AMENDMENT No. 3 TO
GETS Ready - Unisys
CONTRACT NUMBER: 98000-RFQC-1647-UNI

This Amendment No. 3 is made on June 1, 2020 by and between the **GEORGIA TECHNOLOGY AUTHORITY** ("GTA") and **Unisys Corporation** ("Service Provider").

WHEREAS, heretofore GTA entered into that certain agreement for services effective on March 2, 2018, with respect to certain services to be provided to GTA by Service Provider, as more particularly described therein.

WHEREAS, the parties wish to amend the agreement to reflect certain changes.

NOW, THEREFORE, in consideration of the promises, the terms and conditions stated herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereby **agree** as follows:

1. **Scope.** The Agreement is hereby amended to modify the Services and Pricing described within this Amendment 3. The current Exhibit 1 (Catalogue of Services, Service Levels, and Pricing) for Unisys Managed Security Services (MSS) is hereby deleted and replaced in its entirety with Exhibit 1 (Catalogue of Services, Service Levels, and Pricing) for Unisys Managed Security Services (MSS), attached hereto and made a part hereof as though fully set forth herein.

2. **Definitions.** All capitalized terms used herein and not expressly defined herein shall have the respective meanings given to such terms in the Agreement.

3. **Successors and Assigns**. This Amendment No. 3 shall be binding upon and inure to the benefit of the successors and permitted assigns of the parties hereto.

4. **Entire Agreement.** Except as expressly modified by this Amendment No. 3, the agreement shall be and remain in full force and effect in accordance with its terms and shall constitute the legal, valid, binding and enforceable obligations of the parties. This Amendment No. 3 and Amendments No. 1 and No. 2, collectively, are the complete agreement of the parties and supersede any prior agreements or representations, whether oral or written, with respect hereto.

IN WITNESS WHEREOF, the parties have caused this Amendment No. 3 to be duly executed by their authorized representatives as of the date set forth above.

Unisys Corporation

DocuSigned by:
By: Michael Kreager
5F9E4D291F5B41B...

Name: Michael T. Kreager

Title: Client Executive

Date: 5/14/2020

GEORGIA TECHNOLOGY AUTHORITY

DocuSigned by:
By: Mark Latham
11D69D05F85B4BB...

Name: Mark Latham

Title: sourcing governance officer

Date: 5/21/2020

Unisys Managed Security Services (MSS)

Contract Number: 98000-GETS Ready-RFQC-1647-UNI

Service Descriptions and Cost
GTA GETS Ready Contract
(Now known as the GTA Direct Contract)

Managed Security Services Monitoring
Managed Security Service Security Device Management for Firewalls
Managed Security Service Security Device Management for Intrusion Detection/Prevention Systems
Managed Security Service Vulnerability Management
Managed Security Service and Stealth™
Managed Security Consulting Services (Per Amendment #1)

Table of Contents

This document is designed to provide the State of Georgia Entity ("Client") detail behind the Unisys Services that are listed on the GETS Direct (formerly GETS Ready) Contract.

Unisys Managed Security Services (MSS)

As businesses extend their IT organizations into clouds and virtual environments to drive down IT costs, many find substantial challenges in the form of advanced security threats, while at the same time maintaining compliance and assessing the overall security risk. Protection of information distributed throughout the enterprise requires a holistic, comprehensive and integrated security strategy – one that includes solutions for protecting IT assets, securing cloud applications, mobile devices and safeguarding intellectual property.

The Managed Security Services (MSS) division of Unisys will provide the Client best-in-class support from Augusta, GA. With years of experience in the field, Unisys provides direct access to subject matter experts in various word-class security technologies and well-tuned processes that help businesses. Besides providing some of the best security services, the Unisys MSS also provides traditional remote device management of security devices.

Unisys Managed Security Services deliver comprehensive real-time protection solutions – Security Information and Event Management (SIEM), Security Device Management (SDM), Vulnerability Management (VMS), Stealth™ Services, as well as Governance Risk & Compliance (GRC), Managed Identity and Access Management Services (IAM) and Cloud Services, helping organizations to manage overall risk, improve their security posture, prevent emerging threats and demonstrate compliance in a cost-effective manner.

1. Unisys Security Monitoring Service

Unisys Security Information and Event Management (SIEM) Services delivers comprehensive cross enterprise protection by unifying event management and incidents management across towers on a common platform.

Unisys SIEM service incorporates Unisys Noise Cancellation Advanced Analytics Platform (UNCAAP) technology, developed over many years to identify events of interest arising from the ever-evolving threat landscape. It provides the essential feedback loop to senior management on the performance and cost effectiveness of their IT Security program. UNCAAP minimizes false alarm rates and offers advanced forensics & analytics including actionable intelligence, decision support and aids in executing our clients' security strategies.

