsibilities are defined for MSI, SCPs, DIR, and/or DIR Customers as appropriate. • Dependencies and relationships are documented. • Risks associated with procedures are identified and mitigation strategies documented for each risk. • The policies and procedures are consistent with the proposed project approach 	Yes	Yes	Commencement -10 Days	2
1.3.3	SMM Documentation Phase III	The SR will document appropriate policies, processes, and procedures for inclusion in the SMM.	<p>Publication of a .doc document with:</p> <ul style="list-style-type: none"> - the summary of the Phase III scope - the hyperlinks to SMM artifacts in the SMM repository - the screenshots from SMM repository on how to navigate and to find the SMM artifacts <p>Documentation of required 2 reviews conducted with DIR prior to final submission.</p> <p>Publication of required Phase III SMM sections as defined in Attachment 4 SMM Content and Organization</p> <ul style="list-style-type: none"> • SMM content aligned with SMM Phase III contents and structure • Processes reflect the requirements of the Agreement • Detailed descriptions of policies, processes, and procedures are documented in the manual. • Roles and responsibilities are defined for MSI and DIR, SCP, and/or DIR Customers as appropriate. • Dependencies and relationships are documented. • Risks associated with procedures are identified and mitigation strategies documented for each risk. • The policies and procedures are consistent with the proposed project approach 	Yes	Yes	Commencement +60 Days	2

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)	Proposed # of deliverable reviews
1.4	Master Security Baseline Configuration (MSBC) Standards	A set of extensible DCS Enterprise standards for the specification and use of security standards pertaining to DCS	<p>Meet the MSBC requirements of Exhibit 1 and provide: Publication and agreement on MSBC standards as captured in a .docx document that describes the intended scope of design for the Master Security Baseline Standards including:</p> <ul style="list-style-type: none"> - Documented proof of required 1 review conducted with DIR and MSI prior to final submission (March 15 HLD). - Conduct workshop with MSI to review existing MSBC process and standards - Review and update MSBC related SMM process documentation including current design standards, documented system security plan as well as the ITIL based service design, incident, problem and change management process documents - Develop plan to transfer current MSBC remediation plans to SecOps by Commencement including defining the activities and schedule to re-align remediation plans with respective SCPs - Define plan to develop comprehensive documentation detailing security-related configurations necessary for all SCPs to set on all in-service platforms (hardware, software, and services) in order to meet the TAC 202 Controls Catalog, organized by platform, with a crosswalk of the configurations to the control(s). - Compile a listing of cryptographic modules, ciphers, and other commonly used technologies or standards that are no longer considered secure and should not be utilized in the DCS program. 	Yes	No	Commencement + 180 Days	TBD
1.5	Vulnerability Management Program Design		<p>Publication and agreement on the Vulnerability Management Program captured in a SMM document that includes:</p> <ul style="list-style-type: none"> - Purpose and scope - Policy, process, and procedures including: <ul style="list-style-type: none"> - Procedures to identify and report on active threats and security vulnerabilities, provide status on all actions (resolved and open), provide results of remediated items, and schedules, dependencies, activities that address remaining open security actions. - Vulnerability Program Governance including process for SecOps to manage SCP vulnerability remediation activities - Integration points into DIR and SCP functions (e.g. Technology planning, Reference Architecture and Roadmaps, Automation, etc.) <p>Publication and agreement on the Vulnerability Management plan captured in a .docx and .mpp document that includes:</p> <ul style="list-style-type: none"> - Phase 1 objectives, success criteria, and schedule - identifies SCP, MSI dependencies - Additional phase 2 activities identified 	Yes	No	June 1, 2020	TBD
1.6	Security Incident Management Design		<p>Publication and agreement on the Security Incident Management Program captured in a SMM document that includes:</p> <ul style="list-style-type: none"> - Purpose and scope - Policy, process, and procedures including: <ul style="list-style-type: none"> - Procedures to identify and remediate security incidents, provide status and communications of remediation progress, provide results of remediated items, and post-incident remediation activities. - Security Incident Program Governance including process for SecOps to manage security incidents - Dependencies and integration points (e.g. MSI MIM integration, Security incident communications, etc.) <p>Publication and agreement on the Security Incident Management plan captured in a .docx and .mpp document that includes:</p> <ul style="list-style-type: none"> - Phase 1 objectives, success criteria, and schedule - identifies SCP, MSI dependencies - Additional phase 2 activities identified 	Yes	No	June 1, 2020	TBD

