# MICHIGAN MUNICIPAL SERVICES AUTHORITY

## *RFP 2023-1 FOR IT MANAGED SERVICES AND CYBERSECURITY ASSESSMENT SERVICES*

August 21, 2023

Submitted By: Mike Coyne, Account Executive

mcoyne@dewpoint.com

300 S Washington Square #200
Lansing, MI 48933
P (517) 316.2860

Dewpoint

300 S Washington Square #200 Lansing, MI 48933
P (517) 316.2860
Dewpoint.com

August 21, 2023

Samantha Harkins
Chief Executive Officer
PO Box 12012
Lansing, MI 48901

The Michigan Municipal Services Authority (MMSA) released RFP 2023-1 for Information Technology Management Services and Cybersecurity Assessment Services to identify a well-qualified vendor who delivers performance and value. The RFPs requirements attest to the MMSA's vision for a partner in IT managed services and cybersecurity that delivers professional and client-focused services. We're confident our response will demonstrate our ability to deliver quality, valued services to the MMSA and its Public Agencies.

Dewpoint is a Lansing, Michigan-based company. We share many values with the MMSA, like a commitment to collaborate, innovate, and serve our clients. Our success is rooted in our commitment to meeting and exceeding our clients' goals. As an IT company providing managed services for many public and private sector clients, cybersecurity is the foundation of our portfolio.

We look forward to the MMSA's feedback on our proposed managed services and cybersecurity assessment services described in this response. If the MMSA has any questions regarding our response, Mike Coyne, Dewpoint Account Executive, is our point of contact. Mike is a key member of our Account Executive team and has supported Michigan government clients for over 20 years. He can be reached by phone at 517.331.0715 or by email at mcoyne@dewpoint.com.

Dewpoint's proposal to provide information technology managed services and cybersecurity assessment services is extended to the MMSA and participating Public Agencies.

This proposal is signed and authorized by Joe Findlater, Dewpoint's Senior Vice President. The pricing figures provided in this response will remain firm for 60 days. There are no pending or regulatory actions against Dewpoint.

Sincerely,

Joseph P. Findlater

Joe Findlater
Senior VP, Dewpoint

# TABLE OF CONTENTS

Dewpoint

# QUALIFICATIONS & EXPERIENCE

**A general description of responder's qualifications and experience;**

Dewpoint, LLC is a Michigan-based IT services and solutions company established in 1996. Initially servicing the Lansing area, we've grown to include clients throughout the United States. We achieved this growth by ensuring our service delivery meets or exceeds our client's goals and objectives, resulting in both repeatable clients and expansion of our IT services within client organizations.

In January 2015, The 4100 Group (formerly GLM Holding Company) purchased Dewpoint as a wholly-owned subsidiary. Delta Dental of Michigan is the parent company of The 4100 Group. Dewpoint still runs as an independent company; however, the backing of The 4100 Group ensures financial stability. This has also allowed Dewpoint to expand our service offerings and hire additional IT-managed services, cybersecurity, network, and application development experts.

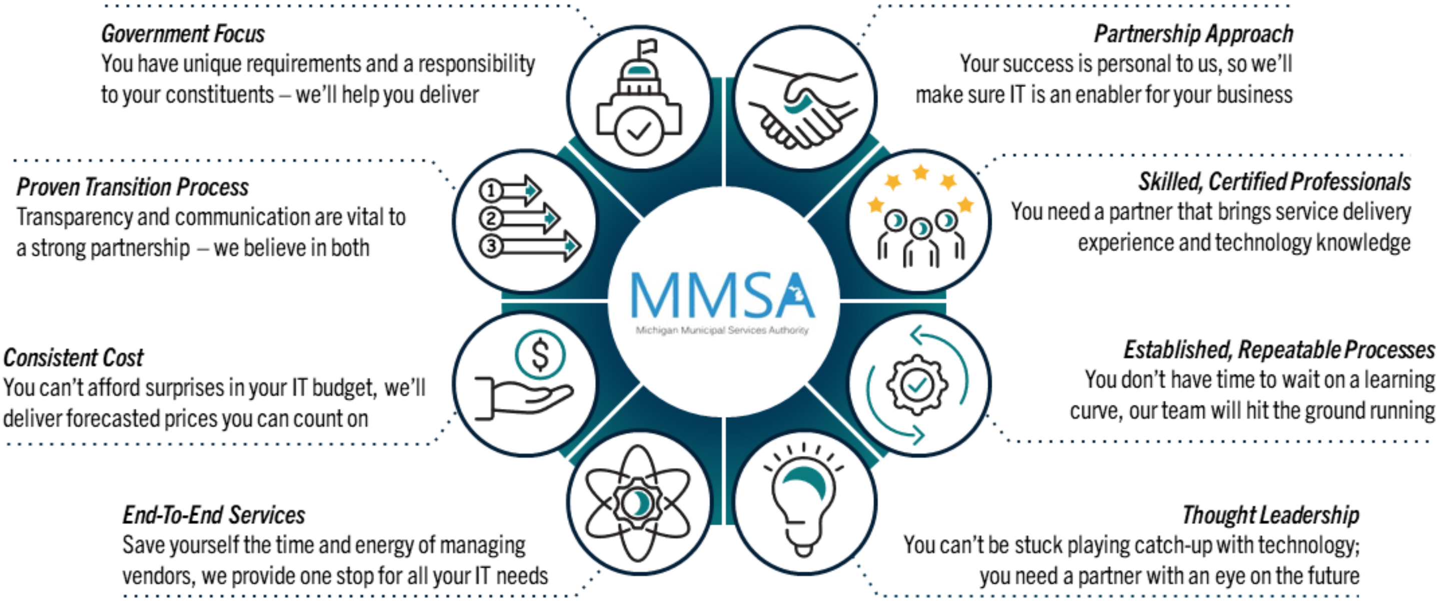
## Company Experience

Dewpoint has assisted many non-profits, small to mid-sized companies, and government clients with their IT journeys, including transitioning and providing ongoing IT-managed services as well as cybersecurity services. The primary factor setting Dewpoint apart from our competitors is our people. We have certified, experienced professionals with in-depth experience managing services to our clients, provided locally from our Lansing-based company headquarters.

Like your mission to deliver innovative solutions that enhance the lives of your member agencies' citizens, Dewpoint strives to make our clients successful by delivering services as promised. We accomplish this by developing a partnership with you and providing innovative thought leadership so you can continue to deliver services to your clients.

Dewpoint has a robust practice of complete managed services and cybersecurity offerings, including everything within this RFP scope. Our experience in successfully delivering services for governmental clients is explained in detail in the references section. We have listed four references in the Technical Component section of this response: City of Lansing (Managed Services), City of Grand Rapids (Managed Services), Michigan DHHS (Cybersecurity Assessment), and City of Eaton Rapids (Cybersecurity Assessment). Many other Managed Services clients are available for the Authority to talk to, including other local governments in Michigan.

Figure 01 below represents additional Dewpoint differentiators that will provide value to the Authority and its participating Public Agencies.



***Government Focus***
You have unique requirements and a responsibility to your constituents – we'll help you deliver

***Partnership Approach***
Your success is personal to us, so we'll make sure IT is an enabler for your business

***Proven Transition Process***
Transparency and communication are vital to a strong partnership – we believe in both

***Skilled, Certified Professionals***
You need a partner that brings service delivery experience and technology knowledge

***Consistent Cost***
You can't afford surprises in your IT budget, we'll deliver forecasted prices you can count on

***Established, Repeatable Processes***
You don't have time to wait on a learning curve, our team will hit the ground running

***End-To-End Services***
Save yourself the time and energy of managing vendors, we provide one stop for all your IT needs

***Thought Leadership***
You can't be stuck playing catch-up with technology; you need a partner with an eye on the future

**Figure 01 – Advantages of Partnering with Dewpoint**

# Qualifications

As an end-to-end complete IT services provider, Dewpoint has the expertise to satisfy the proposed services for the Authority and participating Public Agencies. This is demonstrated by the strength of our IT-managed services and cybersecurity professionals, our referenceable clients, and our commitment to you.