The Security Event Management Service provides the following functionality:

1.1 Log Retention and Log Management Service

Log Retention and Log Management Service provides Log Collection and retention, information searches, reporting, alerting and real-time information displayed via dashboards, to meet specific compliance requirements. The service consists of:

1. Log Collection - Collecting security event data, log and machine data and forensic sensor data (host and network).
2. Log Storage, retention and archival policies –
   - Online raw data: 14 days active data and 351 days archive storage
   - Metadata: Logs are stored for one year.
   - Archive storage: Logs are stored for one year.
3. Log Search - Provide a dedicated Web Console to allow clients to perform forensic searches against all their log data.
4. Log Reporting - Provide out of the box or custom reports. The SIEM platform currently has over 1250 pre-defined reports plus 170 additional templates that can be used to create an unlimited number of reports automatically. The reports provide Auditing, Security and Operations summaries, details, "most frequent/most used" lists, and specific reports for compliance.

1.2 Cyber Threat Intelligence

Security is only as effective as the security intelligence it is based on. Overcoming zero-day security challenges requires security intelligence from a number of trusted threat sources focused on a multitude of threat vectors. To meet these requirements, Unisys has combined multiple key SIEM ingredients powered by LogRhythm technologies into a Security Monitoring offering. This allows Unisys to offer a cost effective SIEM Solution, including the benefits of our Threat Intelligence and Advances Security Analytics to a broader base of customers.

Unisys provides Threat Intelligence Services in accordance with our policies and standards. Unisys delivers Threat Intelligence Services utilizing intelligence gathering sources and actionable intelligence designed to assist with highly valuable decision-making and operational analysis.

1.3 Advanced Security Analytics

Unisys Advanced Security Analytics analyzes data and assess the threats to determine the risks and if a full investigation is necessary. In coordination with Cyber Threat Intelligence, Unisys uses Advanced Analytics to analyze Client security events from Client Devices for security threats to the Client IT Infrastructure using Unisys baseline security policy to aggregate and correlate security events for in-scope Devices into actionable events.

1.4 Incident Response and Orchestration

Unisys takes the market leading and proven LogRhythm technology and integrates our Threat Intelligence and Advanced Security Analytics and couples them with our Incident Response and Orchestration processes to offer a robust all-around solution for our clients, all in one package.

Unisys believes that Threat Intelligence Services are required to ensure that the security services provide are based on the most comprehensive, accurate, and actionable intelligence available. This includes the insight gained from integrating SIEM with the best threat intelligence feeds available.

The service consists of:

1. Security Incidents Investigation – Incidents categorized as requiring further investigation are analyzed in more depth. Unisys hunts for Indicators of Compromise (IoC), analyzes the threat and determines the nature and extent of the incident.
2. Security Incident Response – Unisys will notify the Client of the incident and provide associated information relating to how to mitigate the threat and associated risk by implementing suitable countermeasures. Where possible and appropriate, those countermeasures are platform, with appropriate levels of authorization, utilizing integration with other technologies such as NAC, Firewalls, AD and Unisys Stealth® to quarantine devices, block traffic or disable user accounts.

1.5 MSS Monitoring Service Cost

Monitoring Packages (per year) - US Based Resource						
MPS Volume	**(S) 100-250**	**(P1) 250-500**	**(P2) 501-750**	**(P3) 751-1000**	**(P4) 1001-1250**	**(P5) 1251-1500**
Total Package Price per Year	**$57,554**	**$90,681**	**$116,968**	**$146,162**	**$174,595**	**$200,544**
Packages Include						
Labor Source	100% On-Shore (US based)					
Log Archive Storage per Year	75GB	250GB	400 GB	500 GB	750 GB	1 TB
Standard Reports:	5	5	5	5	5	5
Customer may select from standard available LogRhythm reports						
1 compliance pack						
Monitoring Agents	Pro Agents – 1 Lite Agents – 2	Pro Agents – 2 Lite Agents – 3	Pro Agents – 3 Lite Agents – 4	Pro Agents – 5 Lite Agents – 6	Pro Agents – 5 Lite Agents – 9	Pro Agents – 6 Lite Agents – 10
Restrictions						
Datacenters	Up to 2 Client Sites					
Average Number of Incidents per Month	3	10	15	20	25	30
One-Time Price for Additional Compliance Packs (up to two max)	Not Available	$50	$100	$150	$200	$250

*MPS Volumes above 1500 will require a custom quote

2. Unisys Security Device Management (SDM)

The Security Device Management service provided by Unisys covers the following device types.

- Firewall devices
- IPS devices
- IDS devices
- IDS devices
- UTM devices
- VPN appliances
- Web proxy appliances
- Load balancer appliances.

These devices are accessed and managed remotely over a dedicated management network. Depending on the device, management is performed via a purpose-build management station (e.g., Provider-1 for Checkpoint) or via a dedicated Terminal Server, located on a client site or in a Unisys SOC, using HTTPS or SSH for secure communications. Connectivity between a client's site and the Unisys SOC is provided via a secure Site-to-Site VPN over IPsec or MPLS.

2.1 Security Device Management Services

The Unisys Service Device Management (SDM) services consist of:

- Centralized and Remotely Managed Security Device Management Services
  - Incident and Change Management Services
  - Configuration Management Services
  - Problem Management Services
  - Knowledge Management Services
  - Vendor Management Services
- Reporting Services

Security device management includes system monitoring of a device, including availability and system health.

2.2 Device Management Activity Summary

Exhibit 1 shows a Security Device Management Activity Example.