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)	Proposed # of deliverable reviews
1.7	Advanced Malware Protection Standards		<p>Publication and agreement on Advanced Malware Protection standards as captured in a .docx document that describes the intended scope of design for Advanced Malware Protection including:</p> <ul style="list-style-type: none"> - Documented proof of required 2 reviews conducted with DIR prior to final submission (April 15, May 15). - Perform and document technical capability assessment to define a DCS specific controls baseline environments - Document gap analysis and remediation plan based on comparison of the defined baseline against capabilities of DCS's deployed technologies to satisfy baseline control requirements, identify gaps, and propose recommendations to close those gaps - Perform broad assessment to identify the current baseline of policies, procedures, standards and regulations - Document gap analysis and remediation plan based on compliance requirements that ensure the current DCS operations are compliant, current and effective - Provide recommended standards for SecOps other SCPs and MSI for DCS Security Governance ratification 	Yes	No	June 1, 2020	TBD
1.8	Publish CASB Standards and SMM		<p>Publication of a .doc document that details the processes support the SMM requirements: DIR written acceptance of CASB Approach and Enterprise Design Standard (RN#19)</p> <ul style="list-style-type: none"> - Roles and responsibilities - Inputs and outputs - CASB standard including reference architecture, system security plan, and requirements document to aid CASB solution selection <p>Documentation of required 2 reviews conducted with DIR prior to final submission.</p> <p>Publication of CASB SMM</p> <ul style="list-style-type: none"> • SMM content aligned with SMM Phase II contents and structure • Processes reflect the requirements of the Agreement • Detailed descriptions of policies, processes, and procedures are documented in the manual. • Roles and responsibilities are defined for SecOps, MSI, SCPs, DIR, and/or DIR Customers as appropriate. • Dependencies and relationships are documented. • Risks associated with procedures are identified and mitigation strategies documented for each risk. • The policies and procedures are consistent with the proposed project approach 	Yes	Yes	June 1, 2020	TBD
1.9	Phase 2 Project Plan Complete		<p>The detailed Phase 2 Project Plan must include:</p> <p>Detailed task/Work Breakdown Structure for Phase 2 initiatives, inclusive of all activities, deliverables, dependencies</p> <p>Risk Register</p> <p>Project Integration – among DIR, reliant or dependent DCS SCPs, MSI and DCS Customers;</p> <p>Stakeholder goals and expectations;</p> <p>Project Scope; Project Time; Project Quality Measures and Management Plan; Project Staffing Plan;</p> <p>Plan and associated timelines for developing APIs and other system integrations to support automated reporting, data feeds, etc. into the MSI tools, including any known interdependencies or resource requirements from MSI, DIR, or other SCPs.</p> <p>Any other information and planning artifacts as are necessary such that the Phase 2 project takes place on schedule and without disruption to DCS Customer operations</p>		No	Commencement Date -30 Days	TBD

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)	Proposed # of deliverable reviews
1.10	CyberArk Handover from Atos		<p>Conduct project review and assessment with TPC in April. Review project scope, licensing structure/model, project progress, plan to completion, risks, and dependencies.</p> <ul style="list-style-type: none"> - Review as-built, design, and related documentation including architecture, data model, data flow, project, and operational support documents - SecOps to provide gap analysis {deployed PAM solution} vs. SecOps SOW requirements. - Validate timing and process to provision read-only access to CyberArk and McAfee (Access includes the ability to assess configurations including SIEM rules, CyberArk utilization and profiles, and any customizations made for the DCS environment) - any other tools? <p>Documented proof of required 3 joint sessions and reviews conducted with TPC, DIR, MSI as required prior to final submission (June 1, July 6, Aug 3) resulting in:</p> <ul style="list-style-type: none"> - Documented plan for project handover from TPC to SecOps including access to environment, license transfer/assignment, and knowledge transfer. - Remediation plan to close functionality or scope gaps identified in the gap analysis above as scheduled in Phase 1 or Phase 2. - Facilitate JAD session to validate hardware and networking requirements and required transition - Validate alignment with DIR and TPC concerning Active Directory integration and policy requirements - Documented RACI for priv account management across SCPs and MSI <p>Provide the following:</p> <ul style="list-style-type: none"> - Documented proof of completed Assignment of maintenance and licenses from incumbent - Provide KT Scorecard. The KT Scorecard is a spreadsheet consisting of a punch list of all knowledge transition topics for each functional service. - Documented approval from SecOps SCP confirming system access, license transfer/assignment, and KT complete in accordance with scheduled approved in TPC RN#41. 	Yes	No	Commencement Date	TBD