## IT Managed Services

Brent Olivier leads our IT-managed services team. As the Infrastructure Managed Services Manager, he applies his over 15 years of experience in the IT field to ensure consistent delivery from transition through ongoing support. Brent also strives to develop long-term client relationships by quickly addressing and resolving issues.

Before joining Dewpoint, Brent held positions including Senior Consultant at IBM, IT Operations Manager for Spartan Motors, and Director of IT Portfolio and Shared Services for AF Group. He is a graduate of Michigan State University with a Bachelor of Science in Applied Engineering Science.

Wade Prestonise, Dewpoint's Infrastructure, Network, and End-User Compute Manager, has over 15 years of IT experience incorporating his technical background and customer experience to quickly address and resolve client issues. Wade's experience includes local municipalities and commercial clients. In his current position, Wade oversees Dewpoint's Operations Center (NOC) to ensure client contractual obligations are met.

As part of his current job responsibilities, Wade evaluates the existing staff to ensure they have the right skill sets and recommends additional training or mentoring.

## Cybersecurity

Although we have always emphasized cybersecurity in our technology services, in 2016, recognizing the need for additional expertise in cybersecurity, we hired a Chief Information Security Office (CISO) to establish a formal portfolio offering. In addition to our CISO, Dewpoint has a team of trained security experts. This team allows us to provide our clients with a comprehensive cyber program and cyber consulting services.

Don Cornish, CISO, leads our cybersecurity team. Don applies his diverse background in IT security architecture and consulting to ensure Dewpoint's recommendations comply with current security standards. Don has served in his current role since 2016, assisting our clients in assessing their IT security environment and making recommendations to improve their security posture.

Before joining Dewpoint, Don provided security and compliance consulting to multinational business entities; when working for Hewlett Packard, he held various roles, including Account Security Officer, Senior Security Lead, and Senior Security Solution Consultant. Don's broad range of experience includes developing and implementing solutions covering a vast range of security technologies and products in the server, network, and end-user device space in both traditional outsourcing services environments and the cloud.

Don holds certifications in the following: Certified Information Systems Security Professional (CISSP), ITIL V3 Foundations, ISO 27001 ISMS Master Implementer, and SANS session 504: Hacking Techniques, Exploits & Incident Handling Certificate and Cybersecurity Maturity Model Certification – Registered Practitioner.

Along with Don is Ernesto Cuevas, Sr. Solutions Architect. Ernesto brings over 30+ years of professional Information Technology (IT) experience focusing on network management, network technology infrastructure, support, planning, capacity analysis, implementations, and security. He managed and directed Enterprise LAN/CAN projects and implementations from a technical, financial, and resources perspective. In addition, Ernesto performed a supervisory role in managing over 4000+ network devices (routers, switches, wireless access points, IPS/IDS, firewalls) in several sites across the globe, plus supporting relationships with various vendors. Before joining Dewpoint, Ernesto had a long career with EDS/HPE/DXC, successfully implementing several global network transformation projects.

As a CyberAB registered practitioner, Ernesto regularly performs assessments providing clients with actionable recommendations to improve their overall IT security and analyzes clients' current state environments to develop a future state roadmap.

## Staff Profile

We employ local, certified professionals (with global experience) trained in the latest technologies with an in-depth knowledge of various processes and tools. The majority of our staff either support or have supported state or local government clients, thus understanding the technology issues facing public sector clients and offering viable solutions. Dewpoint believes in investing in our people through tuition reimbursement and offering professional development and training. Listed below are some of the credentials are employees hold:

- On average, over ten years of experience in the IT field
- Over 80% of our employees have bachelor's degrees. Many also hold advanced degrees
- Over 85% of our employees participate in continuing education and training programs, such as attending industry-specific seminars, workshops, conferences, or boot camps for additional certifications

Certifications including:

- Apple Certified Technical Coordinator
- Apple Certified Associate- Mac Integration Basics
- Apple Certified Support Professional
- AWS cloud practitioner
- Azure Fundamentals
- CCNA Security
- CCNP Enterprise (Routing & Switching)
- Certified Security Compliance Specialist
- Certified Information Systems Security Professional
- Cybersecurity Maturity Model Certification Registered Practitioner
- CompTIA A+ and Network+
- CrowdStrike Partner Engineer
- Cybersecurity Fundamentals Certification
- FileMaker 13 and 14
- Geographic Information Systems Professional Certification
- ITIL Foundation - IT Service Management
- ITIL v3 and v4 Foundation
- LogicMonitor Certified Associate
- MCPS Microsoft Certified Professional
- Microsoft Certified Solutions Associate (MCSA) Windows 7

- MCSA Windows 8
- MCSA Office 365
- MCSA SQL 2016 Database Development
- MCSE Business Intelligence
- MCSE Data Management and Analytics
- MCSE Productivity
- Microsoft Certified: Azure Fundamentals
- Microsoft Certified: Data Analyst Associate (Power BI)
- Microsoft Certified SC-900: Security, Compliance, and Identity Fundamentals
- Oracle Certified Professional 10g
- PMI-Agile Certified Practitioner
- Project Management Professional (PMP)
- Prosci Certified Change Management Professional
- Rapid7 Insight IDR Certified Specialist
- Rhapsody Professional Developer
- SAFe 4 Scrum Master Certification
- SAFe 5 Advanced Scrum Master
- SAFe 5 Scrum Master
- SAFe SPC Certification
- VMware VCP-DTM Desktop Mobility
- Azure AI Fundamentals
- Cisco Certified Network Associate (CCNA)
- RFID Professional Institute-Certified Associate
- NetMotion Certified Administrator
- Microsoft Certified Expert in Excel, PowerPoint, Word, and Publisher

## Our Commitment to You

Finally, but most importantly, is our commitment to you. From service desk technicians to our President and CEO, we aim to ensure your satisfaction with Dewpoint's services. We achieve this through regular status meetings, issuing a short customer satisfaction survey at the end of every support call or visit to let your end users rate the experience and accessibility to our leadership team to assist the Authority and participating Public Agencies in your IT strategy and planning.

# SCOPE OF SERVICES & STANDARDS

**A description of how the responder proposes to perform the services detailed in section 2 in compliance with the standards detailed in section 3**

## Scope of Services

**The Authority seeks a qualified contractor capable of providing the Authority or participating Public Agencies, or both, with the following information technology management services and cybersecurity assessment services:**

**1) Information technology management services, including:**
**A) management of firewalls, anti-virus, anti-malware, and threat identification;**
**B) proactive monitoring and alerts;**
**C) on-site and remote support services;**
**D) private, hybrid, and public cloud options; and**
**E) and on-call infrastructure professionals;**

### A) Management of firewalls, anti-virus, anti-malware, and threat identification

### Management of Firewalls

Dewpoint's firewall management services help organizations improve their network security, reduce the risk of data loss, simplify firewall administration, and save time and money. Our experts help organizations fine-tune their firewall policies, control which applications and websites their users can access, and protect their networks from malicious traffic, viruses, and malware.

Our firewall management services include:

- Backup and Restore
- Rule Administration
- Application/URL Filtering Management
- IPS/IDS Management
- Anti-Virus/Anti-Malware Management

### Management of Anti-Virus and Anti-Malware

Dewpoint enrolls all in-scope Windows and Mac devices in the CrowdStrike Falcon portal, our chosen malware protection tool. Our security experts maintain the environment and respond to any triggered alerts.