Activity	Sub-tasks
Incident Management	Device up/down status updates Interface up/down status updates
Change Management	Modify system settings Modify system policy Modify other device configuration Perform content updates Perform firmware/OS updates Perform user access management activities
Configuration Management	Define configuration item Identify and register configuration item (CI) Perform CI Audits Configuration Management Database (CMDB) change control
Problem Management	Identify problem or recurring incidents Perform root cause analysis If problem identified with Unisys managed device, work towards giving a permanent fix to the problem with vendor support
Knowledge Management	Maintain knowledge base

Activity	Sub-tasks
Vendor Management	Track and update support contracts Work with vendor to get bug fixes Escalate issues to vendors and follow up until a fix has been found

Exhibit 1. Device Management Activity Summary Example

2.3 Architecture of Security Device Management service

The following section provides the high-level architecture of security device management service. This section focuses on the various components used to provide the security device management service and summarizes their functions.

Security Device Management Component	Description
Managed Device	Any of the supported security devices that are serving client infrastructure and are under sole management of Unisys. The list of supported device types is given in the previous section.
Management Station	The Palo Alto Panorama Management server, used to manage one or more managed devices over an in band management connection.
In Band Management	This is a process of managing a managed device using management station over a regular WAN connection, such as IPsec/Internet or MPLS VPN.
Unisys Security Operations Center (USOC)	This secure location houses Unisys security engineers and analysts, the management stations and portal servers used to provide the service over an in band or out of band management access connection.

2.4 SDM Services Cost – Firewall Price

Security Device Management (SDM) Firewall Packages One-Time Set-up Cost		
SDM Firewall Packages	New Firewalls	Existing Firewall Takeover
Small (1 -150 rules)	$ 5,357	$ 1,902
Medium (151-350 rules)	$ 5,556	$ 2,101
Large (>350 rules)	$ 6,264	$ 2,808

SDM Firewall Packages (US based resources) On-Going Support			
Description		Price per Month	Price per Year
Small (1 -150 rules)	2 Changes per Month	$ 1,761	$ 23,033
Medium (151-350 rules)	5 Changes per Month	$ 3,829	$ 48,045
Large (>350 rules)	8 Changes per Month	$ 6,138	$ 76,462
Price per Additional Change per Month		$ 566	$ 6,796

2.5 SDM Services Cost – Intrusion Detection/Prevention Systems (IDS/IPS)

Security Device Management (SDM) IDS/IPS Packages One-Time Set-up Cost		
SDM IDS/IPS Packages	New IDS/IPS Set-up	Existing IDS/IPS Takeover
Small (3 Changes/Month)	$ 4,871	$ 1,415
Medium (10 Changes/Month)	$ 5,092	$ 1,636
Large (18 Changes/Month)	$ 5,191	$ 1,736

SDM IDS/IPS Packages (US based resources) On-Going Support		
Description	Price per Month	Price per Year
Small (3 Changes/Month)	$ 1,791	$ 21,489
Medium (10 Changes/Month)	$ 4,977	$ 59,729
Large (18 Changes/Month)	$ 8,785	$ 105,419
Price per Additional Change/Month	$ 441	$ 5,293

3. SDM IDS/Unisys MSS Cloud Based Vulnerability Scanning & Remediation Support Service

Unisys Cloud-Based Vulnerability Management Service will permit the Client to assess their server and infrastructure scanned devices for known vulnerabilities. These scanned devices can be either in the cloud or in the Client data centers.

Features:

- Supports Risk Management process
- Ensures compliance
- Custom fit/tailor made solution
- Agnostic in terms of vulnerability scanning tool
- Infrastructure – market leading tools such as Qualys, McAfee, Nessus and/or any other.
- Remote service components may be connected to client infrastructure in a Stealth™-enabled link
- Utilize combination of remote scanning and cloud based agents to meet specific requirements.
- Service options allow “one-off testing” or an annual subscription

Scanning Activities:

- Define scanning requirements
- Define technical requirements
- Execution of scans
- Reporting

Remediation support and coordination activities:

- Preparation of scan environment (Pre-Scan)
- Completion of preparation of Scan environment (Post Scan)
- Review of report by Unisys Security Officer
- Raise Incidents and Changes based on recommendations
- Incidents and Change closure tracking
- On-Demand Scanning and SAML Integration.

3.1 Vulnerability Management Services

Unisys will provide remote monitoring and management services for three (3) Qualys virtual scanner appliances. During each scan Unisys will follow a vulnerability management lifecycle which consists of the following phases:

1. Define scanning requirements. A discovery will be carried out to provide a list of devices to be scanned. The following will be identified during this scan-scoping activity:
   - Asset identification
   - Asset prioritization

- Asset changes
- Vulnerability assessment
- Vulnerability prioritization

2. Define technical requirements
   - Vulnerability scanning requirements
   - Unisys personnel that require access IDs

3. Network connectivity or limitations – to be reviewed with the Client
   - Execution of scans

4. Execute scans using the Qualys tool
   - Reporting

Unisys Security Officer will review the automated scan reports generated by the Qualys tool, prioritize the vulnerabilities, and provide vulnerability scan reports to the Client.

