Commercial Price List

April 2018

ISO/IEC 20000-1:2011 & **ISO** 9001:2008
CMMI DEV / 3 & **CMMI** SVC / 3

TABLE OF CONTENTS

Section **Page**

1 PROFESSIONAL SERVICES RATE CARD 1
2 CLOUD ASSURED MANAGED SERVICES (CAMS) 2
2.1 Introduction 2
2.2 CAMS Management Portal 2
2.3 Managed Services and Service Management 2
2.4 Cloud Resale and Consolidated Billing 2
2.5 Service Descriptions 3
2.6 Core Services 3
2.6.1 Monitoring and Notification Service 3
2.6.2 SLA Management 4
2.6.3 Event Management & Incident Response 4
2.6.4 Operating System Patch Management 4
2.6.5 Anti-Malware Management Service 5
2.6.6 Boundary Management 5
2.6.7 Log Aggregation Service 6
2.6.8 Backup and Restoration 6
2.6.9 Infrastructure Provisioning 7
2.7 Optional Services 7
2.7.1 CSEM Advisory 7
2.7.2 Infrastructure Advisory 8
2.7.3 Disaster Recovery 8
2.7.4 Advanced Monitoring 8
2.7.5 Enhanced Data Encryption 8
2.7.6 Advanced Security 9
2.7.7 Application Management 9
2.7.8 Database Management 9
2.7.9 Web Management and CDN 9
2.7.10 Help Desk 9
2.7.11 Workspaces Management 9
2.8 Managed Security Services 10
2.8.1 Security Incident Response 10
2.8.2 Enhanced Log Aggregation and Analysis 10
2.8.3 Security and Regulatory Compliance Advisory 10
3 SERVICE LEVEL AGREEMENTS 11
3.1 SLA 1: System Availability 11
3.2 SLA 2: Backup and Restoration 11
3.3 SLA 3: Incident Response 12
3.4 SLA 4: Operating System Patching and Updating 13
3.5 SLA 5: Impending Event Notification 14

3.6 SLA 6: Database Management Service Request 14
3.7 SLA 7: Impending Security Threat Notification 14
4 COMMERCIAL PRICING 16
4.1 Discount Schedule 17
5 SERVICES PURCHASED 18
6 SMARTRONIX VALUE-ADD CLOUD SERVICES PROGRAM - AWS 19
6.1 Cloud Services 19
6.2 Cloud Management Tool 19
6.3 Support Services 19
7 SMARTRONIX VALUE-ADD CLOUD SERVICES PROGRAM - AZURE 20
7.1 Cloud Services 20
7.2 Cloud Management Tool 20
7.3 Support Services 20
APPENDIX A: CLOUD ASSURED MANAGED SERVICES FOR GOVERNMENT 1
1 CLOUD ASSURED MANAGED SERVICES FOR GOVERNMENT (CAMS-G) 1
1.1 Introduction 1
1.2 CAMS-G Management Portal 1
1.3 Managed Services 1
1.4 Cloud Resale and Consolidated Billing 2
2 SERVICE DESCRIPTIONS 2
2.1 Core Services 3
2.1.1 Monitoring and Notification Service 3
2.1.2 SLA Management 3
2.1.3 Event Management & Incident Response 4
2.1.4 Operating System Patch Management 4
2.1.5 Host Based Anti-Malware Management Service 4
2.1.6 Boundary Management 5
2.1.7 Log Aggregation Service 5
2.1.8 Backup and Restoration 6
2.1.9 Infrastructure Provisioning 6
2.2 Optional Services 7
2.2.1 CSEM Advisory 7
2.2.2 Infrastructure Advisory 7
2.2.3 Disaster Recovery 7
2.2.4 Advanced Monitoring 8
2.2.5 Application Management 8
2.2.6 Database Management 8
2.2.7 Web Management and CDN 8
2.2.8 Help Desk 8
2.2.9 Workspaces Management 8
2.2.10 Elastic Map Reduce and Redshift Management 9

2.3 Optional Managed Security Services 10
2.3.1 Security Incident Response 10
2.3.2 Enhanced Log Aggregation and Analysis 10
2.3.3 Security and Regulatory Compliance Advisory 10
2.3.4 Enhanced Data Encryption 10
2.3.5 Advanced Security 11
2.3.6 Assured Compliance Assessment Solution (ACAS) 11
3 SERVICE LEVEL AGREEMENTS 12
3.1 SLA 1: System Availability 12
3.2 SLA 2: Backup and Restoration 12
3.3 SLA 3: Incident Response 13
3.4 SLA 4: Operating System Patching and Updating 13
3.5 SLA 5: Impending Event Notification 14
3.6 SLA 6: Database Management Service Request 14
3.7 SLA 7: Impending Security Threat Notification 15
4 PRICING 16
4.1 Discount Schedule 17

1 PROFESSIONAL SERVICES RATE CARD

Labor Category	Hourly Rate
Cloud Architect	$225
Senior Cloud Engineer	$200
Cloud Engineer	$180
Senior Solutions Architect	$275
Solutions Architect	$225
Cloud Subject Matter Expert I	$300
Cloud Subject Matter Expert II	$325
Cloud Subject Matter Expert III	$350
Senior Solutions Engineer	$210
Solutions Engineer	$180
Senior Developer	$225
Developer	$190
Junior Developer	$130
Senior Data Architect	$225
Data Architect	$190
Senior Business Analyst	$190
Business Analyst	$165
Junior Business Analyst	$110
Senior Security Architect	$200
Security Architect	$175
Senior Security Analyst	$175
Security Analyst	$150
Junior Security Analyst	$100
Senior I&O Engineer	$140
I&O Engineer	$120
Junior I&O Engineer	$100
Cloud Program Manager	$220
Cloud Project Manager	$200

2 CLOUD ASSURED MANAGED SERVICES (CAMS)

2.1 Introduction

The Cloud Assured Cloud Management Platform, and optional Cloud Service Expense Management (CSEM) capabilities comprise the Smartronix Cloud Assured Managed Services solution (CAMS). CAMS gives your organization the ability to leverage the power and scalability of the cloud while reducing the cost and complexity of managing and monitoring infrastructures and applications in-house. Our experts provide complete management of cloud services from initial provisioning through the entire solution life-cycle. Our Managed Services span private, public, multi-cloud, and hybrid cloud offerings, allowing your organization to focus on critical business and strategic technology efforts while leaving resource-intensive IT operations to our professional team of experts.

CAMS includes the software licensing and configurations for the tools required to manage and monitor your environments to meet your Service Level Agreements.

2.2 CAMS Management Portal

Smartronix wraps the customer experience in the CAMS Portal ITSM framework. The CAMS portal provides each customer a unique view of the delivered Managed Services solution and provides access into service request, event and incident ticket management systems. The back-office ITSM functionality is delivered via a Smartronix customized ServiceNow portal to ensure strict, organization-specific separation of customer data. Additionally, the CAMS Portal and supporting ServiceNow implementation can apply access governance across Smartronix personnel in case of regulatory or other Customer-specific compliance requirements (special background investigations, public clearances, or other industry-specific clearance activities.) Cloud Assured Managed Services customers can create, track, manage, and report on all of their service requests from a central location 24/7/365.

2.3 Managed Services and Service Management

The Core Services have been developed and integrated to provide customers with a fully instrumented Cloud experience. Optional Services in the catalog are designed to enhance customer experience and capabilities through delivery of discrete capabilities within the Smartronix Cloud Management Platform inclusive of the processes, procedures, tooling, and licensing necessary to deliver predictable results. **Tables 1 and 2** below identify the portfolio of Core, Custom, Optional, and Optional Security Services.