Our anti-virus management capabilities include:

- Administering anti-virus software to protect operating systems
- Maintaining anti-virus software updates as recommended by the vendor

- Reporting on security incidents involving viruses and the anti-virus solution

## Threat Identification

Dewpoint's security experts monitor threats toward customer devices and technologies, identifying new threats and analyzing potential impact and risk toward the customer environment. Based on the analysis, we provide appropriate measures to remove or reduce the risk. Fortra's Frontline vulnerability scanner is our chosen solution, providing detection and prioritization of internal and external vulnerabilities for a wide range of devices and operating systems.

### B) Proactive monitoring and alerts

Dewpoint uses LogicMonitor for monitoring in-scope IT infrastructure devices and services. LogicMonitor is a leading infrastructure monitoring solution consistently ranked highly by Gartner. It offers a wide range of features and capabilities, including scalability, ease of deployment, and continuous innovation. LogicMonitor can be integrated with a variety of ITSM solutions to automate the incident response process.

In Dewpoint's environment, LogicMonitor is integrated with our internal ITSM service to automatically generate alerts., routing them to Dewpoint's Managed Services organization for the appropriate resolution. This integration allows us to quickly and efficiently respond to incidents, which helps to protect our customers' IT infrastructure.

### C) Onsite and remote support services

Dewpoint's Support Services begin with the quality of the staff we employ. Many companies hire inexperienced staff who primarily follow scripts to move towards a resolution, wasting valuable time. At Dewpoint, we hire highly-knowledgeable professionals who know the "right" questions to ask to resolve customer issues sooner. We believe in "Making IT Personal," and our onsite and remote support services embody that philosophy.

Our services include:

- Break-Fix Support
- Warranty Service
- Software Support
- Install, Move, Add, Change Support
- Patch Management

## Onsite Support Services

Our onsite support services include an agreed-upon number of hours of onsite support per week, so customers receive the personal attention we believe managed services require. This proactive on-site approach delivers a consistent end-user experience for our customers' staff. During the transition to Dewpoint's services, we work with our customers to determine a support structure that works for both parties.

## Remote Support Services

Our Remote Support Services (Service Desk) are the single point of contact (SPOC) for our customers' services. Customers can access our Service Desk via email, phone, or online portal. We employ ServiceNow's industry-leading Information Technology Service Management (ITSM) solution to track and report incidents from submission through resolution. Customers can access the ITSM via the portal to initiate, track, or cancel a ticket.

Upon receiving a ticket, our staff will contact the customer user and validate the ticket information. Our technician will create an event log containing a time-stamped record of activities leading to the ticket's resolution.

Our goal is to resolve user issues on the first call without escalating to onsite support. Issues that cannot be resolved on the first call are escalated as required. As illustrated in Figure 02 below, ticket resolution can occur at any support level, while complex resolution efforts may progress through all support levels.

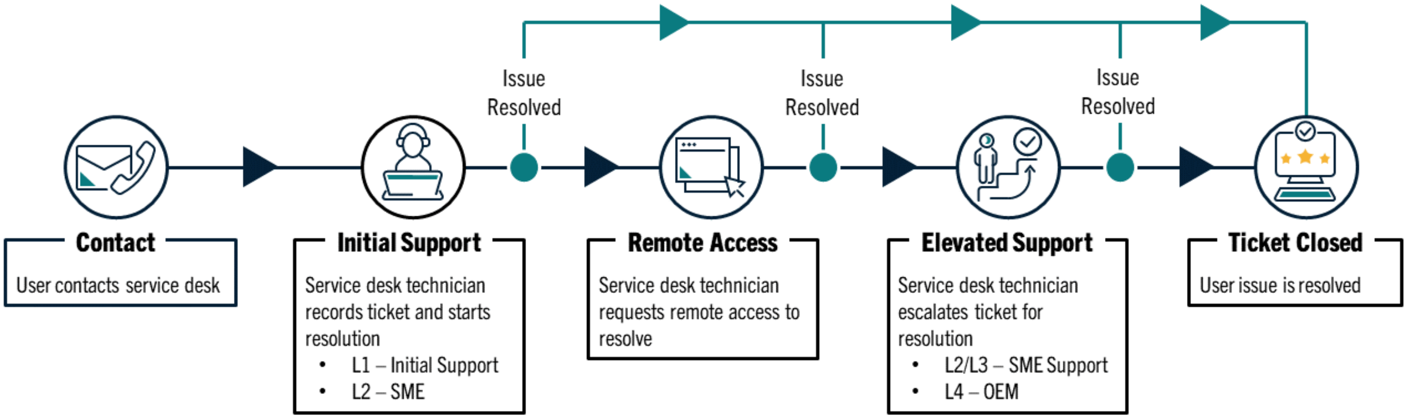

Issue Resolved
Issue Resolved
Issue Resolved
Contact
User contacts service desk
Initial Support
Service desk technician records ticket and starts resolution
• L1 – Initial Support
• L2 – SME
Remote Access
Service desk technician requests remote access to resolve
Elevated Support
Service desk technician escalates ticket for resolution
• L2/L3 – SME Support
• L4 – OEM
Ticket Closed
User issue is resolved

**Figure 02 – End User Support Model to Ensure Timely Resolution**

Support level definitions include:

- **Level 1 Support -** The initial support level responsible for basic end-user issues
- **Level 2/3 Support -** More in-depth technical support level utilizing experienced personnel knowledgeable on a product or service such as system administrators or onsite desktop technicians

- **Level 4 Support -** Original Equipment Manufacturer (OEM) or Vendor support groups support level

To ensure customer satisfaction with our service desk, we provide a Customer Satisfaction Survey at the end of every support call or visit, allowing end users to rate the experience. Our management team reviews any less-than-satisfactory rating with the technician to determine what we could do better. We work to continuously improve our service based on feedback.

### D) Private, hybrid and public cloud options

Dewpoint provides systems engineering and data center services for a variety of customer footprints, including public cloud (Azure, AWS) administration, private on-premise data center management, and support for hybrid environments which incorporate a blend of internally hosted and cloud components, such as Identity and Access Management, Mobile Device Management, or Email hybrid deployments.

### D) On-call infrastructure professionals

We're committed to supporting our customers after hours. If a critical incident occurs, our process leverages onsite and remote support to get customers the support they need when they need it, minimizing risk and downtime.

Our dedicated support professionals operate in an on-call rotation to deliver these services, ensuring critical events in our client environments are swiftly identified, triaged, and engaged. On-call agents receive alerts through an after-hour paging system integrated with our monitoring and ITSM solutions.

We provide customers with contact information for on-call resources and an assigned client success manager. Customers also receive email alerts from our monitoring tool.

**2) Cybersecurity assessment services, including:**

- **A) Independent view of current information technology security measures;**
- **B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities;**
- **C) Recommendations for improving short-term and long-term planning to increase information technology security;**
- **D) Recommendations for information security best practices; and**
- **E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D).**

### A) Independent view of current information technology security measures

Dewpoint's cybersecurity consultants have many years of experience providing security consulting services to state and local government customers as well as customers in the manufacturing, insurance, and financial management industries. We draw upon this experience to guide our customers' security journeys, providing recommendations based on practical best practices with cybersecurity expertise and insight.

Dewpoint's cybersecurity professionals have developed an assessment methodology for assessing an organization's security maturity posture based on either the Center for Internet Security (CIS) framework or the NIST SP 800-53 or NIST SP 800-171 standards.

Our security team assessed the cybersecurity posture of over 50 Michigan counties as part of the DHHS Friends of the Court/ Prosecuting Attorneys IRS assessment, measuring the maturity of their IT security operations. Each county received an assessment findings presentation and report with recommendations for improving their CIS maturity score.