3.2 Remediation Support

1. Preparation of scan environment: before running a scan, the Unisys Project Manager will open a "Preparation of Scan Environment" Change Request in the Client IMS system to handle to flowing activities.
   - Open firewall ports
   - Prepare network changes for required scan environment readiness
   - Provide network data to the Client for VPN to their three (3) data centers
   - Provide the network access to Unisys
2. The Change Request will be kept open until the scan is completed.
3. Completion of preparation of scan environment: Unisys will coordinate with resolver groups to close "Preparation of Scan Environment" Change Request upon completion of scan.
4. Review of report by Unisys Security Officer: the scan reports will be reviewed by Unisys Security Officer. Severities will be identified and a recommendation report will be shared with the Client.
5. Raise Incidents and Changes based on recommendations from Unisys Security Officer: the Client will push the critical/high/medium vulnerabilities remediation via the Client Incident and Change management process.
6. Incidents and Change closure tracking: Unisys Project Manager will maintain a tracking log of open Incidents in the Qualys tool and provide a summary report for the Client review.

The above activities are repeated for a re-scan to identify and report against the remediation achieved in the Client environment. Remediation of any affected systems remains the responsibility of the Client.

3.3 Additional Steps of Remediation Process

1. Open a Remediation Ticket in the Client IMS system and notify the Client by assigning the
2. Ticket to the Client resolver group per the timeline identified by severity type.
3. Perform two follow-ups within the timeframe set forth in Section 7 (Service Level Objectives).
4. Maintain Remediation ticket in a pending status for the Client action after second (2nd) follow-up and then close per the agreed timeline with the Client. The Remediation ticket detail will remain in the incident tracking log maintained by the Unisys Project Manager.

The duration for which the Remediation ticket will remain open after the two (2) follow- up activities will be mutually agreed upon. It is important to note that any vulnerability for which a Ticket was raised but not remediated will reappear in subsequent scans.

3.4 Vulnerability Management Service Cost

VMS Packages (US based resources)			
Package Scope	**One-Time**	**On-Going Price per Month**	**On-Going Price per Year**
Scanning up to 256 IP's	**$2,864**	**$1,329**	**$15,948**
Scanning > 256 up to 512 IP's	**$3,044**	**$1,796**	**$21,548**
Scanning > 512 up to 1024 IP's	**$3,044**	**$2,475**	**$29,700**
Additional Qualys Scanner			**$ 995**

4. Unisys Stealth® MSS

Stealth™ Service Description

Unisys Stealth® provides a unique yet extremely effective mechanism, software defined micro-segmentation, to manage and continually adapt security for mission-critical enterprises. Realizing that merely defining static security policies is not effective – and is increasingly susceptible to advanced threats for our clients – Unisys takes a different approach to implementing and managing a micro-segmented environment.

4.1 Stealth™ Infrastructure Installation

- **Resource Unit Definition:** Installation of base infrastructure consisting of one (1) Stealth Enterprise Manager and two (2) Stealth Authorization Servers
- **Unit of Measurement:** One-time Charge per Client Site
- **Source of Measurement:** Not Applicable
- **Costs Included:** Labor for:
  - Installation of one (1) Stealth Enterprise Manager and two (2) Stealth Authorization Servers (the core components) in the Client Data Center(s)
  - Configuration of up to two (2) Communities of Interest (COI) to support encrypted communications

- Project Management for Installation
- Requires Stealth connectivity with Client's Active Directory scheme for user identity
- Client provides the hardware, virtualization, operating system, and necessary network and infrastructure required for the Stealth Enterprise Manager and Stealth Authorization Servers.

4.2 Stealth™ Agent Installation Support – Stealth Protected Endpoints

- **Resource Unit Definition:** Installation Support of Stealth Agent on client provided endpoints having supported Operating Systems
- **Unit of Measurement:** One-time Charge per Stealth Protected Endpoint
- **Source of Measurement:** Not Applicable
- **Costs Included:** Labor for:
  - Preparation of endpoint package for Stealth Supported Operating System
  - Coordination with the Client's Desktop Team for deployment to client endpoints of endpoint package through Client's Software Distribution Platform
  - Test and validate Stealth endpoint connectivity to the Stealth Authorization Server
  - Addition of endpoint into existing Stealth Community of Interest.

4.3 Stealth™ Agent Installation Support – Stealth Protected Servers

- **Resource Unit Definition:** Installation Support of Stealth Agent on client provided servers having supported Operating Systems
- **Unit of Measurement:** One-time Charge per Stealth Protected Server
- **Source of Measurement:** Not Applicable
- **Costs Included:** Labor for:
  - Preparation of Endpoint Package for Stealth Supported Operating System
  - Coordination with Client's server and application teams for deployment to client servers of server package through Client's software distribution platform
  - Test and validate Stealth server connectivity into the Stealth Authorization Server
  - Addition of server into existing Stealth Community of Interest.

4.4 Stealth™ Virtual Gateway Installation Support

- **Resource Unit Definition:** Installation Support of Stealth Virtual Gateway having supported Operating Systems
- **Unit of Measurement:** One-time Charge per Stealth Protected Virtual Gateway
- **Source of Measurement:** Not Applicable
- **Costs Included:** Labor for:
  - Installation of one (1) Stealth Virtual Gateway pair (primary/backup) in the Client Data Center(s). Client provides the Hardware, Virtualization, Operating System, and necessary network and infrastructure support required for the Stealth Virtual Gateway.
  - Configuration of Stealth Virtual Gateway to support up to ten (10) Stealth protected servers/endpoints protected by the Stealth Virtual Gateway.

