



**Attachment to Data Center Services
Service Component Provider
Master Services Agreement**

DIR-SECOPS-MSA-434

**DCS Security Operations Services
Appendix A
Reports**

August 14, 2020

Change Log

CCR/CN	Amendment	Date	Description
CCR-000XXX	N/A	8/14/2020	<ul style="list-style-type: none"> • Added "Contract Change Log" tab • "DCS Reports" tab: Removed the following reports under the "Security" heading inadvertently not removed in the final agreement: -SMDM Statistical Reports -Endpoint Device Services Operational Reports -Endpoint Device Services Configuration Reports -IDS/IPS Configuration Reports -SMDM Environment Review -HIPS Operational Reports -HIPS Configuration Reports -Managed Firewalls Configuration Reports -WAF Operational Reports -WAF Configuration Reports -MDS/MPS Operational Reports -MDS/MPS Configuration Reports -Response Preparedness Report -Penetration Testing Reports -Cloud Compliance Scan Results -Cloud Compliance Security Checklist Report -Cloud Compliance Security Checklist Response -Vulnerability Scan Report -Web Application Vulnerability Scanning (WAVS) Report -Web or Mobile Application Penetration Testing Report

Overview

This Attachment contains a summary description of the format, content, and frequency of key reports required by DIR and DIR Customer.

Column Name	Column Description
Contract Reference	MSA reference, if applicable
Report Category	Functional Category
Report Name	Name of report
Description	Short description of the report and report content
Frequency	How often the report is distributed.
Recipient	DIR or DIR Customer for whom report is created.
Report Location	Where the report is published ; Portal, email etc...
Report Generator Tool	Tool from which the Service Provider creates the report
New or Existing Report	If the report is currently provided by the Incumbent (Existing) or being requested New
Report Data and Creation	Each column indicates which Service Component Provider provides the data for the report and which Service Component Provider creates the report.
Report Start Date (if other than Commencement)	The starting date for each report after Commencement

											Report Data and Creation	
Contract Reference	Report Category	Report ID	Report Name	Description	Description Revisions	Milestone Deliverable Date (if other than Commencement)	Frequency	Recipient	Report Location	Report Generator Tool	MSI	Security
	CMDB / Software Reports											
			Device Monitoring Report	Listing of servers, mainframes, appliances, and other devices monitored / not monitored, ordered by DCS Customer.			Monthly	DIR	MSI Portal		C,D	D
			Capacity Plan	Current usage of resources, trends and forecasts and exceptions. Supports the on-going program of Capacity Management.			Annual	DIR, DCS Customer	MSI Portal		C,D	D
			Asset Discovery Report	Provide a report to the State of all in-scope devices discovered with identification of DCS allowed exceptions and incompatible/conflicted software items that are unsupported, unpatched, obsolete or unusable in consideration of DCS Standards.			Monthly	DIR, DCS Customer	MSI Portal		C,D	D
	Security											
			Intrusion Detection Report	Report on intrusion attempts and success/failure of prevention systems. Failures generate Incidents and Alerts generate Work Orders.			Daily	DIR, DCS Customer	MSI Portal		C	D
			IAM System Report	Report of number of adds/modifications/disables/deletes done per month.			Daily	DIR, DCS Customer	MSI Portal		C	D
			Vulnerabilities Report - Weekly	Report on vulnerabilities across all SCPs and Customers found			Weekly	DIR, DCS Customer	MSI Portal		C	D
			Vulnerabilities Report - Monthly	Summary report on vulnerabilities discovered, corrected, accepted, and pending. This includes trend analysis and recommendations for security planning and operational improvements.			Monthly	DIR, DCS Customer	MSI Portal		C	D
			SIEM reports - Daily	Report from SIEM tool showing all events.	From SOW 3.1.1		Daily	DIR, DCS Customer	MSI Portal		C	D
			SIEM reports - Quarterly	Validation report that all required security events are collected, correlated and included in security alert and monitoring processes and applicable tools	From SOW 3.1.1		Quarterly	DIR, DCS Customer	MSI Portal		C	D
			Privileged Access Management Compliance Report	Report showing compliance with security access policies and procedures	From SOW 3.1.2		Monthly	DIR, DCS Customer	MSI Portal		C	D
			Targeted Threat Research Report	Report the threat analysis to DIR, SCPs, MSI so that risks are identified and appropriately mitigated	From SOW 3.2		Monthly	DIR	MSI Portal		C	D
			Security Event reporting		From SOW 3.3		Monthly	DIR	MSI Portal		C	D
			System Access Report	perform a review of all users assigned access to Successful Respondent systems and confirm access validity providing report to DIR.	From SOW 3.3		Quarterly	DIR	MSI Portal		C	D
			Risk and Vulnerability Management Report -	monthly status of DIR Shared Services risk and vulnerability management, including prevention and treatment plan actions with	From SOW 3.3 and 3.16		Monthly	DIR	MSI Portal		C	D
			Security Audit and Compliance Report	a monthly audit and compliance report for all DCS Service Assets that includes any identified vulnerabilities identified via continuous monitoring and Successful Respondent concerns. This report must contain DCS Customer name and device specifics as to effectively identify the DCS service element that is not in compliance or of concern, the DCS customer and the appropriate DCS SCP(s) required to address the issue	From SOW 3.8		Monthly	DIR	MSI Portal		C	D
			Confidential Vulnerability and Remediation Report	Report containing all successes/failures, issues, weaknesses; access method and root cause analysis; position statement containing relative exposure details; verification fo integration with MSI vulnerability management; state data access	SOW 3.14		Quarterly	DIR	MSI Portal			
			After-Incident Report. Q: Is this an RCA? Or, the detailed report, post-incident?	Report describing the Security Incident, causes and effects, actions taken by the Successful Respondent, and recommended future actions to mitigate risk.	SOW 3.13		As needed	DIR, DCS Customer	MSI Portal		C	D