We offer this consulting team and its expertise to the Authority and participating Public Agencies engaging in this RFP initiative.

### B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities

Part of any risk management program is identifying vulnerabilities that may exist within the client environment. To identify potential vulnerabilities across the IT environment, Dewpoint can offer vulnerability scanning services through a single engagement or Vulnerability Management as a Service. Dewpoint would need to understand the number of IPs that are in scope to determine pricing.

Whether a single event or a regular service, a vulnerability scan is performed against a defined set of IP addresses, the results are analyzed, and remediation recommendations are provided to the customer. These recommendations describe what actions the client should take to reduce or remove the vulnerability.

A report is generated with recommended remediations prioritized based on the criticality of the system to the customer's business objectives.

After creating the reports, Dewpoint's cybersecurity consultants engage with the customer's IT leadership to discuss the remediation activities. This meeting's objective is to establish prioritized remediation activities that customer operational teams can execute.

Dewpoint partners with Fortra Frontline vulnerability management services to deliver these initiatives. Fortra offers a Frontline portal where vulnerability scanning is configured and run, results are stored, and reports are generated. Dewpoint's consultants use this data to create customer reports and recommendations. Depending on the engagement, scanning can be performed against externally facing IP addresses or internal IP addresses as a single event or a regularly scheduled activity.

### C) Recommendations for improving short-term and long-term planning to increase information technology security

Our consultants are well-versed in delivering short and long-term cybersecurity improvement recommendations to customers. Typically, we leverage the results of a cybersecurity maturity assessment described in this response and any vulnerability scanning results available to deliver recommendations.

We understand that customers may need to procure tools and services to help reduce their organization's risk. However, the procurement cycle can be a long-term activity requiring planning and justification to support the purchase. In these instances, we provide a range of short-term options designed to reduce the risk level for the time being until the client can acquire the necessary tools or services to reach their long-term goals.

### D) Recommendations for information security best practices

Dewpoint cybersecurity consultants base recommendations on information and practices learned over many years of working in the IT industry. They also leverage Dewpoint's IT partners' depth of knowledge. We partner with leading cybersecurity vendors like Rapid7, Fortra, Crowdstrike, KnowBe4, and firms specializing in areas such as storage solutions, operating systems, and virtualization.

Having the backing of these vendors and the expertise of the extended Dewpoint organization allows our consultants to present customers with a range of services and solutions meeting the needs of organizations of all sizes.

### E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D)

Dewpoint's combination of consulting and operational expertise allows us to design, plan, implement, and perform ongoing IT operations to make technology an enabler for our customers in achieving their business objectives.

We have mature project and program management capabilities, having provided IT project management services since our inception. Our project management professionals have extensive experience working with government agencies and a long history of working with the State of Michigan. We have the breadth and depth of IT professionals experienced in delivering project management to successfully meet the Authority's and participating Public Agencies' requirements both on time and on budget.

From assessment, to analysis, to delivery, to ongoing run, Dewpoint has the experience and expertise to help the Authority and its participating Public Agencies achieve their objectives.

# Standards

**a) The services detailed in section 2 must be provided in compliance with the following requirements:**

**c) The contractor shall manage the delivery of services in a competent, professional, and cost-effective manner.**

**d) The contractor shall designate a single individual for each contract with the Authority or a participating Public Agency and that individual shall be responsible for the direction and supervision of services provided. Other individuals performing services under the direction and supervision of the sole point of contact must be qualified to handle the work assigned. The contractor may not change the single point of contact without approval.**

**e) The contractor may not subcontract duties under its contract with the Authority or a participating Public Agency without the approval of the Authority or the participating Public Agency.**

**f) The contractor shall keep the Authority or a participating Public Agency contracting for services informed as to the progress and status of all pending matters as requested.**

### c) The contractor shall manage the delivery of services in a competent, professional, and cost-effective manner.

With over 27 years of IT experience delivering IT services and solutions to state and local government clients, we understand the existing standards, organizational structure, initiatives, and special compliance considerations like CJIS and FOIA, so we know how to get things done in a government setting.

The Dewpoint Team is comprised of IT experts with a track record of successfully delivering projects for governmental organizations at all levels, from the state down to the county and city levels. Our experts are accustomed to dealing with stakeholders at all organizational levels and have experience operating in the second-tier SOW project model that typically follows a pre-qualification contract such as this RFP.

Our references will attest to our competency, professionalism, and ability to successfully deliver managed and cybersecurity assessment services. Dewpoint's company motto is

"Making IT Personal." To our employees, this is more than a tagline; it's how we perform our daily work by taking personal responsibility to achieve our clients' goals and objectives.

d) The contractor shall designate a single individual for each contract with the Authority or a participating Public Agency and that individual shall be responsible for the direction and supervision of services provided. Other individuals performing services under the direction and supervision of the sole point of contact must be qualified to handle the work assigned. The contractor may not change the single point of contact without approval.

The Authority and each participating Public Agency will have a designated single point of contact for the direction and supervision of services. As demonstrated by our references and qualifications, we employ highly qualified professionals with experience and expertise in their fields. All work performed for the Authority and participating Public Agencies will be done by a qualified professional. In the event the designated single point of contact is not able to continue, Dewpoint will work with the Authority or participating Public Agency to identify their replacement.

e) The contractor may not subcontract duties under its contract with the Authority or a participating Public Agency without the approval of the Authority or the participating Public Agency.

Dewpoint agrees that duties under any contracts resulting from this response will not be performed by a subcontractor without the approval of the Authority or participating Public Agency.

f) The contractor shall keep the Authority or a participating Public Agency contracting for services informed as to the progress and status of all pending matters as requested.

We assign a Client Success Manager (CSM) to all our clients to ensure regular communication with our clients during implementation and ongoing relationship management.

# MANDATORY QUALIFICATIONS

**The responder must demonstrate its capability to perform the services proposed in accordance with the standards detailed in section 3 and include a detailed description of the responder's relevant prior experience in the services detailed in section 2.**

Dewpoint has the processes and experienced professionals to deliver the services requested by the Authority in accordance with the standards outlined in this RFP. Our approach is built upon decades of experience with similar clients, applying lessons learned in conjunction with our professionals' real-world experience to deliver successful projects.

We have extensive experience working with local government agencies and a long history of working with the State of Michigan. Over time, our portfolio of government clients has grown significantly to include states such as Hawaii and New Mexico, as well as local government clients such as Oakland County, Ottawa County, Washtenaw County, the City of Grand Rapids, and the City of Lansing.

Our references include the State of Michigan Department of Technology, Management, and Budget (DTMB), the City of Grand Rapids, the City of Lansing, and the City of Eaton Rapids. Throughout this proposal, the Dewpoint team will try to demonstrate our proven capabilities in IT managed services and cybersecurity assessments. We aim to provide the Authority review team with indisputable facts that Dewpoint has proven expertise in both areas, as defined by our work with our Michigan local government clients today. Details of this proposal are not marketing materials but the behind-the-scenes processes we follow to deliver. We also hope the Authority calls our references. When you do, you will also hear directly from our satisfied clients that the way we describe our work is the way they receive it today.

# ADMINISTRATIVE COMPONENT

**The response should clearly describe the responder's understanding of the work required and also should explain the responder's approach to performing the services described in section 2 in compliance with the standards in section 3 and detail any expenditure that the responder expects will be absorbed by the Authority or a participating Public Agency with the applicable fee or rate for any such expenditure.**

The Authority and participating Public Agencies seek a reputable, qualified IT solutions and services provider capable of delivering IT managed services and cybersecurity assessment services, emphasizing professionalism, clear communication, and cost-effectiveness.