4.5 Stealth™ Managed Service – Stealth Protected Endpoints

- **Resource Unit Definition:** Ongoing management of the deployed Stealth endpoint agents
- **Unit of Measurement:** Monthly Charge per Stealth Protected Endpoint
- **Source of Measurement:** Stealth Protected Endpoint
- **Costs Included:** Labor for:
  - Administration of as-built configurations in the Enterprise Manager. For example, adding a new endpoint to the Community of Interest
  - Ongoing endpoint package preparation and support for Client to deploy endpoint agents
  - Assistance with troubleshooting and root cause diagnosis
  - Stealth software maintenance (includes; new Feature Releases, Maintenance Releases and Interim Corrections)
  - Services delivered by North America based resources, Monday through Friday, 9am-5pm Eastern Time (8x5).

4.6 Stealth™ Managed Service – Stealth Protected Servers

- **Resource Unit Definition:** Ongoing management of the deployed Stealth Server Agents
- **Unit of Measurement:** Monthly Charge per Stealth Protected Server
- **Source of Measurement:** Stealth Protected Server
- **Costs Included:** Labor for:
  - Administration of as-built configurations in the Enterprise Manager, for example, adding a new Server to the Community of Interest
  - Ongoing endpoint package preparation and support for Client to deploy endpoint agents
  - Assistance with troubleshooting and root cause diagnosis
  - Stealth software maintenance (includes new Feature Releases, Maintenance Releases and Interim Corrections)
  - Services delivered by North America based resources, Monday through Friday, 9am-5pm Eastern Time (8x5).

4.7 Stealth™ Managed Service – Stealth Virtual Gateways, Service IP Address License Pricing

- **Resource Unit Definition:** Ongoing management of the deployed Stealth Virtual Gateway
- **Unit of Measurement:** Monthly charge per Stealth Protected Virtual Gateway
- **Source of Measurement:** per Stealth Protected Virtual Gateway
- **Costs Included:** Labor for:
  - Administration of Stealth Virtual Gateway configuration
  - Assistance with troubleshooting and root cause diagnosis
  - Stealth software maintenance (includes; new Feature Releases, Maintenance Releases and Interim Corrections)
  - Services delivered by North America based resources, Monday through Friday, 9am-5pm Eastern time (8x5)

4.8 Stealth™ MSS Cost

Unisys Stealth® Services			
Resource Unit Name	**Service Description / Included Features**	**Unit of Measurement**	**Price (per server / per month)**
Stealth™ Infrastructure Installation	**Remote installation of base infrastructure consisting of one (1) Stealth™ Enterprise Manager and two (2) Stealth Authorization Servers**	**One-time Charge per client site**	**$ 70,000.00**
Stealth™ Agent Installation Support – Stealth Protected Endpoints	**Remote installation support – Stealth agents on endpoints, Stealth supported operating systems only; distribution and installation of Stealth software is the responsibility of the Client.**	**One-time Charge per Stealth Protected Endpoint**	**$ 14.00**
Stealth™ Agent Installation Support – Stealth Protected Servers	**Remote installation support – Stealth agents on servers, Stealth supported operating systems only; distribution and installation of Stealth software is the responsibility of the Client.**	**One-time Charge per Stealth Protected Server**	**$ 173.00**
Stealth™ Virtual Gateway Installation Support	**Remote installation support - Stealth™ Virtual Gateway software, Stealth supported operating systems only; distribution and installation of Stealth software is the responsibility of the Client.**	**One-time Charge per Stealth Protected Virtual Gateway**	**$ 3,000.00**
Stealth™ Management Services - Stealth Protected Endpoints *	**Managed Service and Support - per Stealth Endpoint – 8x5 North America resources**	**Monthly Charge per Stealth Protected Endpoint**	**$ 9.25**
Stealth™ Management Services - Stealth Protected Servers *	**Managed Service and Support - per Server – 8x5 North America resources**	**Monthly Charge per Stealth Protected Server**	**$ 65.00**
Stealth™ Management Services - Stealth Virtual Gateways, Server IP Address License Pricing *	**Managed Service and Support - per Stealth™ Virtual Gateway – 8x5 North America resources**	**Monthly per installed Stealth Virtual Gateway**	**$ 890.00**

* Volume Discounts available based on larger quantity purchases.