The Smartronix cloud management framework can also address scenarios where customers may have existing tools, interoperability or business requirements that drive custom service integrations. These custom integrations are priced separately to accommodate unique licensing costs and labor required for a tailored solution.

2.4 Cloud Resale and Consolidated Billing

The Smartronix Cloud Resale and Consolidated Billing service delivers value-added Cloud Service Expense Management (CSEM) capabilities. Customers consume Cloud Services through

re-sale from Smartronix. Re-sale customers receive a single consolidated invoice of all utilized services across all managed accounts. Billing detail is tailored to support customer business and financial management requirements including organizational and divisional separation for show-back / chargeback purposes. The CSEM Advisory service (Optional Services) is bundled in to CRCB as part of the value-added service offering designed to optimize your cloud expense efficiency.

2.5 Service Descriptions

The following sections describe the Core, Custom, Optional, and Managed Security Services offerings.

Table 1. Cloud Assured Managed Services.

CORE Managed Services
Monitoring and Notification
SLA Management
Event Management and Incident Response
Operating System Patch Management
Anti-malware Management
Boundary Management
Log Aggregation
Backup and Restoration
Infrastructure Provisioning

Table 2. Cloud Assured Optional Managed Services.

Optional Services	Optional Security Services
Cloud Service Expense Management Advisory Service	Security Incident Response
Infrastructure Advisory Service	Enhanced Log Aggregation and Analysis
Disaster Recovery	Security and Regulatory Compliance Advisory
Advanced Monitoring	
Data Encryption	
Advanced Security	
Application Management / Database Management	
Web and CDN Management	
Workspace Management	

2.6 Core Services

2.6.1 Monitoring and Notification Service

The Smartronix M&N Service leverages the CAMS Monitoring Solution (CMS) automation framework. The CMS leverages micro services to detect all assets that are tagged for

management and enables a defined set of standardized alarms/alerts. Each alarm can be customized to a tagged instance definition, allowing customer environments to have different defined alarm triggers for specific workloads. The CMS framework leverages web hooks to pull in the alarms/alerts and to automate creation of ITSM tickets.

Triggers include:

High CPU Utilization*	Instance failed health check	CSP Login authentication failures
Disk space utilization*	Root account logins	Security group changes
Excessive disk IOPs*	Object storage policy changes	Network ACL changes
Excessive disk write queue length*	IAM policy changes	Change to cloud network gateway
Excessive network utilization*	Logins without MFA	Network route table changes
High memory usage*	CloudTrail configuration changes	

**Triggers can be customized to customer workloads.*

2.6.2 SLA Management

Customer service requirements are monitored and tracked against documented Service Level Agreements (SLAs). The SLA Management Service reports service performance against standard Service Level targets identified below in Section 3. The reports are provided periodically and are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement.

2.6.3 Event Management & Incident Response

The Smartronix' Event Management and Incident Response (EM&IR) Service supports identification, classification, and filtering of Events, as well as structured response for mitigation and remediation of exception Incidents within customer environments.

Event management includes detection and notification via the Monitoring and Notification Service; Filtering of events via notification service topics; and, registration of events as Informational, Warning, or Exception.

Event Warnings initiate low priority Incident response workflows. Exception Events trigger high priority Incident response processes and procedures. The Smartronix' Cloud Assured team employs structured processes for the identification, classification, escalation where necessary, and remediation of managed cloud infrastructure and supported operating system incidents.

2.6.4 Operating System Patch Management

Smartronix' Operating System Patch Management (PM) Service monitors the availability of and proactively applies operating system patches and updates through the use of a patch management life-cycle. Smartronix' Cloud Assured team performs monthly patching of guest operating systems based on the vendor release schedule. Maintenance and patching windows are coordinated with each customer to ensure operations are not impacted by system patching. The patching capability is a scripted process that will trigger the guest OS to download and

apply the identified guest OS patches. The applied patches are tracked through the Cloud Assured MSP system to track system configuration. Critical or security related patches are quickly escalated to the customer for approval to deploy during an out of cycle maintenance window.

Customers can opt-in (patch and update) or opt-out (do not patch, do not update) individual systems via the instance tag.

Supported Operating Systems include:

- Amazon Linux 2015.03+
- RedHat Enterprise Linux
- CentOS 6/7
- Ubuntu 12.04/14.04 LTS
- Windows 2008-2016

2.6.5 Anti-Malware Management Service

Smartronix' Anti-malware (AMS) Management Service protects your environment against malware (viruses, trojans, spyware/grayware) by ensuring that the CAMS provided antimalware is installed, up-to-date, active, and is running current malware signatures on managed OS instances. When malware is detected, we proactively ensure quarantine and automatically create an incident ticket for the remediation of the issue. Audits are performed to ensure individual server compliance with customer antimalware policies.

The service is provided through a consolidated management framework. Smartronix' Cloud Assured MSP offering leverages distributed relays and customer policy-based isolation. The AMS functionality is currently provided by the TrendMicro Deep Security Suite (DSS). Smartronix deploys the Deep Security Agent (DSA) on the customer guest OS image. These instances are registered through the customer DSA relay and transmitted through encrypted IP-restricted transport to the Cloud Assured Deep Security Manager (DSM). Through the DSM, policies are applied to customer agents to ensure signature updates are applied as soon as available to enable up-to-date protection of customer systems. Customers can request custom agent exclusions through the Cloud Assured ServiceNow portal.

The anti-malware service protects against many file-based threats, including the following: Viruses (file infectors), Trojans, Backdoors, Worms, Network, Rootkits, Spyware, Grayware, packers, and keyloggers.

2.6.6 Boundary Management

Smartronix' Boundary Management (BM) Service is a proactive monitoring and management service providing configuration management of cloud service provider components for networking, firewalls, virtual private networking (VPN), subnets, access control lists (ACLs), and virtual networks.

Our Cloud Assured team will manage and monitor boundary protection and cloud environment network operations to ensure a secure and highly-available environment for customer data and applications. The BM service identifies, mitigates, and implements network level changes in

response to events or customer requests. Supported change requests include VPN tunnel configuration, firewall policy changes to ACLs, IP route configurations, public IP allocation for service advertising, deployment of load balancing capabilities, and deployment of new cloud IP subnets. Technologies used in support of boundary management include:

- VPC Flow Logs
- CloudWatch Events
- M&N for ACL and Security Group changes

2.6.7 Log Aggregation Service

Smartronix' Log Aggregation (LA) Service captures cloud service provider logs, guest OS logs, and network logs. Alerts are generated for critical events and key performance indicators within the environment, which then automatically trigger an operational response.

Using the LA Service and Smartronix' change management process, the Cloud Assured team monitors the IaaS environment for possible security incidents through event filters and alerts, and performs change management of event filters implemented to ensure known critical events are identified and escalated. This service is filter-driven by a set of unwanted event types. These events include items such as cloud infrastructure configuration changes, instance termination, and excessive CPU utilization. These event filters are customized through-out the MSP term as patterns develop from lessons learned specific to the customer's applications.

Please note that log correlation, advanced search, and analysis is not part of this service – see Security Services – Enhanced Log Aggregation and Analysis. Technologies used in support of log aggregation include:

- CloudTrail Logs
- OS Logs (SSM required)
- VPC Flow Logs
- S3
- ELB
- ALB

2.6.8 Backup and Restoration

Smartronix' Backup (BU) Services include system, configuration, environment and cloud services backup and restore. Backups are created and stored in the customer's cloud environment and data storage costs associated with backups are part of the customer cloud environment operating costs.