The managed services requested include information technology management encompassing firewall management, anti-virus and anti-malware management, threat identification, proactive monitoring, on-site and remote support, cloud options, and access to infrastructure professionals.

The Authority and participating Public Agencies require cybersecurity assessment services involving an independent evaluation of current IT security measures, recommendations for enhancing security based on priorities and vulnerabilities, suggestions for short-term and long-term security planning improvement, advice on best practices, and assistance with implementing recommended measures.

In our response, we have detailed our staff's extensive experience, expertise, and passion for delivering IT services and solutions that enable our clients to meet their goals. We share many of the Authority's values, including a commitment to collaborate, innovate, and serve our clients. We perform our services with professionalism, emphasizing communication and clarity to deliver cost-effective solutions.

The Authority or participating Public Agency would be expected to maintain currency in licensing and maintenance contracts for operating systems, third-party vendors, hardware, and application software. They would also be expected to procure hardware and peripherals as their purchasing policy and vendor preferences dictate.

# TECHNICAL COMPONENT

**A response should include satisfactory evidence of the responder's capability to provide the services detailed in section 2 in compliance with standards under section 3 in a professional and timely manner, including:**

**1) A description of the responder's sole point of contact for responder's provision of services to the Authority and other personnel that would provide services to the Authority or a participating Public Agency, including the educational background, certifications, and professional licenses held;**

Mike Coyne, Sr. Account Executive, Government, is our single point of contact for provisioning services. A graduate of Central Michigan University, Mike applies his 25+ years of IT experience to develop strong customer relationships striving to deliver customer-centric solutions. Mike has been with Dewpoint as an Account Executive for 11 years. Prior to Dewpoint, Mike worked for Symantec, who at the time was the #1 security software company in the world. While at Symantec, Mike supported all government clients in Michigan. Mike has in-depth knowledge of the state, local government, and education sectors, focusing on providing consultative assistance with technology strategy, IT security, and overall IT planning to meet current and future needs. To continue to develop and maintain customer relationships and stay abreast of changes, Mike regularly attends government and education IT conferences such as MiGMIS, Infragard, Michigan Cyber Security Summit, Michigan Digital Summit, MISA, and MAEDS.

Following our motto of "Making IT Personal," ongoing support is critical to our client partnerships. To that end, we assign a Client Success Manager (CSM) to all our engagements. The CSM is assigned to ensure regular communication with our clients during implementation and ongoing relationship management.

John Varilek, your CSM, will meet regularly with your team to provide status updates and thought leadership to help you on your IT journey. With over 35 years in the IT field, John focuses his proven organizational leadership skills on identifying process improvements to drive return on investment from technology solutions. In his current role, John ensures Dewpoint services are provided as contracted, striving to develop a successful client relationship by delivering results. He has also spent time as an Executive on Loan (acting CIO) to improve operations, create a three-year road map and assist with locating and hiring a permanent CIO. Before joining Dewpoint, Hewlett-Packard employed him for over 31 years with roles ranging from account manager, account executive, client delivery manager, and project manager. John is a graduate of the University of Texas at Dallas.

### 2) A description of the adequacy of personnel to handle communications with the Authority and participating Public Agencies;

Communication and a commitment to our clients' success is central to our services. The CSM regularly meets with clients to conduct a service delivery review, address any issues, and discuss future project management service needs. Our CSM reports directly to Jerry Steenson, Senior Vice-President, Delivery. If the client is unsatisfied with the CSM or delivery of Dewpoint services, Jerry is available to meet and ensure client needs are met. Jerry reports directly to Bob Bartholomew, President and CEO. Bob is a hands-on CEO and makes it a point to get to know our clients and their satisfaction with our services. Bob also has over 15 years of experience supporting government clients in Michigan.

If selected for this contract, Dewpoint would also enjoy the opportunity to cooperatively market this valuable contract vehicle to the Authority's participating Public Agencies. Dewpoint's Mike Coyne would be the appropriate point of contact for Authority in this regard. Dewpoint would also bring our marketing expertise to this effort to effectively promote this contract vehicle and the advantages of IT managed services and cybersecurity assessments to our combined clients through social media, webcasts, and events such as the Michigan Municipal Executive conference.

### 3) A description of the level of assistance that will be expected from Authority or participating Public Agency staff;

Dewpoint would like the Authority to provide a single point of contact to partner with us to explore ways to market and advertise this exciting contract vehicle. We would also ask that this individual assist with the tier-two contract processes when participating Public Agencies look to leverage this contract. We would also look for Authority assistance in capturing the positive experiences our tier two clients are having while dealing with any contract disputes that could arise.

### 4) A proposed model work plan and schedule for a potential Public Agency client for both service components described in section 2;

We have included high-level work plan outlines for our managed services and security assessment services. The samples below are based on a medium-tier client, as defined in the Pricing section of this response. They are meant to be an illustrative sample of our processes and may change depending on the scope of the Authority or participating Public Agency.

#### Managed Services

We know seamless transition is important, so we use a tested, repeatable six-step methodology to ensure the smooth transitioning of services. We built this approach from experience transitioning clients as well as project management best practices. At the core of our methodology is understanding your current processes (through knowledge transfer) and ensuring your team is comfortable with any changes resulting from the transition. Our phased methodology is illustrated in Figure 03. A critical element is maintaining clear and open communication with you throughout the process.

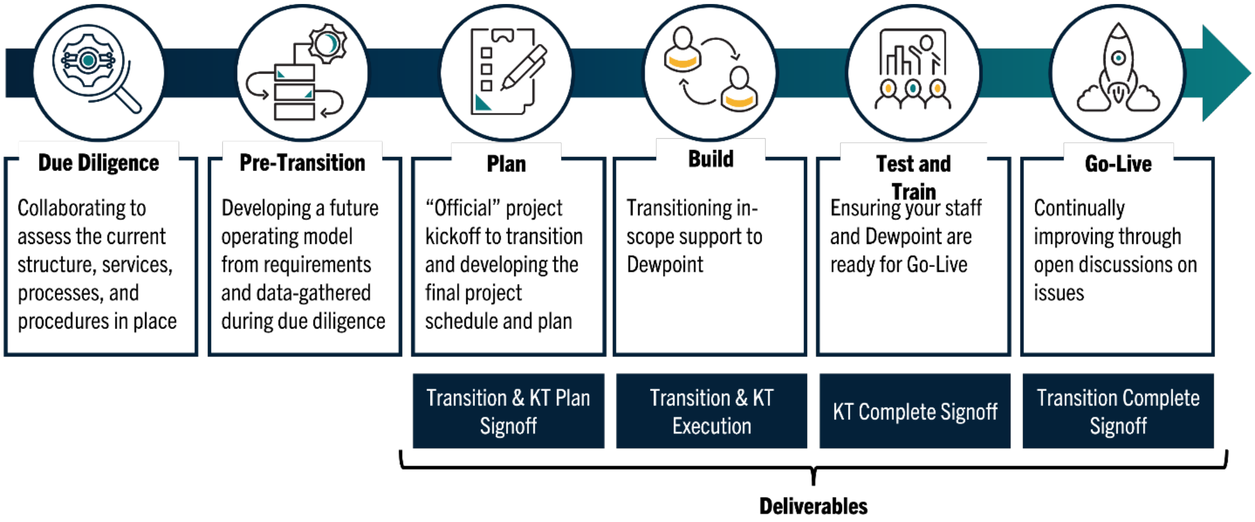

Due Diligence
Collaborating to assess the current structure, services, processes, and procedures in place
Pre-Transition
Developing a future operating model from requirements and data-gathered during due diligence
Plan
"Official" project kickoff to transition and developing the final project schedule and plan
Build
Transitioning in-scope support to Dewpoint
Test and Train
Ensuring your staff and Dewpoint are ready for Go-Live
Go-Live
Continually improving through open discussions on issues
Transition & KT Plan Signoff
Transition & KT Execution
KT Complete Signoff
Transition Complete Signoff
Deliverables