5. Managed Security Consulting Services

Title	Description	On-Site Travel	Cost Including travel
Program Assessment [Small]	Conduct a cybersecurity program assessment of one agency or a similar function. The focus is adherence to GTA IT security policies (28+/- policies). Includes a Scoping Call, two Assessors with up to two weeks of on-site assessment (arrive Monday, leave Thursday or Friday) up to 500 questions/tests and physical security evaluation of two facilities (e.g. agency headquarters and a branch office). Assessment activity consists of interviews, observation of controls and documentation review. Deliverables include Assessment Report and Assessment Slide Deck. The presentation will be conducted remotely. Out of scope: Vulnerability scans, configuration reviews of system components and other methods of deep technical inspection. Dependency: Current GTA IT security policy assessment work papers established under a separate engagement (below).	4 trips	$85,005
Program Assessment [Medium]	Aligns to elements within the 'Program Assessment - Small' service. Intended for a medium or large-sized agency or similar function. Includes an additional week of assessment hours and a third trip to be used for additional on-site assessment activity.	6 trips	$83,119
Assessment Work Paper Creation	Create assessment work papers based on GTA IT security policies (28+/- policies). This is an add-on component to the Program Assessment service offerings. This service offering includes 120 hours with a Consulting Principal with 1 trip. Aligns to the 'Program Assessment - Small' service.	1 trip	$30,777
Assessment Work Paper Update	Update assessment work papers based on GTA IT security policies (28+/- policies). Intended to be used by the client annually as security policies are revised. This is an add-on component to the Program Assessment service offerings. This service offering includes 60 hours with a Consulting Principal with 1 trip. Aligns to the 'Program Assessment - Small' service.	1 trip	$16,488

Title	Description	On-Site Travel	Cost including travel
TrustCheck™ Annual Subscription	Unisys TrustCheck™ is a unique digitally transformed cyber risk assessment and management solution that offers an innovative, patented method for understanding financial exposure to cyber risk and making effective risk management decisions. TrustCheck brings the financial rigor trusted by the global insurance industry and automation to enterprise cyber risk management. • The TrustCheck Platform is always on and updated to allow modeling new risk scenarios whenever you need to – in stark contrast with legacy point-in-time risk assessment services. • TrustCheck is credibly calibrated and normalized, leveraging objective data analytics that billions of dollars of cyber insurance underwriting is based on. • TrustCheck delivers immediate feedback for senior business leaders and security teams in hours and days compared to other options requiring full time dedicated staff for months or even years before reliable results can be obtained. • TrustCheck combines both access to the platform and professional consultative services together during the subscription term. **Service Components:** • TrustCheck Setup Transition – once per site ○ Provisioning of the TrustCheck portal for use including setting up authorized users and access as well as initializing the portal environmental and variables for the site(s) included with the service. • TrustCheck Site Appraisal – annual per site ○ Collection, translation, and validation of data for risk modeling with TrustCheck through interviews and other means. Customer specific data set updates are completed on a negotiated frequency after initial setup transition (add-on services). Appraisals for different organizational units are considered a new site which incur additional Setup Transition, TrustCheck Site Appraisal, and TrustCheck Platform SaaS fees. • TrustCheck™ platform software as a service (SaaS) subscription fee ○ Access for up to five (5) users to the portal (described above). Additional sites may have up to three (3) additional users per site. Additional Details: https://www.unisys.com/offerings/security-solutions/trustcheck-cyber-risk-management Pricing: Unisys TrustCheck™ pricing is based on two primary components:		See Description for pricing

	• The Unisys TrustCheck Platform usage for the subscription term including platform application, analytics, and data updates. • Professional services such as initial site setup, baseline services, and optional add-on services for assistance during refreshes throughout the term of the subscription. Following are further details explaining TrustCheck pricing. • TrustCheck Platform fees are $49,000 per site per 1 year term. • TrustCheck Initial site setup and baseline services fees are $64,000 per site per 1 year term. Where a single organization purchases TrustCheck to cover more than one site, additional site setup effort often decreases but may vary based on client's desired level of services. Initial site setup and baseline services are not required after year one for the same client in a multi-year term. • Optional Add-on services are available in 40 hour increments at a rate of $325.00 per hour for a Consulting Manager. Example: A single site for a local government entity with initial site services plus quarterly add-on services for the remainder of the year (3 @ 1 week increments) - the price for a one year term would be $152,000.00. After year one, pricing for the TrustCheck Platform and ongoing quarterly add-on services (4 @ 1 week increments) would be $101,000.00 per additional year, exclusive of any travel and expenses for onsite visits. Final pricing is dependent on agreement of Statement of Work (SOW), scope and schedule. Consulting Principal - Experienced and specialized consultant to work directly with Senior Government Leaders and C-Suite executives to translate how IT and cybersecurity engagements they are performing influence their mission to provide services to the citizens they serve. The consultant will be responsible for taking the results of current and new IT projects, apply them to the goals and objectives of the executive branch and make recommendations for future IT projects. Rate $400.00 per hour. Consulting Manager - Experienced and specialized consultant who will combine research, analytics and technology to develop IT and cybersecurity trends within an organization. The Consulting Manager will have direct input working at times with the Consulting Principle to develop IT and cybersecurity strategies. Rate $325.00 per hour.		