1.11	SIEM Phase 1 Service Implementation		<p>DIR written Acceptance of Transition milestones: SIEM Integration Approach (RN# 5), Design (RN#9), Build/Deploy (RN#11) and Testing (RN#17), SIEM Tuning and Operational Readiness (RN#25);</p> <ul style="list-style-type: none"> - All remaining test defects resolved or DIR approved business workaround 	Yes	Yes	Commencement Date	TBD
1.12	Phase 1 Transition Milestones complete		<p>The submission of this deliverable is confirmation by the parties that all interim and major milestones, due to be completed according to the July 2020 monthly baseline schedule, are both submitted by SCP and accepted by DIR in writing in accordance with Acceptance Criteria defined in the Transition Milestone document following the transition governance framework and process.</p>	Yes	Yes	Commencement Date + 20 days	TBD
1.13	Service Automation Approach and Phase 2 Plan		<p>Publication and agreement on Service Automation opportunities and implementation plan as captured in a .docx document that describes the intended scope and implementation plan for Service Automation including:</p> <ul style="list-style-type: none"> - Documented proof of required 2 reviews conducted with DIR prior to final submission July 15, Oct 15). - Integration approach and project dependency checkpoint (MSI, TPC, PCM, MF) - Automation goals and desired outcomes including but not limited to: <ul style="list-style-type: none"> - PAM solution integration - SCP priv access account integration and service request automation in ServiceNow - SIEM alert correlation and remediation - Automated threat analysis models - Identify functional service areas to be automated with desired outcomes - Detail tooling integration requirements - Identify methods of automation - Process Changes that reflect the responsibilities of SecOps and other SCPs - Process Changes that outline the touchpoints with DIR Customers - Process Changes that outline the integration points with the MSI 	Yes	No	Commencement Date + 90 days	TBD
1.14	PAM Phase 2 Service Implementation		<p>DIR written Acceptance of PAM Phase 2 Approach (RN#30), Design (RN#31), Build/Deploy (RN#34) and Testing (RN#35)</p> <ul style="list-style-type: none"> - All remaining test defects resolved or DIR approved business workaround 	Yes	No	1/15/21	TBD
1.15	Phase 2 Transition Milestones complete		<p>The submission of this deliverable is confirmation by the parties that all interim and major milestones, due to be completed according to the TBD monthly baseline Phase 2 schedule, are both submitted by SCP and accepted by DIR in writing in accordance with Acceptance Criteria defined in the Transition Milestone document, following the transition governance framework and process.</p>	Yes	No	5/1/2021	TBD

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)
2.1	Annual Technology Plan and Roadmap	<p>TSS, with the support of the Respondent and other SCPs, shall complete a Technology Plan and Roadmap for each DIR Shared Service on July 15th of each calendar year or as such time as mutually agreed to by DIR and the Successful Respondent. The Technology Plan shall include unique DIR Customer plans as appendices. The Technology Plan will be the basis for generation of technology roadmaps which will include schedules, dependencies, and requirements for introduction of new technology changes as well as acquisition, support, and retirement of software and hardware. The Technology Plan will specify the solutions, plans, cost estimates, and schedules for achieving Technology Evolution goals for DIR Shared Services and Services.</p> <p>TSS, with the support of the Respondent and other SCPs, shall manage ongoing updates to the Technology Plan as the Technology Roadmap to include proposed updates to reference technical architecture and software currency designations. The Roadmap will identify specific, short-term steps and schedules for projects or changes with estimated timing for DIR and DIR Customers.</p> <p>The Successful Respondent shall develop and implement a Technology Plan that is consistent with DIR's strategic planning and shows how the Successful Respondent and SCPs will provide the Services to enable DIR and DIR Customers to achieve technology evolution, efficiencies, productivity improvements, cost savings, modernization, and enhanced security, etc.</p>	<p>Provide TSS with the Successful Respondent's Technology Plan and Roadmap in the required format, to be included in the complete Technology Plan and Roadmap deliverable submission to DIR.</p> <p>Publication and agreement on the Annual Technology Plan and Roadmap as captured in a .docx document and ServiceNow PPM that includes:</p> <ul style="list-style-type: none"> - Output from the Annual Technology Summit - Schedules, dependencies, and requirements for introduction of new technology changes into the DCS environment including the acquisition, support, and retirement of software and hardware. These plans include views at the enterprise and DIR Customer levels. - Specification of the solutions, plans, cost estimates and schedules for achieving Technology Evolution goals for DCS 	Yes	No	July 15th Annually