BU Services includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The duration of backup retention will have an impact on cloud storage costs. Through the ITSM process, the Cloud Assured team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured

to ensure a rollback is available if the restore is unsuccessful. Backup and restore testing is performed annually to ensure backup consistency.

2.6.9 Infrastructure Provisioning

Smartronix Infrastructure Provisioning (IP) services ensure consistent and repeatable deployment of cloud infrastructure. Customers submit IP requests through the Cloud Assured ITSM portal for any service that requires management. Smartronix receives the requests, confirms the requirements, provisions the resource, and instruments the resource to ensure any core or additionally procured managed service is configured appropriately for M&N, SLA, ER&IR, AMS, BU, PM, and LA services.

Core Infrastructure Provisioning covers:

- Compute
- Storage
- Boundary Configuration
- Identity and Access Management Credentials
- Load Balancers
- Workspace provisioning

2.7 Optional Services

2.7.1 CSEM Advisory

The Smartronix Cloud Service Expense Management (CSEM) Advisory Service facilitates environmental cost optimization based on actual usage data aggregation and correlation. Recommendations are based on analysis of CSEM actuals; application of advanced tool sets to model future spend as a function of utilization and execution of “what-if” scenarios; familiarity with customer workloads and environments; and, extensive experience across customer cloud environments. The CSEM Advisory Service is included as an integrated component of the Cloud Resale and Consolidated Billing Service.

Examples of cost optimization opportunities include:

- Resource utilization (Throttling under-utilized instances; Parking off-period resources)
- Right-sizing instance type
- Selection of workload-appropriate pricing models
- Resource tagging
- Reclamation of orphaned resources
- Optimization of BYOL (Bring-your-own-license)
- Storage life-cycle management
- Cost Monitoring and Alerting

This service requires deployment of the Smartronix CSEM tool which requires read only access to the CSP billing data and optional read only access to performance data (for service utilization optimization.)

2.7.2 Infrastructure Advisory

Smartronix' Infrastructure Advisory (IA) Services provides prescriptive guidance on cloud services optimization, including capacity management reviews, architectural reviews and best practices reviews, auto scaling tuning, and migration paths for on premise workloads. These reviews leverage our Cloud Assured - Well Architected guidelines and ITSM process.

The Cloud Assured - Well Architected Review is a detailed analysis of your infrastructure, a thorough review of security practices, application integration architectures, and sizing of resources. This review enables Smartronix' Cloud Assured team to ensure customers are leveraging cloud services in line with CSP best practices while delivering cost effective and secure service delivery.

2.7.3 Disaster Recovery

Smartronix' Disaster Recovery (DR) Service defines a DR architecture and processes to provide full planning, annual testing and execution of a managed disaster recovery solution encompassing applications, systems, and environments. Our Cloud Assured team will work with you to ensure your Recovery Time Objective/Recovery Point Objective (RTO/RPO) are appropriate to your mission and to architect the solution to fulfill the requirements at the lowest cost.

2.7.4 Advanced Monitoring

Smartronix' Advanced Monitoring (AM) Service provides deeper visibility into your entire environment. Using header tags, synthetic transactions, agent based heath tools, and state-of-the-art tools, processes, and best practices, the Smartronix Cloud Assured team will configure advanced monitoring to discover and optimize a comprehensive suite of availability and performance metrics.

2.7.5 Enhanced Data Encryption

Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' Cloud Assured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

2.7.6 Advanced Security

Smartronix' Advanced Security (AS) Services is a custom solution. Our Cloud Assured team works with your security organization to implement layered, comprehensive protection against data loss, advanced identity management services, host based intrusion detection/intrusion prevention solutions (IDS / IPS / HIPS), security assessments, security vulnerability scanning, and continuous security monitoring. AS Services is a foundational capability for creating high security enclaves in cloud environments.

2.7.7 Application Management

Smartronix' Application Management (AM) Service delivers COTS and custom-built applications under the managed Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) model. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

2.7.8 Database Management

Smartronix' Database Management (DBM) Service is a full-lifecycle capability available for industry- leading RDBMSs. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

2.7.9 Web Management and CDN

Smartronix' Web Management and CDN (WMC) Service provides monitoring, availability, maintenance, security and configuration management for web applications and frameworks, including the operations and management of third party CDN services. We provide proactive security monitoring of the site distribution, availability monitoring, maintenance, configuration management, patching and security of the environment and applications. External availability and performance monitoring is also available.

2.7.10 Help Desk

Smartronix' Help Desk (HD) provides front line (Tier 1) support for end users in your organization. Smartronix' Cloud Assured team user support specialists create and track issues from report to resolution, collecting and documenting circumstances, researching and recommending resolution activities, and ensuring customer satisfaction or timely escalation for prompt closure.

2.7.11 Workspaces Management

Smartronix' Workspaces Managed Services (WMS) brings server-class management and assurance to virtual desktop users. WMS includes operating system patch and update management, software packaging, and software lifecycle management (deployment, configuration management, updating, and deprovisioning). Workspaces Management Services Backups let you choose an RPO that's right for your organization and know that your virtual workstation data is protected. Antivirus and antimalware are included, and compliance is enforced. Integration with your existing directory service means organizational configurations,

policies, and controls are applied to your Workspaces and managed by Smartronix WMS the same as they are for your servers.

2.8 Managed Security Services

2.8.1 Security Incident Response

Smartronix' Security Incident Response (SIR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments. Smartronix' Cloud Assured team will support the incident response process through incident escalation, break/fix remediation of infrastructure and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The Cloud Assured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the environment or guest operating systems.

2.8.2 Enhanced Log Aggregation and Analysis

Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service is captures all events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core *Log Aggregation* service by integrating search capabilities, counters, and proactive log review analysis. The *Analysis* capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

2.8.3 Security and Regulatory Compliance Advisory

Smartronix' Security and Regulatory Compliance Advisor (SRCA) Service utilizes Global Intelligence for security and threat analytics to provide clients guidance in regulatory requirements and recommend mitigation of threats that have potential to impact client-specific environments as they appear and evolve. Email notification is provided the day of significant threats are surfaced in industry analyses.

Monthly Summaries are provided by the 10th day of the following month.

3 SERVICE LEVEL AGREEMENTS

3.1 SLA 1: System Availability

SLA 1: "System" Availability	
Description	This SLA applies to "system availability" of a service. A system is considered a series of components that make up the infrastructure service that hosts and provides the compute and storage capabilities consumed by the customer applications and services. System availability applies to the following products and services: • Virtual Compute Instances (AWS EC2 and Azure Virtual Machines deployed in the same availability set) • Block Storage (AWS EBS, Azure System/Data Disks) Smartronix SLA incorporates the AWS and Azure SLA terms defined below which are subject to change in accordance with the AWS and Azure Agreements. • AWS Compute SLA: https://aws.amazon.com/ec2/sla/ • Microsoft Azure Compute SLA: https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_6/
Measurement	Smartronix will measure system infrastructure availability by using tools that will access the cloud infrastructure compute availability at 5 minute intervals to analyze cloud IaaS regional compute availability.
Calculation	NUMERATOR Uptime (Seconds) ÷ DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside Smartronix control and approved as such by customer. Examples of these type of exception events include: Force majeure events; and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

3.2 SLA 2: Backup and Restoration

SLA 2: Backup and Restoration	
Description	This SLA measures the percent of times that the platform is restored to last agreed and documented state and last transactional dataset after failure, data loss or user request for restoration.
Measurement	Initiation of restore for individual file or database requests within 8 hours of receipt of request or notification of failure

SLA 2: Backup and Restoration	
	Backup retention periods are defined by Client.
Calculation	NUMERATOR: Number of successful restore initiations within 8 hours or Number of full restoration within 48 hours ÷ DENOMINATOR: Number of Requests for Restores = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully restored 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

3.3 SLA 3: Incident Response

SLA 3: Incident Response Time	
Description	This SLA measures Smartronix' response time, per the Exceptions/Conditions in this SLA, following issue identification.
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incident receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is successful if 95% of incidents receive a response within response time for given severity level, as measured on a monthly basis.
Exceptions / Conditions	Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of incident occurring 24x7x365. Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of incident occurring 24x7x365. Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain functional. Minimal user impact. Within 24 hours of incident occurring during business hours. (8am-8pm EST M-F). Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No or minimal user impact. Within 1 business day of incident occurring during business hours. (8am-8pm EST M-F).