Title	Description	On-Site Travel	Cost including travel
Program Development [Small]	Program Development support varies based on the needs of the agency or depending upon assessment findings. Examples of program development include process design, policy development and creation of documentation such as an Incident Response Plan or a Program Welcome Packet. Includes 40 hours with a Unisys Consulting Principal with 1 trip (arrive Monday, leave Thursday or Friday). NOTE: This offering is intended to provide a catalog entry for unique needs of the agencies which cannot be forecast. Also allows for existing service offerings to be customized. Includes a Statement of Work to clearly articulate requirements and deliverables.	1 trip	$ 11,726
Program Development [Medium]	Aligns to elements within the 'Program Development - Small' service. Includes 120 hours with a Consulting Principal with 2 trips.	2 trips	$ 32,977
Program Development [Large]	Aligns to elements within the 'Program Development - Small' service. Includes 200 hours with a Consulting Principal with 3 trips.	3 trips	$ 54,228
Security Awareness Briefing	Create and present a security awareness briefing. Provide a brief summary of threat actors with an overview of GTA IT security policies (28+/- policies). The briefing slide deck will be designed to be presented within 50 minutes, leaving 10 minutes for questions. One or more policies may be omitted based on risk severity and time allotted in consideration of the audience. Includes 40 hours with a Consulting Principal with 1 trip to conduct the presentation on-site.	1 trip	$ 11,726
Threat Landscape Briefing	Create a slide deck based upon the current Threat Landscape. Address threat actors, techniques for compromising data and the cybercrime ecosystem. The deck will be designed to be presented within 50 minutes, leaving 10 minutes for questions. Includes 40 hours with a Consulting Principal with 1 trip to conduct the presentation on-site.	1 trip	$ 11,726
Conducting a Cybersecurity Assessment Briefing	Present a briefing that addresses how to conduct a Cybersecurity Assessment. The deck will be designed to be presented within 100 minutes, leaving 20 minutes for questions. Includes 40 hours with a Consulting Principal with 1 trip to conduct the presentation on- site. Templates will be provided to attendees as well (work papers, report and slide deck).	1 trip	$ 11,726

Title	Description	On-Site Travel	Cost including travel
Cybersecurity Risk Assessment [Small]	Conduct a cybersecurity risk assessment of one agency or a similar function. Focuses on critical controls that must be in place to address the threat landscape. Evaluates controls within insider threat, privacy, fraud prevention, process design, application governance and data management. Includes a Scoping Call, two Assessors with up to two weeks of on-site assessment (arrive Monday, leave Thursday or Friday) up to 500 questions/tests and physical security evaluation of two facilities (e.g. agency headquarters and a branch office). Assessment activity consists of interviews, observation of controls and documentation review. Deliverables include Assessment Report and Assessment Slide Deck. The presentation will be conducted remotely. Out of scope: Vulnerability scans, configuration reviews of system components and other methods of deep technical inspection.	4 trips	$ 63,621
Cybersecurity Risk Assessment [Medium]	Aligns to elements within the 'Cybersecurity Risk Assessment - Small' service. Intended for a medium or large-sized agency or similar function. Includes an additional week of assessment hours and a third trip to be used for additional on-site assessment activity.	6 trips	$ 83,119
Incident Response Plan Review	Comparison of existing Incident Response Plan against cybersecurity best practices to identify gaps and provide recommendations to mitigate identified issues. Deliverables include IRP Review Document and Slide Deck. Includes 80 hours with a Consulting Principal with 1 trip to conduct the presentation on-site.	1 trip	$ 21,251
Incident Response Tabletop Exercise	On-site, scenario-driven exercise designed to help organizations improve their cyberattack preparedness and resilience through practical exercise and experience. Deliverables include Table Top Exercise Results Document and Slide Deck. Includes 100 hours with a Consulting Principal with 2 trips (to conduct the exercise and present results on-site).	2 trips	$ 28,214
Email Security	Our security advisory service begins the process with an evaluation of existing controls to ensure they are configured optimally. This includes evaluation of the following: Spam Filtering, Spam Reporting Button on Email Client, Malware Protection, Sender Policy Framework (SPF), and Domain Message Authentication Reporting and Conformance (DMARC). We can also provide specific settings for Exchange and Office365 environments. We manage this process methodically in order to minimize legitimate emails from being mistakenly blocked. Most of the effort is done during the initial few weeks, but then time is needed for logging to identify email senders that may need to be approved prior to enabling any blocking.	1 trip	$ 22,547

Title	Description	On-Site Travel	Cost including travel
Firewall & Network Device Configuration	Proper configuration of firewalls and network devices is essential for protecting information, and for adherence to regulatory requirements such as PCI-DSS and HIPAA compliance. Our experienced network security professionals will evaluate firewall rules to ensure they are not overly permissive, as well as router and switch configurations to ensure they are secure. We will also validate software and firmware versions to ensure they are not subject to known vulnerabilities. The estimated cost is based on a single firewall ruleset, a single router configuration, and up to three different switch configurations.	1 trip	$ 23,176
Active Directory Audit	With Active Directory at the center of many organization's networks, it is essential to run periodic health and security checks to ensure continued operation. Our Active Directory team will collaborate with your team to perform a health check. This will include an evaluation of the health and settings specific to the version of AD being run by your organization. Examples of some evaluated areas include: domain OU structure, trust relationships, administrative accounts and permission inheritance, Group Policy Objects, audit policies, time synchronization, replication status, anomalous event detection, and utilizing advanced capabilities such as File Server Resource Manager (FSRM), DHCP Failover, DHCP Failover Auto Config Sync (DFACS), Device Guard, and Credential Guard.	2 trips	$ 25,583
Qualys Vulnerability Scanning implementation	Qualys scanning comes with an array of modules that each need to be configured in order to properly scan and report on vulnerabilities and configurations. We will provide customized configuration services to match the modules that your organization is using. These services can include account configuration, scheduled scans, authenticated scanning, scheduled report, dashboards, and agents for deployment. We will also train up to three users on how to deploy agents and monitor the system. Some of the Qualys modules include: Vulnerability Management (VM), Policy Compliance (PC), Security Configuration Assessment (SCA), Security Assessment Questionnaire (SAQ), Cloud Agent (CA), Asset View (AV), File Integrity Monitoring (FIM), and Web Application Scanning (WAS).	1 trip	$ 24,776