**Figure 03 – Apply Proven Transition Methodology to Ensure Success**

Dewpoint's philosophy during all phases of the transition is to ensure success with as little disruption as possible by:

- Respect the Authority or participating Public Agency's business cycles
- Help managing your third-party contracts
- Establish a SPOC to coordinate resources, plans, and handovers of business operations
- Support business operations during implementation

Dewpoint assigns a project manager to oversee the transition and knowledge transfer to completion. Our experienced project managers use applicable PMBOK guidelines to deliver projects on time, within budget, and meeting project goals and objectives. The project manager will strive to build relationships with your team. Table 01 on the following page shows high-level tasks and the approximate transition and knowledge transfer timeline.

| 1 to 30 Days | 31 to 55 Days | 56 to 60 Day |
|---|---|---|
| Perform due diligence validation on the environment<br>Onboarding & tool development<br>Access transfer & record analysis/documentation<br>Initiate client ServiceNow Portal<br>Confirm licensing & maintenance agreements<br>Conduct knowledge transfer from the current provider<br>Design dashboard | Deploy server, network, and end-user management tools<br>Hold process integration workshops on workflows for requests and incidents<br>Inventory current hardware and endpoints and identify any immediate needs<br>Update knowledge base with the server, VDI, storage, backup, switches, firewall, and mail-filtering documents | Perform testing & training<br>Go Live |
| <<< Ongoing Communication & Feedback >>> | | |

**Table 1 – High-Level Transition and Knowledge Transfer Tasks**

### Cybersecurity Assessments

Dewpoint utilizes the CIS Version 8 controls framework to evaluate security maturity. The CIS CSAT platform is our chosen tool for assessments, with an on-premises CIS CSTAT v8.0 instance to ensure consistency and efficiency. Our standard assessment covers Implementation Group 1 controls; additional safeguards can be included for an additional cost.

We create an organizational structure that mirrors our customers' structure, ensuring relevant results that align with their business needs. This structure forms the assessment foundation, enabling ongoing tracking and evaluation.

## Data Collection

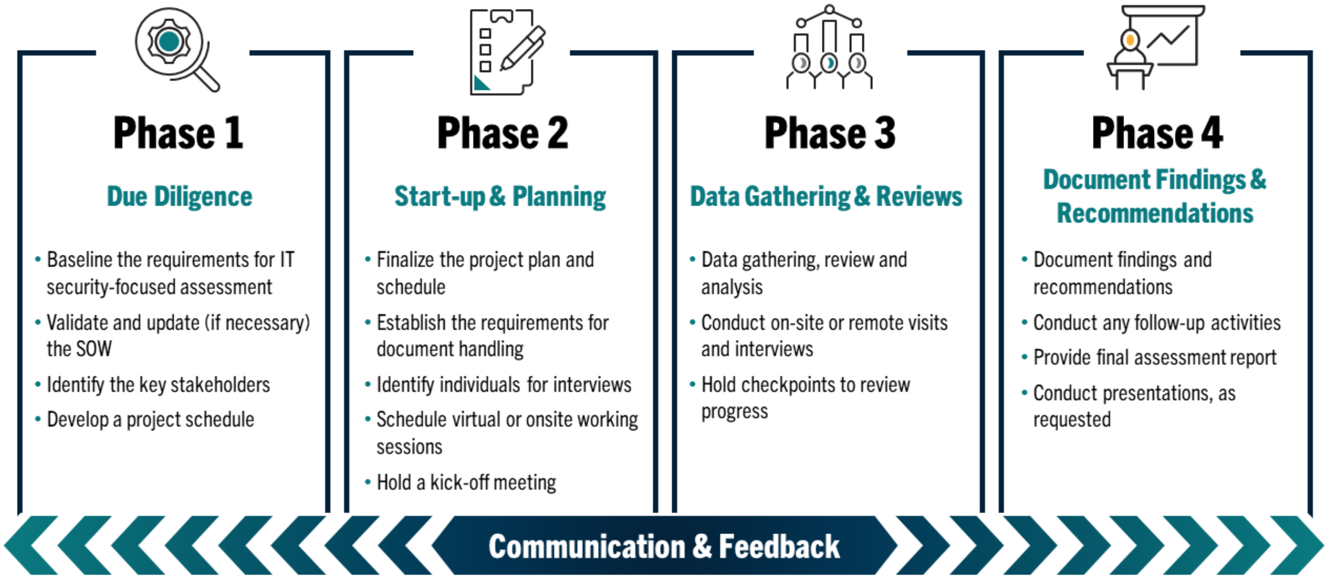
To evaluate current security controls, Dewpoint requires data collection and assessment that may include the following:

- A pre-assessment questionnaire outlining security status before interviews
- Examination of current IT security policies, processes, and procedures
- Review of supporting data and documents
- Conversations with key stakeholders
- Review of implemented recommendations from previous security assessments (if applicable)

Understanding customers have daily commitments, Dewpoint strives for minimal workplace disruption in our approach. This involves predetermined contact windows, focused agendas, and document reviews before meetings. This strategic process aids our comprehension of the present context, enabling us to ask specific, targeted questions for deeper insights. Drawing from our 25-year experience, we apply proven strategies from past projects to establish effective communication, uphold accountability, and maintain a well-managed schedule, aligning with expectations.

## Phased Approach

Dewpoint uses a four-phased process, as shown in Figure 04. During the project planning phase (before these activities start), our project manager will assign specific dates to each task and deliverable.



**Phase 1**

**Due Diligence**

- Baseline the requirements for IT security-focused assessment
- Validate and update (if necessary) the SOW
- Identify the key stakeholders
- Develop a project schedule

**Phase 2**

**Start-up & Planning**

- Finalize the project plan and schedule
- Establish the requirements for document handling
- Identify individuals for interviews
- Schedule virtual or onsite working sessions
- Hold a kick-off meeting

**Phase 3**

**Data Gathering & Reviews**

- Data gathering, review and analysis
- Conduct on-site or remote visits and interviews
- Hold checkpoints to review progress

**Phase 4**

**Document Findings & Recommendations**

- Document findings and recommendations
- Conduct any follow-up activities
- Provide final assessment report
- Conduct presentations, as requested

**Communication & Feedback**

**Figure 04 – Phased Approach for Consistent Success**

## Critical Security Control Evaluation

Using the CSAT portal, Dewpoint's assessment evaluates the organization's security against CIS Critical Security Controls, utilizing information from the data gathering section described earlier. Controls are rated by maturity on a scale of 0% to 100%. These measures determine overall safeguard maturity. After grading all safeguards, average maturity scores are given for each control (Table 02). Maturity ratings are defined on the next page.

| Maturity Level | Description |
|---|---|
| **Needs Improvement 0-50%**<br>🔴 | Current implementation for the control area is very limited and immature. Subcontrols lack implementation on systems as well as lack policies and reporting mechanisms. Immediate action should be evaluated to improve maturity for this control and may require significant resource or capital investment or both. |
| **Fair 51-75%**<br>🟠 | Current implementation for the control is at an average level of maturity. Controls have been implemented on some or most systems but may still lack overarching policies and procedures. A moderate level of change is required to continue elevating the control's maturity. |
| **Satisfactory 76-90%**<br>🟡 | Current control implementation meets accepted standards in the industry. There are documented policies and procedures, but they may lack formal adoption and reporting. |
| **Excellent 91-100%**<br>🟢 | Current control implementation is in near or complete compliance with standards in the industry. There are documented policies, procedures, and reporting mechanisms in place. |

**Table 02 – Critical Security Control Evaluation**

After gathering data and conducting interviews, data is entered into the CSAT assessment tool. The tool creates a heat map illustrating how the customer aligns with the in-scope controls. This report is aimed at executive-level management to provide them with an easily readable snapshot.