SLA 3: Incident Response Time	
	Exception: Impending events; notification will happen; incident response will be initiated before follow-up notification; as clients will be previously notified (SLA 5) of the likelihood of the event.

3.4 SLA 4: Operating System Patching and Updating

SLA 4 – Operating System Patching	
Description	This SLA measures Smartronix' ability to patch all operating systems protecting on a planned schedule. All critical patches will be applied in accordance to the client planned schedule that will be defined in the Concept of Operations document. All other patches will be executed upon a customer pre-approved schedule.
Measurement	All operating systems will be up to date with critical patches within 10 days of release and measured by scanning with vulnerability software.
Calculation	NUMERATOR: Total number of patched systems within 10 calendar days of critical patch release ÷ DENOMINATOR: Number of systems requiring patches = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is considered successful when 95% of critical patches are applied to the initial environment within 10 calendar days of release from vendor and subsequent patches are applied per the customer patch schedule. Patches must be approved by customer. This will be measured on a monthly basis.
Exceptions / Conditions	Ten (10) day SLA applies to the initial environment patched. Patching of subsequent environments follow customer patch schedule. Smartronix failure to execute patching of subsequent environments per customer patch schedule shall also be considered an SLA failure for purposes of the Calculation. Any patches not approved by customer or Smartronix' CCB are excluded from the SLA Calculation.

3.5 SLA 5: Impending Event Notification

SLA 5 – Impending Event Notifications	
Description	Smartronix will notify the customer of the possibility of an impending event or events that have occurred which might affect system operation. Examples include cloud service provider notifying Smartronix of service degradation, service unavailability, or service termination.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending event.
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

3.6 SLA 6: Database Management Service Request

SLA 6 – Service Request – Database Management	
Description	Smartronix will initiate requested support on-demand functions for Database support made by the customer within one business day. Examples include request for database refresh from prod to Test or development, launching database instances, preforming performance analysis.
Measurement	Smartronix will measure request response based on the time requested as documented in the ITSM reporting system and the request initiation being within 1 business day.
Calculation	NUMERATOR: Number of successful request initiations within 1 business day ÷ DENOMINATOR: Number of Requests = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully initiated responses 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

3.7 SLA 7: Impending Security Threat Notification

SLA 7: Impending Security Threat Notifications	
Description	Smartronix will notify the Client of the possibility of an impending Security Threat or events that have occurred which may impact system operation. Examples include global intelligence sources identifying new

SLA 7: Impending Security Threat Notifications	
	threats in the environment that may impact OS, Applications, or services used by Client.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending threat
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

**SLA usage can vary dependent on services purchased.*

4 COMMERCIAL PRICING

Table 3. Core Managed Services

Service Title	Price
Monitoring and Notification	$300/instance
SLA Management	
Incident Response	
Operating System Patch Management	
Antivirus (AV) Management	
Boundary Management	
Log Aggregation (Basic)	
Backup Services	
Infrastructure Provisioning Service	$50/Provisioning Request

Table 4. Optional Services

Service Title	Price
Cloud Service Expense Management Advisory Service	1% of Invoice monthly
Infrastructure Advisory Services	Priced based on scope.
Disaster Recovery Services	Price based on request
Advanced Monitoring Services	$100 / instance
Enhanced Data Encryption Services	Price based on request
Advanced Security Services	$150 / instance
Application Management Services	$300 / instance
Database Management Services	$400 / instance
Web Management Services and CDN	$400/ site distribution
Workspaces Management Services	Tier per Workspace Instance Fee $25 Per less than 150 Instances $22 for 150 through 300 $18 for 300 through 700 $14 Greater than 700

Table 5. Optional Security Services

Service Title	Price
Security Incident Response	Priced based on scope.
Enhanced Log Aggregation and Analysis	Log Monitoring and Analysis - $320/per GB of indexed data, based on average daily consumption in a month.
Security & Regulatory Compliance Advisory Service	$6,000

Notes:

- Customized service/pricing for customer environments that have reduced requirements, e.g. Development, Test, Quality Assurance, or Labs is available.

- Clients are required to enable Config, CloudTrail, CloudWatch, and allow SMX to install AWS CloudWatch agent and AWS Inspector Agent on managed instances in regions that run services supported by Smartronix.
- Smartronix will reserve one AWS resource tag for use in the management of the resources.

4.1 Discount Schedule

Monthly Cost	Discount Tier
$0 - $15,000	0%
$15,001 - $30,000	2.5%
$30,001 - $45,000	5%
$45,001 - $60,000	10%
$60,001 - $100,000	12.5%
$100,001 - $500,000	15%
$500,001 -$1,000,000	17.5%
Over $1,000,001	20%

5 SERVICES PURCHASED

The following services have been purchases under the MSA.

Table 6. Purchased Services.

Service
Core Managed Services
Infrastructure Provisioning Service
Cloud Service Expense Management Advisory Service
Infrastructure Advisory Service
Disaster Recovery
Advanced Monitoring
Data Encryption
Advanced Security
Application Management / Database Management
Web and CDN Management
Workspace Management
Security Incident Response
Enhanced Log Aggregation and Analysis
Security and Regulatory Compliance Advisory

6 SMARTRONIX VALUE-ADD CLOUD SERVICES PROGRAM - AWS

MFR	Model Number	Description
AWS	AWS-LOT-001	AWS Lot - $1.00 in usage fees at AWS list price

Smartronix Value-Add Cloud Services Program provides customers with access to the AWS cloud with invoicing based off of the monthly CSP list price spend. The current AWS list prices can be found here: https://calculator.s3.amazonaws.com/index.html. The calculator will show AWS items with their associated list prices and estimated monthly spend. This offer includes:

6.1 Cloud Services

Provides access to Government approved cloud services from AWS.

- AWS Commercial Regions
- AWS GovCloud Region (customer must qualify)

6.2 Cloud Management Tool

Provides access to Cloud Management Tool. The Cloud Management Platform (CMP) provides full visibility and control to reduce costs, improve cybersecurity posture, and automate critical tasks to accelerate cloud agility for modern enterprises and service providers

6.3 Support Services

All orders are required to purchase:

- For AWS orders: Business Class Support which provides 24x7 AWS Technical Helpdesk Support with SLA response times

These are support products that are provided by the CSP and invoiced by Smartronix at the same discounted rate as the Cloud Services.

7 SMARTRONIX VALUE-ADD CLOUD SERVICES PROGRAM - AZURE

MFR	Model Number	Description
MSFT	AZURE-LOT-001	Azure Lot - $1.00 in usage fees at AZURE list price

Smartronix Value-Add Cloud Services Program provides customers with access to the Azure cloud with invoicing based off of the monthly CSP list price spend. The current Azure list prices can be found here: https://azure.microsoft.com/en-us/pricing/calculator/. The calculator will show Azure items with their associated list prices and estimated monthly spend. This offer includes:

7.1 Cloud Services

Provides access to Government approved cloud services from Azure.