2.2	Annual Refresh Plan	<p>The Successful Respondent, through the MSI, shall deliver annually on January 15th or at such time as mutually agreed to by DIR and Successful Respondent, a Refresh Plan that addresses Refresh for all Equipment and Software for which a Refresh cycle is provided in Attachment 2 Financial Responsibility Matrix for the Successful Respondent.</p> <p>As a part of the Refresh plan, the Successful Respondent shall provide a recommendation to upgrade Software to supported levels and to Refresh Equipment in accordance with the Technology Plan and Technology Roadmap.</p> <p>Following the initial Refresh plan, the Successful Respondent shall include, in subsequent Refresh Plans, a report describing the Refresh status of all Equipment and Software included in the Refresh plan.</p>	<p>Provide the MSI with the Successful Respondent's Annual Refresh Plan in the required format, to be included in the complete Annual Refresh Plan deliverable submission to DIR.</p> <p>Publication and agreement on the Annual Refresh Plan captured in a .docx document and ServiceNow PPM that includes:</p> <ul style="list-style-type: none"> - Refresh forecast eligibility, dependencies, and recommendations for refreshing technology (hardware and software) in the Private Cloud Services environment for the upcoming year. These plans include views at the enterprise and DIR Customer levels. - Preliminary business-level assessment of the solutions, plans, cost estimates, and schedules for achieving Refresh goals (including software to n/n-1 levels) for Services. - A report identifying all refresh performed in the prior calendar year 	Yes	No	January 15th Annually
2.3	Quarterly Refresh Plans	<p>The Successful Respondent, with the support of the SCPs, will deliver quarterly updated Refresh Plans and refresh completion reports as deliverables demonstrating SCP progress toward attaining refresh goals identified in the plan.</p>	<p>Publication and agreement on the Quarterly Refresh Plan and Refresh completion reports captured in a .docx document and ServiceNow PPM that includes:</p> <ul style="list-style-type: none"> - Refresh forecast eligibility, dependencies, and recommendations for refreshing technology (hardware and software) in the Security Services environment for the upcoming year. These plans include views at the enterprise and DIR Customer levels. - Preliminary business-level assessment of the solutions, plans, cost estimates, and schedules for achieving Technology Refresh goals (including software to n/n-1 levels) for Services. - A report identifying all refresh performed in the prior calendar year 	No	No	Quarterly
2.4	Annual Security Plan	<p>Support the MSI in the publication of Annual Security Plan as defined in Exhibit 1</p>	<p>Support the MSI with their creation and publication and agreement on of the Annual Security Plan as described in Exhibit 1 and captured in a .docx document and draft ServiceNow PPM that includes:</p> <ol style="list-style-type: none"> 1. Draft schedules, dependencies, and recommendations that address security improvements, including new services and industry best practices correlated to the annual security plan roadmap for the DIR Shared Services environment for the upcoming year including, any DCS cloud environments, Consolidated Data Center and other facilities as applicable, software and equipment deployment specifically for data and online security, annual security assessment findings, and other standard security concepts. 2. Security Operations SCP provided Input from the annual MSBC. 3. Business-level specification of the solutions, plans, cost estimates, and schedules for achieving Security goals for DIR Shared Services and MSI Services. 4. Summary of performance vs. preceding year's Security Plan. 5. Summary of results from previous year's security monitoring and measuring. 6. Identify and recommend any changes in Security Scope, Policy, Standards, Reference Architectures, Roles, Responsibilities, Activities, or systems and tools. 7. Recommendations for investments and initiatives to improve the overall Security of the Program. 	Yes	No	October 1st Annually

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)
2.5	Security Assessment Remediation Plan & Schedule	<p>Monthly, the Successful Respondent will provide all remediation plans and associated schedules for any Assessment conducted pursuant to the Statement of Work.</p> <p>The Successful Respondent's remediation plans and schedules should include remediation activities for all identified risks and vulnerabilities, in accordance with the standards provided in the Statement of Work for those actions within the Successful Respondent's systems. The Successful Respondent will monitor and report the status of all SCPs' remediation activities to ensure timely completion.</p>	<p>Publication and agreement on the Security Assessment Remediation Plan and Schedule as describe in Exhibit 1 and captured in a .docx document and tracked via a ServiceNow Project PPM that includes:</p> <p>Track and remediate security risks as identified in all Assessments conducted in the DCS environment</p> <ul style="list-style-type: none"> - Provide analysis of the results from the assessment(s) that identifies security gaps and determines which issues must be remediated and make recommendations to DIR for tools, processes, and long-range planning improvements - Report on agreed remediation actions and status of all actions (resolved and open) - Provide documented results of remediated items - Provide schedules, dependencies, and activities that address remaining open security actions to 	Yes	No	Quarterly