We also break down the findings by control and safeguard, explaining them in terms customer business leaders can understand. This report includes the control requirements, a summary of the situation related to the control, why that control matters, the risks linked to the controls, specific findings for the safeguard, and a rating for how mature the control is (shown in Figure 03). Each suggestion will explain how the customer can remediate that safeguard.

5) **A description of similar services previously performed for governmental entities, including a contact name and phone number for each governmental entity referenced;**

## Government Managed Services References

### City of Grand Rapids

**Contact**: Douglas Start, Information Technology Director
dstart@grand-rapids.mi.us
616-387-9339
**Duration:** March 2016 - Current

**Project Overview**: Dewpoint was awarded a competitive bid to provide Information Technology (IT) managed services for the Technology and Change Management Department's IT operations.

**Dewpoint Role**: Dewpoint transitioned the services from the then-staff augmentation provider within the agreed-upon time. Dewpoint's single point of contact had the full support of Dewpoint's management team to "do what it takes" to transition the services and start providing full service to the City. We currently provide operational support for the City's computer operations and infrastructure, including network, server, internet edge, enterprise solutions, desktop computing, and telephone environments. We also provide service desk, training, and network cabling as required.

### City of Lansing

**Contact**: Christopher Mumby, Chief Information Officer
christopher.mumby@lansingmi.gov
517-483-4453
**Duration:**

**Project Overview**: Dewpoint developed a partnership with the City of Lansing to address the City IT Department's challenges with dwindling budgets, aging infrastructure, staff turnover, and missing IT skill sets.

**Dewpoint Role**: Over the past ten years, Dewpoint has provided long-term IT staff augmentation, managed on-site IT infrastructure services, IT assessment services, technology project support, program management, IT/business governance, technical guidance, change management, and vendor management services.

With Dewpoint's support, the City of Lansing has achieved the following milestones:

- Implemented a new IT architecture leading to improved uptime, performance, and security
- Migrated 1000 Exchange users successfully
- Virtualized 85% of physical servers

- Architected a Virtual Desktop solution for all City employees
- Managed implementation of Cityworks across multiple departments

## Cybersecurity References

### DTMB Cybersecurity Assessment and Advisory Services

**Contact**: Pratin Trivedi, Director of Technology & Operations
trivedip@michigan.gov
517-334-6560
**Duration:** November 2021 - Current

**Project Overview**: The State of Michigan, through the Department of Technology, Management, and Budget (DTMB), required a vendor to perform an independent assessment using the Center for Internet Security (CIS) framework for each Friend of Court (FOC) and Prosecuting Attorney (PA) offices with a contract between the County and the state to provide these services to ensure security controls are in place.

**Dewpoint Role**: Dewpoint deployed a team consisting of our CISO, security architect, Sr. program manager, business analyst, and technical writer to assess over 50 Michigan Friend of the Court and Prosecuting Attorney Offices within various Michigan counties. Dewpoint provided a consistent county-level assessment and reported on the security findings and a comprehensive statewide summary report for each county.

We worked with each County to develop a Cybersecurity Improvement Plan of Action and Milestones (POAM), identifying priority actions to complete in the coming 24 months and other lesser priority activities over a longer time horizon. Dewpoint continues to provide remediation services for the remainder of the three-year contract.

### City of Eaton Rapids

**Contact:** Robert Pierce, Utilities Director
rpierce@cityofeatonrapids.com
517-525-3889

**Duration:** January 2022 – July 2022

**Project Overview:** Dewpoint conducted a comprehensive security assessment using CIS controls and an internal/external vulnerability assessment

**Dewpoint Role**: Dewpoint applied the Center for Internet Security (CIS) Version 8 controls framework to assess the maturity of the City of Eaton Rapids security maturity. Our team set up a separate instance in the CSAT assessment tool to provide an easily readable snapshot of the results. In addition, our security consultants created a detailed report listing each CIS control with the assessment findings and recommendations (if needed) to improve security.

To complement our assessment, a Fortra Frontline pen test was used to perform internal and external (internet-facing assets) penetration testing and create downloadable reports with test results. Along with the actual testing, Dewpoint provided support following the completion of each penetration test to help the City interpret the pen test results.

Our partners at Fortra conducted vulnerability scanning of the City's external network address space and vulnerability assessment of the internal and external networks. Upon completing the scanning, reports with detailed results were provided to the City. Dewpoint's subject matter experts reviewed the results with the city to advise on remediation actions. To assist the City of Eaton Rapids with financially supporting this initiative, Dewpoint collaborated with the State Emergency Management regional leadership to identify grant funding for this project.

**6) A description of the manner in which the respondent will retain and dispose of records related to its provision of services;**

Upon completion of contracted activities or the end of a contract period, Dewpoint will return the Authority's or the participating Public Agency's relevant materials or provide a statement attesting to the disposal or destruction of the materials. These activities will be performed using best practices and in accordance with applicable laws and regulations.

**7) A statement that the responder maintains comprehensive liability insurance and workers' compensation insurance for its employees, and cybersecurity insurance for its activities;**

Dewpoint carries and maintains comprehensive liability insurance and workers' compensation insurance. Delta Dental provides Dewpoint's cyber liability insurance.

**8) A description of any strategic relationships, or both, the responder currently has or has used that could bring significant value to the Authority or a participating Public Agency**.

We take pride in truly adding value to the partner solutions we propose to our clients. Some companies in the IT industry use the term "value-added reseller" despite simply selling solutions as a prime contract holder. We differentiate ourselves from our competition by leveraging the depth and breadth of our experts' knowledge in their given fields and the expertise of the organizations we partner with to provide solutions that deliver value and performance with a personal touch.

Some of the strategic partners we engage with in cybersecurity include Rapid7, the Center for Internet Security (CIS), CrowdStrike, Fortra, Fortinet, KnowBe4, and Microsoft.

# PRICING & ASSUMPTIONS

## Pricing

### Information Technology Management Services

We have provided three pricing tiers below (small, medium, and large) with baseline volumes to help demonstrate pricing for the Authority or participating Public Agency. Any volumes above the three listed would require custom pricing. Upon beginning the tier two contracting process, the Dewpoint team would expect to perform a due diligence assessment in order to provide an optimal solution with accurate pricing for the prospective Public Agency.