- Azure Commercial Regions
- Azure Government Region (customer must qualify)

7.2 Cloud Management Tool

Provides access to Cloud Management Tool. The Cloud Management Platform (CMP) provides full visibility and control to reduce costs, improve cybersecurity posture, and automate critical tasks to accelerate cloud agility for modern enterprises and service providers.

7.3 Support Services

All orders are required to purchase:

- For Azure orders: Standard Support which includes 24x7 Azure Technical Helpdesk Support with SLA response times

These are support products that are provided by the CSP and invoiced by Smartronix at the same discounted rate as the Cloud Services.

APPENDIX A: CLOUD ASSURED MANAGED SERVICES FOR GOVERNMENT

The Cloud Assured Managed Services for Government (CAMS-G) is offered to our Federal and Department of Defense (DoD) customers that require enhanced security above our commercial offering.

1 CLOUD ASSURED MANAGED SERVICES FOR GOVERNMENT (CAMS-G)

1.1 Introduction

The Cloud Assured Cloud Management Platform and optional Cloud Service Expense Management (CSEM) capabilities comprise the Smartronix Cloud Assured Managed Services solution. CAMS-G gives your organization the ability to leverage the power and scalability of the cloud while reducing the cost and complexity of managing and monitoring infrastructures and applications in-house. Our experts provide complete management of cloud services from initial provisioning through the entire solution life-cycle. Our Managed Services span private, public, multi-cloud, and hybrid cloud offerings, allowing your organization to focus on critical business and strategic technology efforts while leaving resource-intensive IT operations to our professional team of US based cleared experts.

CAMS-G includes the software licensing and configurations for the tools required to manage and monitor your environments to meet your Service Level Agreements.

1.2 CAMS-G Management Portal

Smartronix wraps the customer experience in the CAMS-G Portal ITSM framework. The CAMS-G portal provides each customer a unique view of the delivered Managed Services solution and provides access into service request, event and incident ticket management systems. The back-office ITSM functionality is delivered via a Smartronix customized ServiceNow portal to ensure strict, organization-specific separation of customer data. Additionally, the CAMS-G Portal and supporting ServiceNow implementation can apply access governance across Smartronix personnel in case of regulatory or other Customer-specific compliance requirements (special background investigations, public clearances, or other industry-specific clearance activities.) Cloud Assured Managed Services customers can create, track, manage, and report on all of their service requests from a central location 24/7/365.

1.3 Managed Services

The Core Services have been developed and integrated to provide customers with a fully instrumented Cloud experience. Optional Services in the catalog are designed to enhance customer experience and capabilities through delivery of discrete capabilities within the Smartronix Cloud Management Platform inclusive of the processes, procedures, tooling, and licensing necessary to deliver predictable results. **Tables 1, 2, and 3** below identify the portfolio of Core (up to FedRAMP Moderate & DoD IL2), Optional, Optional Security Services, and DoD Impact Level 4 (IL4).

The Smartronix cloud management framework can also address scenarios where customers may have existing tools, interoperability or business requirements that drive custom service

integrations. These custom integrations are priced separately to accommodate unique licensing costs and labor required for a tailored solution.

1.4 Cloud Resale and Consolidated Billing

The Smartronix Cloud Resale and Consolidated Billing (CRCB) service delivers value-added Cloud Service Expense Management (CSEM) capabilities. Customers consume Cloud Services through re-sale from Smartronix. Re-sale customers receive a single consolidated invoice of all utilized services across all managed accounts. Billing detail is tailored to support customer business and financial management requirements including organizational and divisional separation for show-back / chargeback purposes. The CSEM Advisory service (Optional Services) is bundled in to CRCB as part of the value-added service offering designed to optimize your cloud expense efficiency.

2 SERVICE DESCRIPTIONS

The following sections describe the Core, Optional, Optional Security Services, and DoD Required Managed Services for IL4.

Table 1. Cloud Assured Managed Services.

	CORE Managed Services (FedRAMP Moderate/DoD IL)
Monitoring and Notification	X
SLA Management	X
Event Management and Incident	X
Operating System Patch Management	X
Host Based Anti-malware Management	X
Boundary Management	X
Log Aggregation	X
Backup and Restoration	X
Infrastructure Provisioning	X

Table 2. Cloud Assured Optional Managed Services.

Optional Services	Optional Security Services
Cloud Service Expense Management Advisory Service	Security Incident Response
Infrastructure Advisory Service	Enhanced Log Aggregation and Analysis
Disaster Recovery	Security and Regulatory Compliance Advisory
Advanced Monitoring	Enhanced Data Encryption
Application Management	Advanced Security
Database Management	Assured Compliance Assessment Solution (ACAS)
Web and CDN Management	

Optional Services	Optional Security Services
Workspace Management	
Elastic Map Reduce and Redshift Management	

Table 3. DoD IL4 Services.

	DoD IL4 Package
Monitoring and Notification	X
SLA Management	X
Event Management and Incident Response	X
Operating System Patch Management	X
Host Based Anti-malware Management	X
Boundary Management	X
Log Aggregation	X
Backup and Restoration	X
Enhanced Data Encryption	X
ACAS	X

2.1 Core Services

2.1.1 Monitoring and Notification Service

The Smartronix M&N Service leverages the CAMS-G Monitoring Solution (CMS) automation framework. The CMS leverages micro services to detect all assets that are tagged for management and enables a defined set of standardized alarms/alerts. Each alarm can be customized to a tagged instance definition, allowing customer environments to have different defined alarm triggers for specific workloads. The CMS framework leverages web hooks to pull in the alarms/alerts and to automate creation of ITSM tickets.

Triggers include:

High CPU Utilization*	Instance failed health check	CSP Login authentication failures
Disk space utilization*	Root account logins	Security group changes
Excessive disk IOPs*	Object storage policy changes	Network ACL changes
Excessive disk write queue length*	IAM policy changes	Change to cloud network gateway
Excessive network utilization*	Logins without MFA	Network route table changes
High memory usage*	CloudTrail configuration changes	

**Triggers can be customized to customer workloads.*

2.1.2 SLA Management

Customer service requirements are monitored and tracked against documented Service Level Agreements (SLAs). The SLA Management Service reports service performance against standard

Service Level targets identified below in Section 3. The reports are provided periodically and are designed to ensure service transparency by providing quality metrics throughout your experience. These metrics become the baseline for our ITSM Continuous Process Improvement.

2.1.3 Event Management & Incident Response

The Smartronix' Event Management and Incident Response (EM&IR) Service supports identification, classification, and filtering of Events, as well as structured response for mitigation and remediation of exception Incidents within customer environments.

Event management includes detection and notification via the Monitoring and Notification Service; Filtering of events via notification service topics; and, registration of events as Informational, Warning, or Exception.

Event Warnings initiate low priority Incident response workflows. Exception Events trigger high priority Incident response processes and procedures. The Smartronix' Cloud Assured team employs structured processes for the identification, classification, escalation where necessary, and remediation of managed cloud infrastructure and supported operating system incidents.

2.1.4 Operating System Patch Management

Smartronix' Operating System Patch Management (PM) Service monitors the availability of and proactively applies operating system patches and updates through the use of a patch management life-cycle. Smartronix' Cloud Assured team performs monthly patching of guest operating systems based on the vendor release schedule. Maintenance and patching windows are coordinated with each customer to ensure operations are not impacted by system patching. The patching capability is a scripted process that will trigger the guest OS to download and apply the identified guest OS patches. The applied patches are tracked through the Cloud Assured MSP system to track system configuration. Critical or security related patches are quickly escalated to the customer for approval to deploy during an out of cycle maintenance window.