Title	Description	On-Site Travel	Cost including travel
Support Desk Social Engineering Assessment	Social engineering is a broad term encompassing the many non-technical methods attackers use to gain access to information or systems. Voice phishing is the act of an attacker calling a target and pretending to be someone else to persuade them into revealing sensitive information. The attacker may use credentials obtained from a successful vishing attempt to impersonate individuals within a corporation or to gain access to privileged company resources. Unisys's approach over a 2 week period consists of reconnaissance, scenario creation, target engagement, assessment report and executive debrief. Unisys will conduct an assessment of one support desk inclusive of social engineering, vishing, spear phishing and controls evaluation. Deliverables will include an assessment report and a debrief slide deck. Prerequisite: Signed document by client acknowledging that Unisys is has been engaged to conduct a social engineering assessment in the event an employee asks for proof. Assessment will be coordinated with client security in the event the support desk calls them.	2 trips	$ 34,597
Security Operations Controls Assessment On-Premise	There are three areas of security operations threat prevention, threat detection and incident management. This offering provides a controls review of on-premise hosted information systems, Unisys will deliver a findings, gap analysis using industry best practices, strengths, weakness, opportunities and threats (SWOT) matrix, and recommendations. Our scope will include network/application firewalls, IDS/IPS, vulnerability management, application security, data loss prevention, infrastructure patching and hardening guidelines, log analysis and SIEM, alerting, SOC/NOC integration, threat hunting, incident response, media relations, DR, forensic investigation and data breach preparation.	9 trips	$ 200,179
Security Operations Controls Assessment Hybrid	There are three areas of security operations threat prevention, threat detection and incident management. Our hybrid assessment offering consist of a controls review of on-premise and cloud hosted information system assets. Unisys will deliver a findings, gap analysis using industry best practices, strengths, weakness, opportunities, and threats (SWOT) matrix and recommendations. Our scope will include network/application firewalls, IDS/IPS, vulnerability management, application security, data loss prevention, infrastructure patching and hardening guidelines, log analysis and SIEM, alerting, SOC/NOC integration, threat hunting, incident response, media relations, DR, forensic investigation and data breach preparation.	6 trips	$ 140,828

Title	Description	On-Site Travel	Cost including travel
Security Operations Controls Assessment Cloud	There are three areas of security operations threat prevention, threat detection, and incident management. Our cloud assessment offering consist of a controls review of cloud hosted information system assets. Unisys will deliver a findings gap analysis using industry best practices, strengths, weakness, opportunities, and threats (SWOT) matrix, and recommendations. Our scope will include network/application firewalls, IDS/IPS, vulnerability management, application security, data loss and protection, infrastructure patching, and hardening guidelines, log analysis and SIEM, alerting, SOC/NOC integration, threat hunting, incident response, media relations, DR, forensic investigation, and data breach preparation.	6 trips	$ 119,727
Business Continuity Plan Review and Business Impact Analysis - 10 processes	Business Continuity (BC) and Disaster Recovery (DR) are commonly used together but are considerably different. Business Continuity is how business operations continue in case of a disaster. Disaster Recovery is how IT (Information Technology) recovers business operations information systems in case of a disaster. Unisys will conduct a review of the latest BC plans up to 10 critical business processes, applications and most recent results of a plans exercise. We will provide a gap analysis report between current BC plans, latest plan exercise and existing IT system configuration supporting those business processes and applications. In addition, we will conduct a new or updated business impact analysis of 10 critical business processes and applications.	12 trips	$ 532,812
Cloud Security Assessment	Cloud Security Assessment will evaluate the current state cloud services (IaaS, PaaS, Saas) and provide a gap analysis, recommendations and actionable execution plan for securing cloud services. The assessment will comprise of four phases: discover, analyze, strategize/plan and present findings/executive review. Both questionnaires and workshops/meetings will be used to perform the assessment.	5 trips	$ 69,075
Cloud Strategy Assessment	Cloud Strategy Assessment will evaluate the current state data center(s) and cloud services (IaaS, PaaS, SaaS) and provide a current state analysis, future state roadmap and actionable execution plan for adopting and deploying cloud services. The assessment will comprise of four phases: discover, analyze, strategize/plan and present findings/executive review. Both questionnaires and workshops/meetings will be used to perform the assessment.	5 trips	$ 74,308
Cloud Architecture & Design	Cloud Architecture & Design engagement will evaluate the current state data center(s) and cloud services (IaaS, PaaS, Saas) and provide a cloud reference architecture and level of effort for build & deployment of target state cloud reference architecture services. The engagement will comprise of four phases: discover, analyze, strategize/plan and present findings/executive review. Both questionnaires and workshops/meetings will be used to perform the engagement.	5 trips	$ 74,308