											Report Data and Creation	
Contract Reference	Report Category	Report ID	Report Name	Description	Description Revisions	Milestone Deliverable Date (if other than Commencement)	Frequency	Recipient	Report Location	Report Generator Tool	MSI	Security
			Monthly Incident Management Report	Key issues relating to Incident Management processes. Number of Incidents during the month, grouped by severity, service, agency, region, classification or other criteria as appropriate. List of Incidents, short description, reference number, and a shortcut to detailed description. Detailed description, including timing of activities. Links to Problems and Known Errors. Trend analysis of the Incidents reported during the thirteen (13) most recent months. Calculate metrics and provide monthly reports to DIR and Customers, which include: The number of Incidents. Sources of the Incidents. Frequency regarding the types or categories of Incidents. The duration of open Incident (average and quantities by age). Number and percentage of Incidents Resolved upon first contact. Trending metrics in terms of MTTRS (mean time to restore service) by category, priority and by service or SLA. Number and percentage of SLA impacting Incidents. Number and percentage of Incidents (by category, priority, service and SLA) that were handled within the SLA targets. Number and percentage of Incidents (by category, priority, service and SLA) reopened. Number and percentage of Incidents (by category, priority, service and SLA) reoccurring. Number and percentage of Incidents that have resulted in the creation of problem records. Percentage (by category, type and priority) of Incidents that were resolved by use of an Incident Model; Number and percentage of Incidents escalated by organization, category, priority and Service. The association of Incidents by cause and resolution by Service Component. Other pertinent information regarding Incident Resolution, including Service Level measurement reporting			Monthly	DIR, Customer	MSI Portal		C	D
			Enterprise Event Management Report	Provides statistics, lists and charts illustrating the Events collected in the STC supported environment including the number of, source, destination and type of event. Provides reports on Incidents and Problems initiated by the Enterprise Event Management system with trends over the past 13 months. Number of events per CIs. Number of occasions when an event is collected and can't be matched with a CI Summary and details of events which resulted in an automated correction made to remediate errors. Statistical information about the number of, source, destination and type of event			Weekly	DIR	MSI Portal		C	D
			Monthly Security Status Review	Roll-up of multiple sources: Monthly Security Updates Monthly Mainframe Security Services Monthly Identity and Access Management Services status report Monthly Background Checks TDCJ and DFPS status report Monthly Documentation and Process status reports (PPM updates, ISeC updates, etc.) Monthly ISeC status reports (number of exceptions, number pending, DCSCustomer issues with ISeC implementation (delays in implementation, DCS Customer failure to submit exceptions, etc.) Monthly Antivirus/Malware status report Monthly Security Reports information derived from ISS Security Services			Monthly	DIR	MSI Portal		C	D
			Monthly On-boarding/Off-boarding Report	Identify new personnel on-boarded and off-boarded personnel.			Monthly	DIR	MSI Portal		C	D
			Access Management Report	Report on all Access Requests and their status, access rights granted or removed, approver and dates of the request lifecycle.			Quarterly	DIR, Customer	MSI Portal		C	D

											Report Data and Creation	
Contract Reference	Report Category	Report ID	Report Name	Description	Description Revisions	Milestone Deliverable Date (if other than Commencement)	Frequency	Recipient	Report Location	Report Generator Tool	MSI	Security
			IDS/IPS - Operational Reports	Report of most frequent sources of blocked/detected inbound traffic sorted by volume High to Low, Report of most frequent sourced geolocations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent destinations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent destination geolocations of blocked/detected inbound traffic sorted by volume High to Low Report of most frequent sources of blocked/detected outbound traffic sorted by volume High to Low Report of most frequent destinations of blocked/detected outbound traffic sorted by volume High to Low Report of most frequently activated filters - most blocks; sorted by volume - High to Low Report of most frequently activated filters - Permits and Blocks; sorted by volume - High to Low			Weekly	DIR, Customer	MSI Portal		C	D
			SIEM - Operational Reports	Report summarizing and providing data for the SIEM including SIEM event counts per month, week, day or other time period required by the Customer with the counts broken down into the Customer's source categories. Number and types of alerts sent to Customer, Current list of all devices providing Syslog (feeds) to the SIEM for monitoring Number of events by device Summary of real time rule alerts in the past 30 days, including details for top 10 rules for which the most alerts were generated.			Monthly	DIR, Customer	MSI Portal		C	D
			Log Management Device Report	Monthly report detailing the number of devices being logged.			Monthly	DIR, Customer	MSI Portal		C	D
			Log Management Event Report	Monthly report detailing the number of events logged by device and amount of bandwidth used for logging			Monthly	DIR, Customer	MSI Portal		C	D
			Targeted Threat Research Report	Report the threat analysis to the Customer in a format to be agreed upon by the Customer and Service Provider.			As Requested	DIR, Customer	MSI Portal		C	D
			Security Incident Reporting	Details of all Security incident responses and activities, to include a timeline of events and activities.			As Requested	DIR, Customer	MSI Portal		C	D
			Digital Forensics Report	Report on the results of digital forensics investigations in a format frequency to be mutually agreed upon by the IR Service Provider and Customer.			As Requested	DIR, Customer	MSI Portal		C	D
			Risk Assessment Report	Risk assessment report, including but not limited to priorities, recommendations and a narrative of findings.			As Requested	DIR, Customer	MSI Portal		C	D