Customers can opt-in (patch and update) or opt-out (do not patch, do not update) individual systems via the instance tag.

Supported Operating Systems include:

- Amazon Linux 2015.03+
- RedHat Enterprise Linux
- CentOS 6/7
- Ubuntu 12.04/14.04 LTS
- Windows 2008-2016

2.1.5 Host Based Anti-Malware Management Service

Smartronix' Anti-malware (AMS) Management Service protects your environment against malware (viruses, trojans, spyware/grayware) by ensuring that the CAMS-G provided antimalware is installed, up-to-date, active, and is running current malware signatures on managed OS instances. When malware is detected, we proactively ensure quarantine and

automatically create an incident ticket for the remediation of the issue. Audits are performed to ensure individual server compliance with customer antimalware policies.

The service is provided through a consolidated management framework. Smartronix' Cloud Assured MSP offering leverages distributed relays and customer policy-based isolation. The AMS functionality is currently provided by the TrendMicro Deep Security Suite (DSS). Smartronix deploys the Deep Security Agent (DSA) on the customer guest OS image. These instances are registered through the customer DSA relay and transmitted through encrypted IP-restricted transport to the Cloud Assured Deep Security Manager (DSM). Through the DSM, policies are applied to customer agents to ensure signature updates are applied as soon as available to enable up-to-date protection of customer systems. Customers can request custom agent exclusions through the Cloud Assured ServiceNow portal.

The anti-malware service protects against many file-based threats, including the following: Viruses (file infectors), Trojans, Backdoors, Worms, Network, Rootkits, Spyware, Grayware, packers, and keyloggers.

Note: For DoD IL4 environments the CAMS-G provided antimalware and host IPS solution is an approved DoD Host Based Security Solution.

2.1.6 Boundary Management

Smartronix' Boundary Management (BM) Service is a proactive monitoring and management service providing configuration management of cloud service provider components for networking, firewalls, virtual private networking (VPN), subnets, access control lists (ACLs), and virtual networks.

Our Cloud Assured team will manage and monitor boundary protection and cloud environment network operations to ensure a secure and highly-available environment for customer data and applications. The BM service identifies, mitigates, and implements network level changes in response to events or customer requests. Supported change requests include VPN tunnel configuration, firewall policy changes to ACLs, IP route configurations, public IP allocation for service advertising, deployment of load balancing capabilities, and deployment of new cloud IP subnets. Technologies used in support of boundary management include:

- VPC Flow Logs
- CloudWatch Events
- M&N for ACL and Security Group changes

2.1.7 Log Aggregation Service

Smartronix' Log Aggregation (LA) Service captures cloud service provider logs, guest OS logs, and network logs. Alerts are generated for critical events and key performance indicators within the environment, which then automatically trigger an operational response.

Using the LA Service and Smartronix' change management process, the Cloud Assured team monitors the IaaS environment for possible security incidents through event filters and alerts, and performs change management of event filters implemented to ensure known critical events are identified and escalated. This service is filter-driven by a set of unwanted event

types. These events include items such as cloud infrastructure configuration changes, instance termination, and excessive CPU utilization. These event filters are customized through-out the MSP term as patterns develop from lessons learned specific to the customer's applications.

Please note that log correlation, advanced search, and analysis is not part of this service – see Security Services – Enhanced Log Aggregation and Analysis. Technologies used in support of log aggregation include:

- CloudTrail Logs
- OS Logs (SSM required)
- VPC Flow Logs
- S3
- ELB
- ALB

2.1.8 Backup and Restoration

Smartronix' Backup (BU) Services include system, configuration, environment and cloud services backup and restore. Backups are created and stored in the customer's cloud environment and data storage costs associated with backups are part of the customer cloud environment operating costs.

BU Services includes scheduled point in time disk volume snapshots to backup iterations of the storage volume. The service can be customized to retain backups for a customer-specified duration. The duration of backup retention will have an impact on cloud storage costs. Through the ITSM process, the Cloud Assured team can restore system volumes to a customer-specified point-in-time. Prior to restoration of the requested volumes, a new snapshot will be captured to ensure a rollback is available if the restore is unsuccessful. Backup and restore testing is performed annually to ensure backup consistency.

2.1.9 Infrastructure Provisioning

Smartronix Infrastructure Provisioning (IP) services ensure consistent and repeatable deployment of cloud infrastructure. Customers submit IP requests through the Cloud Assured ITSM portal for any service that requires management. Smartronix receives the requests, confirms the requirements, provisions the resource, and instruments the resource to ensure any core or additionally procured managed service is configured appropriately for M&N, SLA, ER&IR, AMS, BU, PM, and LA services.

Core Infrastructure Provisioning covers:

- Compute
- Storage
- Boundary Configuration
- Identity and Access Management Credentials
- Load Balancers

- Workspace provisioning

2.2 Optional Services

2.2.1 CSEM Advisory

The Smartronix Cloud Service Expense Management (CSEM) Advisory Service facilitates environmental cost optimization based on actual usage data aggregation and correlation. Recommendations are based on analysis of CSEM actuals; application of advanced tool sets to model future spend as a function of utilization and execution of "what-if" scenarios; familiarity with customer workloads and environments; and, extensive experience across customer cloud environments. The CSEM Advisory Service is included as an integrated component of the Cloud Resale and Consolidated Billing Service. Examples of cost optimization opportunities include:

- Resource utilization (Throttling under-utilized instances; Parking off-period resources)
- Right-sizing instance type
- Selection of workload-appropriate pricing models
- Resource tagging
- Reclamation of orphaned resources
- Optimization of BYOL (Bring-your-own-license)
- Storage life-cycle management
- Cost Monitoring and Alerting

This service requires deployment of the Smartronix CSEM tool which requires read only access to the CSP billing data and optional read only access to performance data (for service utilization optimization.)

2.2.2 Infrastructure Advisory

Smartronix' Infrastructure Advisory (IA) Services provides prescriptive guidance on cloud services optimization, including capacity management reviews, architectural reviews and best practices reviews, auto scaling tuning, and migration paths for on premise workloads. These reviews leverage our Cloud Assured - Well Architected guidelines and ITSM process.

The Cloud Assured - Well Architected Review is a detailed analysis of your infrastructure, a thorough review of security practices, application integration architectures, and sizing of resources. This review enables Smartronix' Cloud Assured team to ensure customers are leveraging cloud services in line with CSP best practices while delivering cost effective and secure service delivery.

2.2.3 Disaster Recovery

Smartronix' Disaster Recovery (DR) Service defines a DR architecture and processes to provide full planning, annual testing and execution of a managed disaster recovery solution encompassing applications, systems, and environments. Our Cloud Assured team will work with you to ensure your Recovery Time Objective/Recovery Point Objective (RTO/RPO) are appropriate to your mission and to architect the solution to fulfill the requirements at the lowest cost.

2.2.4 Advanced Monitoring

Smartronix' Advanced Monitoring (AM) Service provides deeper visibility into your entire environment. Using header tags, synthetic transactions, agent based heath tools, and state-of-the-art tools, processes, and best practices, the Smartronix Cloud Assured team will configure advanced monitoring to discover and optimize a comprehensive suite of availability and performance metrics.

2.2.5 Application Management

Smartronix' Application Management (AM) Service delivers COTS and custom-built applications under the managed Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) model. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

2.2.6 Database Management

Smartronix' Database Management (DBM) Service is a full-lifecycle capability available for industry- leading RDBMSs. This includes monitoring, maintenance, backup and restore, configuration management, patching and security assessments, and is designed to meet specific availability and/or performance SLAs.