2.6	Annual Vulnerability & Remediation Report	<p>The Successful Respondent, via the MSI, shall deliver an Annual Vulnerability Report in accordance with the Statement of Work. The Successful Respondent shall provide to the MSI all vulnerability information, scan results, risk assessments, etc., that identify potential security vulnerabilities or risks in DIR's environments. The Successful Respondent shall evaluate vulnerabilities and recommend to DIR mitigation strategies for either DIR Customers or SCP to implement. Any Customer findings from these activities shall be timely parsed out Customer by Customer and communicated to the individual Customer cybersecurity teams so as to enable a response. The Successful Respondent shall report via the MSI relevant data trends each year and evaluate trend direction with suggested risk mitigation strategies.</p>	<p>Provide the MSI with the Successful Respondent's portion of the Annual Vulnerability Report in the required format, to be included in the complete Annual Security Plan deliverable submission to DIR.</p> <p>Publication and agreement on the Annual Vulnerability Report captured in a .docx document that includes:</p> <ul style="list-style-type: none"> - List of Service Providers (SCPs and MSI) required to run vulnerability scans - Proof scans were run and vulnerabilities were reported to the associated SCP and DIR Customer(s) - Proof scans were provided by the SCP directly to the DIR Governance, Risk and Compliance (GRC) tool - A status update of closed and open identified vulnerabilities and risk mitigation actions - Proof that on a quarterly basis, a review of all users assigned access to SCP systems was performed and access confirmed - A forward-looking schedule for the planned Security vulnerability testing, assessments and 	Yes	No	March 1st Annually
2.7	Service Management Manual Currency - Quarterly Report	<p>The Successful Respondent will comply with the MSI's established annual schedule for reviewing and updating the SMM. The Successful Respondent shall support the MSI in providing a quarterly report of the review findings which demonstrates the currency and accuracy of the SMM sections reviewed in that quarter. At the beginning of each calendar year, MSI will provide a schedule for the year that outlines the sections of the Service Management Manual that will be reviewed in each quarter. The MSI's schedule may be modified throughout the year per mutual agreement with DIR. The Successful Respondent shall provide content and updates according to the MSI's timeline to ensure SMM validity and currency.</p>	<p>Publication of the SMM review plan for the upcoming four quarters and report on the findings and updates made in the most recent quarter, including:</p> <ul style="list-style-type: none"> - SMM review plan, agreed by DIR, by topics (e.g., sections, processes or functional area) with timeline and participants. Plan is to include a listing of all documents or content included in the review (e.g., policies, processes, procedures, work instructions, templates). - Report of the review findings and updates made over the previous quarter. 	Yes	No	Quarterly
2.8	Annual Customer Satisfaction Improvement Plan	<p>Three (3) months after the results of the annual Customer Satisfaction Surveys are available, the Successful Respondent shall provide an improvement plan to measure the applicable improvement of the Services identified in the Customer Satisfaction Surveys as requiring improvement. The Successful Respondent shall work with MSI and other SCPs as appropriate to create improvements for each Service requiring improvement. The Customer Satisfaction Improvement Plan shall be approved by DIR and reported against by the MSI monthly or such other time as required by DIR.</p>	<p>Provide the MSI with the Successful Respondent's portion of the Annual Customer Satisfaction Improvement Plan in the required format, to be included in the complete Annual Customer Satisfaction Improvement Plan deliverable submission to DIR.</p> <p>Publication of the Customer Satisfaction improvement plan, including:</p> <ul style="list-style-type: none"> - Action plans addressing issues identified in the previous survey across all Services and survey groups. - Definitions of the issue being addressed, targeted improvement, timeline, owners, and solution approaches. - Previously agreed SCP actions and activities. - Plans should be approved by DIR - Previous plan to have been reported against by the MSI monthly or such other time as required by 	Yes	No	June 1st Annually
