

**AMENDMENT No. 1 TO
GETS Ready - Unisys
CONTRACT NUMBER: 98000-GETS Ready-RFQC-1647-UNI**

This Amendment No. 1 is made this 30th day of September, 2018 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 February 22, 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 premises, the terms and conditions stated herein, and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties hereto hereby agree as follows:

1. Scope. The Agreement is hereby amended to add the Services and Pricing described within this Amendment No. 1 to Exhibit 1 (Catalogue of Services, Service Levels, and Pricing) of the Agreement. The attached Services and Pricing are also added to the Agreement and made a part thereof.
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. 1 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. 1, 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. 1 and the Agreement, collectively, are the complete agreement of the parties and supersede any prior agreements or representations, whether oral or written, with respect thereto.

IN WITNESS WHEREOF, the parties have caused this Amendment No. 1 to be duly executed by their authorized representatives as of the date set forth above.

Unisys Corporation

By: Michael T Kreager

Name: _____

Title: Client Executive

Date: 10/02/2018

GEORGIA TECHNOLOGY AUTHORITY

By: Mark Latham

Name: Mark Latham

Title: Southern Governance Officer

Date: 10/10/18

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
Program Assessment [Small]	<p>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.</p> <p><u>Out of scope:</u> Vulnerability scans, configuration reviews of system components and other methods of deep technical inspection.</p> <p><u>Dependency:</u> Current GTA IT security policy assessment work papers established under a separate engagement (below).</p>	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

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
TrustCheck Annual Subscription	<p>TrustCheck evolves cyber risk assessments by focusing on continued analysis rather than providing a point-in-time gap assessment:</p> <ul style="list-style-type: none"> • The cyber risk model is updated on a monthly basis to ensure that threats are current and relevant for a specific client and its industry. • TrustCheck can fine tune risk measurement based on what is actually happening in the client's network. This improves fidelity in risk measurement, providing objective data to augment interview-based control assessments. • TrustCheck provides economically prioritized guidance so that remediation priorities can be aligned with economic impact. • The Unisys cyber risk advisor meets with the client quarterly to help understand its risk exposure and provide guidance on using its scores to prioritize risk remediation activities. <p><u>Additional Details:</u> https://www.unisys.com/offerings/security-solutions/trustcheck-cyber-risk-management</p>	4 trips	\$ 250,000
Program Development [Small]	<p>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).</p> <p><u>NOTE:</u> 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.</p>	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

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
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
Cybersecurity Risk Assessment [Small]	<p>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.</p> <p><u>Out of scope:</u> Vulnerability scans, configuration reviews of system components and other methods of deep technical inspection.</p>	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

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
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
Firewall & Network Device Configuration	<p>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.</p> <p>The estimated cost is based on a single firewall ruleset, a single router configuration, and up to three different switch configurations.</p>	1 trip	\$ 23,176

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
Active Directory Audit	<p>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.</p>	2 trips	\$ 25,583
Qualys Vulnerability Scanning implementation	<p>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.</p> <p>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).</p>	1 trip	\$ 24,776
	Social engineering is a broad term encompassing the many non-technical methods attackers use to gain access to information or	2 trips	\$ 34,597

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
Support Desk Social Engineering Assessment	<p>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.</p> <p>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.</p>		
Security Operations Controls Assessment On-Premise	<p>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.</p>	9 trips	\$ 200,179
Security Operations Controls Assessment Hybrid	<p>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.</p>	6 trips	\$ 140,828

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

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

EXHIBIT FOR SECURITY CONSULTING SERVICES FOR AMENDMENT #1

Title	Description	On-Site Travel	Cost including travel
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