2.2.7 Web Management and CDN

Smartronix' Web Management and CDN (WMC) Service provides monitoring, availability, maintenance, security and configuration management for web applications and frameworks, including the operations and management of third party CDN services. We provide proactive security monitoring of the site distribution, availability monitoring, maintenance, configuration management, patching and security of the environment and applications. External availability and performance monitoring is also available.

2.2.8 Help Desk

Smartronix' Help Desk (HD) provides front line (Tier 1) support for end users in your organization. Smartronix' Cloud Assured team user support specialists create and track issues from report to resolution, collecting and documenting circumstances, researching and recommending resolution activities, and ensuring customer satisfaction or timely escalation for prompt closure.

2.2.9 Workspaces Management

Smartronix' Workspaces Managed Services (WMS) brings server-class management and assurance to virtual desktop users. WMS includes operating system patch and update management, software packaging, and software lifecycle management (deployment, configuration management, updating, and deprovisioning). Workspaces Management Services Backups let you choose an RPO that's right for your organization and know that your virtual workstation data is protected. Antivirus and antimalware are included, and compliance is enforced. Integration with your existing directory service means organizational configurations, policies, and controls are applied to your Workspaces and managed by Smartronix WMS the same as they are for your servers.

2.2.10 Elastic Map Reduce and Redshift Management

Smartronix' EMR and Redshift Support (ERS) Service provides enhanced visibility into your running AWS big data environment. Using tags and monitoring capabilities designed specifically for Amazon EMR and Amazon Redshift, the Smartronix CAMS-G Cloud Management platform alerts on exceptions and abnormalities, provides proactive notification to client contacts, and expedites troubleshooting and administrative support.

ERS is priced on a per cluster / per month basis, and covers the following health, security, availability, cost, and performance dimensions:

- Cluster Management
- Cluster RI analysis
- Snapshot management and restore
- Add or remove cluster nodes – ad hoc requests
- Database Audit Logging
- Resize requests
- Cost optimization
- Capacity monitoring / Disk Space Alarm management
- User Management / Permissions Management (GRANT/REVOKE etc.)

ERS support also provides the extra level of expertise, consultancy, or staffing needed to meet your most complex and sophisticated usage scenarios. We support customers from the small businesses to large enterprise and public sector, and can offer a customer-specific solution priced to match your needs and customized to your environment.

ERS support services for Amazon EMR and Amazon Redshift include:

- Version upgrade support
- Database upgrade support
- Table resorts
- Cluster renaming and resizing
- Enhanced VPC Routing support and Endpoints
- Table level restores
- Database Encryption
- Key Rotation
- Query / Load Performance monitoring
- Performance optimization
- Log management (Connection, User, User Activities)
- Schema creation
- Workload management configuration

- Schema management
- Troubleshooting and Break Fix support

2.3 Optional Managed Security Services

2.3.1 Security Incident Response

Smartronix' Security Incident Response (SIR) Service provides analysis, tracking, and corrective actions for issues impacting customer environments. Smartronix' Cloud Assured team will support the incident response process through incident escalation, break/fix remediation of infrastructure and guest operating systems, support of in-scope disaster recovery, system restore, instance isolation, and event information reporting related to the cloud environment and guest operating systems. The Cloud Assured IR capability can also be leveraged by customer application teams to help identify application-impacting problems related to the environment or guest operating systems.

2.3.2 Enhanced Log Aggregation and Analysis

Smartronix' Enhanced Log Aggregation and Analysis (ELAA) Service is captures all events, logs, audit information and monitoring information provided by operating systems, platforms, networks, applications and infrastructure. Alerts are defined for key events within the environment to trigger further analysis or incident response.

ELAA extends the core *Log Aggregation* service by integrating search capabilities, counters, and proactive log review analysis. The *Analysis* capability enables the correlation of events by generating a process chain. For example, a web site health check failure can be linked to a john.doe login and a john.doe action of stopping the web service. The standard Log Aggregation event filter service will only identify the user logged on, the user stopped a service, or the web health check failed, but the causality link between events would be a manual process. The search capability also enhances the ability of the customer's applications teams to quickly identify underlying system events linked to a service incident.

2.3.3 Security and Regulatory Compliance Advisory

Smartronix' Security and Regulatory Compliance Advisor (SRCA) Service utilizes Global Intelligence for security and threat analytics to provide clients guidance in regulatory requirements and recommend mitigation of threats that have potential to impact client-specific environments as they appear and evolve. Email notification is provided the day of significant threats are surfaced in industry analyses.

Monthly Summaries are provided by the 10th day of the following month.

2.3.4 Enhanced Data Encryption

Smartronix' Enhanced Data Encryption (EDE) Service is a custom solution. Smartronix' Cloud Assured team works with the customer to define a service architecture compliant with their regulatory or policy requirements, and then implements the architecture with encryption built-in. The CAMS-G team provides all support for encryption key management and rotation, encryption of volumes and data, and implementation and management of service encryption certificates.

Areas of applicable support include:

- Use of cloud or collocated hardware security modules
- Database, disk volume, object store, and/or application level encryption
- End-to-end security – data ingestion, data at rest, data in transit, data in use, and data extraction
- Certificate management for secure protocols (SSL, HTTPS, TLS, etc.)
- Key lifecycle management (creation, deployment, expiration, rotation, invalidation)

Note: For DoD IL4 environments the solution will use an approved DoD IL4 encryption (such as AWS KMS and Azure Key Vault) for enforcement of cloud virtual server volume, data base, and object storage encryption.

2.3.5 Advanced Security

Smartronix' Advanced Security (AS) Services is a custom solution. Our Cloud Assured team works with your security organization to implement layered, comprehensive protection against data loss, advanced identity management services, host based intrusion detection/intrusion prevention solutions (IDS / IPS / HIPS), security assessments, security vulnerability scanning, and continuous security monitoring. AS Services is a foundational capability for creating high security enclaves in cloud environments.

2.3.6 Assured Compliance Assessment Solution (ACAS)

Smartronix' ACAS Service utilizes Tenable's Nessus Security Scanner and Nessus Security Manager. The ACAS service enables the assessment of networks and connected IT systems against DoD standards and identifies any known system vulnerabilities, the solution offers automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery.

3 SERVICE LEVEL AGREEMENTS

3.1 SLA 1: System Availability

SLA 1: "System" Availability	
Description	This SLA applies to "system availability" of a service. A system is considered a series of components that make up the infrastructure service that hosts and provides the compute and storage capabilities consumed by the customer applications and services. System availability applies to the following products and services: Virtual Compute Instances (AWS EC2 and Azure Virtual Machines deployed in the same availability set) Block Storage (AWS EBS, Azure System/Data Disks) Smartronix SLA incorporates the AWS and Azure SLA terms defined below which are subject to change in accordance with the AWS and Azure Agreements. AWS Compute SLA: https://aws.amazon.com/ec2/sla/ Microsoft Azure Compute SLA: https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_6/
Measurement	Smartronix will measure system infrastructure availability by using tools that will access the cloud infrastructure compute availability at 5 minute intervals to analyze cloud IaaS regional compute availability.
Calculation	NUMERATOR Uptime (Seconds) ÷ DENOMINATOR= Total amount of time (seconds) for the monitoring period = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if the system is fully available for use 99.95% of the time.
Exceptions / Conditions	Instances scheduled to occur during the following periods are excluded from the Numerator and Denominator for calculation purposes: Downtime approved by customer; and Downtime due to events outside Smartronix control and approved as such by customer. Examples of these type of exception events include: Force majeure events; and Outages determined to be caused by customer or customer contractor-developed application code provided by customer. Systems must be implemented in a functional high availability configuration.