2.9	Disaster Recovery Test Plan and Schedule	<p>The MSI shall develop and provide a consolidated disaster recovery test plan and schedule in accordance with the approach outlined in the Statement of Work. The disaster recovery test plan and schedule shall be updated annually thereafter. The Successful Respondent is responsible for participating in any disaster recovery exercises planned by the MSI and providing any needed information for the disaster recovery test plan and schedule.</p>	<p>Publish .doc/.xls document(s) that describes the Annual Disaster Recovery Test Plan and Schedule including:</p> <ul style="list-style-type: none"> - New schedule developed for the upcoming year inclusive of RTO/RPO for each system/application - Identifies major changes in requirements and new applications since the previous year's test - Report contains the list of eligible applications per customer not scheduled for testing - After approval, publish DR test plan and schedule - A narrative evaluation of the previous years' testing against the DR program objectives to determine areas of risk, indicating any DR program or process changes to be incorporated in the next years' test plan schedule. 	Yes	No	June 1st Annually

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)
2.10	Financial Forecast	Semi-annual forecast of Successful Respondent and SCP Charges and usage trends by Service (aligned with the State's fiscal year). The forecast must be inclusive of all Successful Respondent and SCP volumes and Charges, including Projects, New Services, and forecasted DIR Customer volume and Charge changes required to support their budgeting process. The forecast must include all known and expected changes captured as part of the Technology Plan and Capacity Management processes.	Provide the MSI with the Successful Respondent's portion of the Financial Forecast in the required format, to be included in the complete Financial Forecast deliverable submission to DIR. Submit .xlxs document with: data, methodology, charges and volume views, rate data and calculations Inclusive of information gained from Refresh Plan, Triage, Consolidation, Technology Plan, Capacity Planning, New/Special Projects, Transition Charges, HSC, SSC, New Services, and Co-Location Services.	Yes	No	Semi-annually on April 1st and October 1st, or as other such time as mutually agreed to.
2.11	DIR Shared Services Annual Review	Complete an Annual Review for each Security Operations Service in October of each calendar year.	The Annual Review shall contain the actual service volumes against the forecasted monthly volume for the previous year, and forecasted service volumes for the next year. In addition, the review shall contain: (i) whether the Charges are consistent with DIR's forecasts and industry norms; (ii) the quality of the performance and delivery of the Services; (iii) whether the Successful Respondent or SCPs have delivered cost saving or efficiency enhancing proposals; (iv) the level and currency of technologies and processes employed; (v) the operations and technology strategy and direction; (vi) whether the Successful Respondent and SCP Service Levels are achieving the desired outcome (including continuous improvement updates, more efficient measurement methodologies, modification, additions and deletions of services levels to align with strategy, and the Metric Inclusions and Data Sources for the Data Quality SLA), and (vii) such other things as DIR may reasonably require.	No	No	Annually on October 1st
2.12	Annual Cybersecurity Assessment	At DIR's sole discretion this Cybersecurity Assessment of the Security Program may be conducted by the Successful Respondent, DIR or, a third-party security assessment SCP (the "Security Assessment Company") through the Managed Security Services program. The assessment will address strengths, challenges, opportunities and direction with regard to protecting the State enterprise from Cyber threats. The assessment will serve as input to continuous improvement of DCS security. Following the assessment, the Successful Respondent will perform a fit/gap analysis using State capabilities and industry best practices to identify a multi-year strategy and plan to enhance the State's capabilities in response to ongoing evolutions in the Cyber-threat detection, mitigation and response.	(At DIR's Request) 1. Perform a Cybersecurity Assessment that meet the requirements described in Exhibit 2. Established Maturity and Risk Rating for the DCS environment from the assessment results including: a. Maturity and Risk Rating based on Texas Administrative Code 202, National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF) and COBIT 5 for Information Security Models b. Highlight successes and identify gaps based on CSF target maturity of "Implemented" or level 3 c. Security maturity comparison against similar organizations (public sector) and similarly sized organizations d. Rank criticality of gaps (For Cybersecurity Assessments performed, either by Successful Respondent or another party) e. Recommend mitigation solutions f. Estimated timing and criticality requirements for mitigation deployment and ongoing support g. Estimated deployment timelines 3. Identification of any security/privacy risks in current practices based on Annual Assessment, including with respect to: a. Organizational/Personnel (Skill/Knowledge Level) b. Policy/Process/Procedures c. Tools, Methods, Implementation and Operations specific Issues d. Access, implementation of NIST, industry/best practices e. Dependencies between State Security and DCS Customers as well as DCS service providers Detailed recommendation to close gaps identified in the Assessment	Yes	No	TBD
2.13	Annual SOC 2, Type II, Report	Annual report to evaluate an organization's information systems that are relevant to security, availability, processing integrity, confidentiality or privacy. The criteria for these engagements are contained in the Trust Services Principles, Criteria and Illustrations.	The report must be performed according to the requirements set out in Exhibit 1, section 3.22.1. SOC 2 Reports	No	No	Annually December 31
2.14	Master Security Baseline Configuration (MSBC)	Document defining the security configurations and technical control settings and standards as agreed to by DIR and required of the SCPs.	1. Updated MSBC as described in Exhibit 1 that includes: a. Comprehensive documentation detailing configurations necessary for all SCPs to set on all in-service platforms (hardware, software, and services) in order to meet the TAC 202 Controls Catalog, organized by platform, with a crosswalk of the configurations to the control(s). b. A listing of cryptographic modules, ciphers, and other commonly used technologies or standards that are no longer considered secure and should not be utilized in the DCS program.	No	No	Annually August 1 or next business day

Reference ID	Deliverable Name	Description	Minimum Acceptance Criteria (Specific, Measurable, Timebounded Outcomes)	Critical (C)	Payment Deliverable (to be determined during Negotiations)	Due Date (mm/dd/yy)
2.15	Quarterly Tech Plan and Roadmap	The Successful Respondent, in support of TSS, will deliver quarterly updated Tech Plans and Roadmap reports as deliverables demonstrating SCP progress toward attaining goals identified in the plan as well as variances from standards.	Publication and agreement on the Quarterly Technology Plan and Roadmap as captured in a .docx document and ServiceNow PPM that includes: - Output from the Annual Technology Summit - Schedules, dependencies, and requirements for introduction of new technology changes into the DCS environment including the acquisition, support, and retirement of software and hardware. These plans include views at the enterprise and DIR Customer levels. - Specification of the solutions, plans, cost estimates and schedules for achieving Technology Evolution goals for DCS.	No	No	Quarterly
2.16	Annual Automation Plan	The Successful Respondent, with support of TSS and other SCPs, shall complete an Automation Plan for each Security Operations service on July 15th of each calendar year or as such time as mutually agreed to by DIR and the Successful Respondent. The Automation Plan will be the basis for process and tooling automation to eliminate events as well as automation of service restoration activities.	Publication and agreement on the Annual Automation Plan captured in a .docx document and ServiceNow PPM that includes: - Analysis of event and incident patterns with associated planning for continued improvements and measurements of success of previous automation execution. - Automation opportunities and recommendations for process and technology automation in the Security Operations Services environment for the upcoming year. These plans include views at the enterprise levels. - Report on targets from previous plans with overall success and impacts to the environment. - Be consistent with DIR's strategic planning and shows how the Security Operations Services will enable DIR and DIR Customers to achieve technology evolution, efficiencies, productivity improvements, cost savings, modernization, and enhanced operations, etc.	Yes	No	Annually on July 15
2.17	Semi-Annual Automation Plan	The Successful Respondent, in support of TSS, will deliver quarterly updated Automation Plans demonstrating Security Operations SCP progress toward attaining process and tooling automation goals identified in the Automation Plan. This is the semi-annual refresh of the Annual Automation Plan	Publication and agreement on the Annual Automation Plan captured in a .docx document and ServiceNow PPM that includes: - Analysis of event and incident patterns with associated planning for continued improvements and measurements of success of previous automation execution. - Automation opportunities and recommendations for process and technology automation in the Security Operations Services environment for the upcoming year. These plans include views at the enterprise levels. - Report on targets from previous plans with overall success and impacts to the environment.	No	No	Annually on Feb 15
2.18	Evergreen Staffing Results	The Successful Respondent will deliver an Annual Evergreen Staffing plan.	This plan should include the team and individual overall performance in driving higher Customer Satisfaction, progress in execution of an operating culture that drives Customer value. Details should also include identification of ways in which Training, Skills Rotations, Key Personnel development have contributed to service improvements and incorporation of best practices within the operations, maintenance and support of service.	No	No	Annually on Feb 15