3.2 SLA 2: Backup and Restoration

SLA 2: Backup and Restoration	
Description	This SLA measures the percent of times that the platform is restored to last agreed and documented state and last transactional dataset after failure, data loss or user request for restoration.
Measurement	Initiation of restore for individual file or database requests within 8 hours of receipt of request or notification of failure

SLA 2: Backup and Restoration	
	Backup retention periods are defined by Client.
Calculation	NUMERATOR: Number of successful restore initiations within 8 hours or Number of full restoration within 48 hours ÷ DENOMINATOR: Number of Requests for Restores = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully restored 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLAs may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

3.3 SLA 3: Incident Response

SLA 3: Incident Response Time	
Description	This SLA measures Smartronix' response time, per the Exceptions/Conditions in this SLA, following issue identification.
Measurement	SLA attainment is validated by 100% inspection of reporting documentation.
Calculation	NUMERATOR: Number of incident receiving response within time for given severity level ÷ DENOMINATOR: Total number of Incidents = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is successful if 95% of incidents receive a response within response time for given severity level, as measured on a monthly basis.
Exceptions / Conditions	• Severity 1 - Critical - An entire service is down. All users affected. Within 1 hour of incident occurring 24x7x365. • Severity 2 - High - Operation of the service is severely degraded, or major components of the services are not available. Significant user impact. Within 2 hours of incident occurring 24x7x365. • Severity 3 - Medium - Some non-essential features of the service are impaired or subject to interruptions while most vital components of the service remain functional. Minimal user impact. Within 24 hours of incident occurring during business hours. (8am-8pm EST M-F). • Severity 4 - Low - Errors that are minor and clearly have little to or no impact on the normal operation of the service. No or minimal user impact. Within 1 business day of incident occurring during business hours. (8am-8pm EST M-F). • Exception: Impending events notification - incident response will be initiated before follow-up notification as clients will be previously notified (SLA 5) of the likelihood of the event.

3.4 SLA 4: Operating System Patching and Updating

SLA 4 – Operating System Patching	
Description	This SLA measures Smartronix' ability to patch all operating systems protecting on a planned schedule. All critical patches will be applied in accordance to the client planned schedule that will be defined in the Concept of Operations document. All other patches will be executed upon a customer pre-approved schedule.
Measurement	All operating systems will be up to date with critical patches within 10 days of release and measured by scanning with vulnerability software.
Calculation	NUMERATOR: Total number of patched systems within 10 calendar days of critical patch release ÷ DENOMINATOR: Number of systems requiring patches = RESULT: Service Level (%) Attained.
Success Criteria	Smartronix is considered successful when 95% of critical patches are applied to the initial environment within 10 calendar days of release from vendor and subsequent patches are applied per the customer patch schedule. Patches must be approved by customer. This will be measured on a monthly basis.
Exceptions / Conditions	Ten (10) day SLA applies to the initial environment patched. Patching of subsequent environments follow customer patch schedule. Smartronix failure to execute patching of subsequent environments per customer patch schedule shall also be considered an SLA failure for purposes of the Calculation. Any patches not approved by customer or Smartronix' CCB are excluded from the SLA Calculation.

3.5 SLA 5: Impending Event Notification

SLA 5 – Impending Event Notifications	
Description	Smartronix will notify the customer of the possibility of an impending event or events that have occurred which might affect system operation. Examples include cloud service provider notifying Smartronix of service degradation, service unavailability, or service termination.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending event.
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

3.6 SLA 6: Database Management Service Request

SLA 6 – Service Request – Database Management	
Description	Smartronix will initiate requested support on-demand functions for Database support made by the customer within one business day. Examples include request for database refresh from prod to Test or development, launching database instances, preforming performance analysis.

Measurement	Smartronix will measure request response based on the time requested as documented in the ITSM reporting system and the request initiation being within 1 business day.
Calculation	NUMERATOR: Number of successful request initiations within 1 business day ÷ DENOMINATOR: Number of Requests = RESULT Service Level (%) Attained.
Success Criteria	Smartronix will be considered successful if successfully initiated responses 95% of the time as measured on a Monthly basis.
Exceptions / Conditions	SLA's may not be met during Client Disaster Recovery and Client Disaster Recovery exercises, during those periods best effort will replace the SLA.

3.7 SLA 7: Impending Security Threat Notification

SLA 7: Impending Security Threat Notifications	
Description	Smartronix will notify the Client of the possibility of an impending Security Threat or events that have occurred which may impact system operation. Examples include global intelligence sources identifying new threats in the environment that may impact OS, Applications, or services used by Client.
Measurement	Smartronix will measure impending event notification based on reporting within 1 hour of detection of the event or impending threat
Calculation	Best Effort. Availability SLA ultimately determines client access to the system or service.
Success Criteria	N/A
Exceptions / Conditions	Events outside of Smartronix control are not included.

*SLA usage can vary dependent on services purchased.

4 PRICING

Table 4. Core Managed Services.

Service Title	Price
Monitoring and Notification	$292.18/instance per month
SLA Management	
Incident Response	
Operating System Patch Management	
Antivirus (AV) Management	
Boundary Management	
Log Aggregation (Basic)	
Backup Services	
Infrastructure Provisioning Service	$48.86/Provisioning Request

Table 5. Optional Services.

Service Title	Price
Cloud Service Expense Management Advisory Service	1.25% of Invoice monthly Or provided as part of Resell Bundle
Infrastructure Advisory Services	Priced based on scope.
Disaster Recovery Services	Price based on request
Advanced Monitoring Services	$97.73/ instance / month
Application Management Services	$293.18/ instance / month
Database Management Services	$390.91/ instance / month
Web Management Services and CDN	$390.91/ site distribution / month
Elastic Map Reduce and Redshift Management	$4,886.38/ cluster / month
Workspaces Management Services	Tier per Workspace Instance Fee / month • $24.43 Per less than 150 Instances • $22 for 150 through 300 • $18 for 300 through 700 • $14 Greater than 700

Table 6. Optional Security Services.

Service Title	Price
Security Incident Response	Priced based on scope.
Enhanced Log Aggregation and Analysis	Log Monitoring and Analysis - $312.73/per GB of indexed data, based on average daily consumption in a month.
Security & Regulatory Compliance Advisory Service	$5,863.65/month
Enhanced Data Encryption Services	Price based on request
Advanced Security Services	$146.59/ instance / month
ACAS	$2,443.19/per month block of 50 instances

Table 7. DoD IL4 Managed Services.

Service Title	Price
Monitoring and Notification	$518.86/instance per month
SLA Management	
Incident Response	
Operating System Patch Management	
Host Based Antivirus (AV) Management	
Boundary Management	
Enhanced Log Aggregation and Analysis	
Backup Services	
Enhanced Data Encryption Services	
ACAS	
Infrastructure Provisioning Service	$48.86/Provisioning Request

Notes:

- Customized service/pricing for customer environments that have reduced requirements, e.g. Development, Test, Quality Assurance, or Labs is available.
- Clients are required to enable Config, CloudTrail, CloudWatch, and allow SMX to install AWS CloudWatch agent and AWS Inspector Agent on managed instances in regions that run services supported by Smartronix.
- Smartronix will reserve one AWS resource tag for use in the management of the resources.

4.1 Discount Schedule

Monthly Cost	Discount Tier
$0 - $15,000	0%
$15,001 - $30,000	2.5%
$30,001 - $45,000	5%
$45,001 - $60,000	10%
$60,001 - $100,000	12.5%
$100,001 - $500,000	15%
$500,001 -$1,000,000	17.5%
Over $1,000,001	20%