#### Baseline Volumes (Small)

Estimated Monthly Pricing $5,700 (Includes Transition)

| Description | Baseline |
|---|---|
| **PCs** | Up to 50 |
| **Switches** | Up to 4 |
| **Access Points** | Up to 3 |
| **Firewalls** | 1 |
| **Servers** | Up to 5 |
| **Crowdstrike** | Up to 55 |
| **LogicMonitor License** | Up to 10 |

#### Baseline Volumes (Medium)

Estimated Monthly Pricing $9,500 (Includes Transition)

| Description | Baseline |
|---|---|
| **PCs** | 50-100 |
| **Switches** | 4-8 |
| **Access Points** | 3-4 |
| **Firewalls** | 1 |
| **Servers** | 5-10 |
| **Crowdstrike** | 55-110 |
| **LogicMonitor License** | 10-20 |

### Baseline Volumes (Large)

Estimated Monthly Pricing $13,200 (Includes Transition)

| Description | Baseline |
|---|---|
| **PCs** | 100-150 |
| **Switches** | 8-10 |
| **Access Points** | 4-6 |
| **Firewalls** | 2 |
| **Servers** | 10-15 |
| **Crowdstrike** | 110-165 |
| **LogicMonitor License** | 20-27 |

### Cybersecurity Assessment Services

| Description | Price |
|---|---|
| **Requirements A-D** | $8,000 per assessment |
| **Requirement E** | Custom Pricing |

## Assumptions

- Pricing is estimated based on volumes of users and devices. It is presented in a small/medium/large sizing approach for informational and comparative purposes, based on the high end of each tier.
- Prices, as presented, are non-binding; we accurately determine pricing based on diligence and adjust to the variables unique to each customer environment.
- The Authority or participating Public Agency designates a primary and secondary Single Point of Contact (SPOC) to act as an on-site resource at each location.
- Contracts will not start until Dewpoint receives a purchase order.
- The consultants assigned by Dewpoint to perform managed services or cybersecurity assessment services are not to be solicited for permanent employment by the Authority or participating Public Agencies.
- Services are provided as a managed service leveraging a shared resource team (not dedicated or named individuals).
- The Authority or participating Public Agency will maintain currency in licensing and maintenance contracts for operating systems, third-party vendors, hardware, and application software.

- The Authority or participating Public Agency will procure hardware and peripherals per their purchasing policy and vendor selections.
- All multi-functional devices and non-network printers are under maintenance and/or under a managed print contract with a third-party vendor. On-site support will be provided by supporting third-party or during monthly onsite visits.
- For hardware not under maintenance that is no longer functioning, Dewpoint will request the respective agency to procure new hardware.
- The Authority or participating Public Agency will update network contracts and/or maintain letters of agency with carriers for Dewpoint to perform as a customer agent.
- Inventory lists and volumes will be validated during the transition discovery phase. Change control may be required if volumes change.

GLOBAL SOLUTIONS GROUP, INC.

# Technical and Price Proposal

# Information Technology Managed Services and Cybersecurity Assessment Services

## Michigan Municipal Services Authority

## RFP Number: 2023-1

**Due Date: August 21, 2023, 5:00 P.M**

**Submitted to:**
**Samantha Harkins**
**Chief Executive Officer**

MMSA
Michigan Municipal Services Authority

Michigan Municipal Services Authority
PO Box 12012
Lansing, MI 48901-2012

**Submitted by:**
**Global Solutions Group, Inc.**

GLOBAL SOLUTIONS GROUP, INC.

25900 Greenfield Road, Suite 220
Oak Park, MI 48237
www.GlobalSolGroup.com

FORTINET AUTHORIZED PARTNER · ORACLE PARTNERNETWORK · MANDIANT · IBM PartnerWorld · CISCO Partner · Microsoft Gold Partner · MICRO FOCUS BUSINESS PARTNER · Trellix · tenable · Laserfiche · amazon web services Partner Network

This proposal contains proprietary information that shall not be duplicated, used, or disclosed for any reason other than evaluation of the proposal. If release is required due to transparency requirements, all information regarding performance methodology, pricing methodology, other items that are considered trade secrets and any Personally Identifiable Information must be redacted.

## Offeror

Global Solutions Group, Inc.
25900 Greenfield Road, Suite 220
Oak Park, MI 48237
www.GlobalSolGroup.com

| | |
|---|---|
| **UEI** | VH3UE9S2T6E5 |
| **CAGE** | 6M9L5 |
| **DUNS** | 078343325 |
| **EIN** | 20 0010736 |

ISO/IEC 27001:13 · 20000-2018 · 9001:2015

**US DoD Top-Secret Facility Clearance**

**CMMC C3PAO Candidate – ML3**

Certified EDWOSB · SBA Economically Disadvantaged Woman-Owned Small Business · SBA 8(a) Certified · SBA WOSB Woman Owned Small Business · Certified NMSDC MBE

## Contracting Vehicles

GSA Multiple Award Schedule Contract # GS-35F-171AA (Formerly Schedule 70)

GSA Multiple Award Schedule Contract # GS-02F-025GA (Formerly Schedule 736)

GSA Multiple Award Schedule Contract # GS-03F-132DA (Formerly Schedule 36)

8(a) STARS III Contract # 47QTCB21D0281

## Persons authorized to negotiate with the Government and sign the proposal and subsequent award on Offeror’s behalf:

Lisa Salvador, Vice President
Direct: (248) 291-5440
Mobile: (313) 333-0188
lisas@globalsolgroup.com

## Acknowledgement of Addenda, Questions and Answers, and other Modifications

GSG acknowledges Q/As received on August 03, 2023.

## Submit to:

**Samantha Harkins**
**Chief Executive Officer**

Michigan Municipal Services Authority
PO Box 12012
Lansing, MI 48901-2012
ceo@michiganmsa.gov

August 17, 2023

Samantha Harkins
Chief Executive Officer
Michigan Municipal Services Authority
PO Box 12012
Lansing, MI 48901-2012

**Subject:** Global Solutions Group's Response to **RFP No: 2023-1** for **Information Technology Managed Services and Cybersecurity Assessment Services**

Ms. Harkins:

Global Solutions Group, Inc. (GSG) hereby presents our proposal to provide Information Technology Managed Services and Cybersecurity Assessment Services to Michigan Municipal Services Authority (Authority). GSG is a multifaceted technology company incorporated in the State of Michigan in 2003. We are headquartered in Oak Park, Michigan.

GSG is an:

- SBA 8(a) Certified Small Business
- Certified Women Owned Small Business (WOSB)
- Certified Minority Business Enterprise (MBE)
- Economically Disadvantaged Woman - Owned Small Business (EDWOSB).

**The following is the list of GSG's Michigan Contracts:**

- Michigan Economic Development Corporation
- Macomb County
- Lansing Board of Water and Light
- Detroit Wayne Integrated Health Network
- Suburban Mobility Authority for Regional Transportation
- University of Michigan
- University of Michigan School of Medicine
- University of Michigan Hospitals
- Oakland County Academy of Media and Technology and Sigma Academy for Leadership and Early Middle College
- Grand Valley State University

GSG is an ISO/IEC 27001:2013 Information Security Management Systems, ISO 9001:2015 Quality Management System, and ISO 20000:2018 - Service Management System Certified Firm. Our team is capable of consistently delivering products and services that fulfill the needs of our customers as well as applicable legislative and regulatory requirements.

Our cyber team has experience with industry standards and best practices including NIST CSF, FISMA, FedRAMP, PCI–DSS, OWASP, CIS–CSC for Effective Cyber Defense, and others. Our expertise extends to a wide array of IT and cybersecurity technologies such as HPE, Micro Focus, IBM, Splunk, Palo Alto, FireEye, Fortinet, and Cisco, as well as premier cloud technologies such as AWS and Azure.

GSG understands that the Authority is looking for a qualified contractor who can offer cybersecurity assessment services as well as information technology management services to the Authority or participating Public Agencies, or both.

**Acknowledgments:**

| | | |
|---|---|---|
| GSG acknowledges that we will provide information technology managed services and cybersecurity assessment services to Authority and Public Agencies. **[RFP 4.1]** | GSG acknowledges that our price quote estimate remains valid for 60 days. **[RFP 4.5.e]** | There are no active legal or regulatory actions against GSG. **[RFP 4.5.f]** |

Our certified cybersecurity and IT specialists are here to provide a comprehensive approach to Authority's Information Technology Managed Services and Cybersecurity Assessment Services requirements. Our team is experienced in identifying an organization's strengths and vulnerabilities, as well as in reviewing policy requirements to ensure compliance.

Our mission is characterized by a desire to form and maintain good client relationships, provide exceptional work performance, and improve our clients' cybersecurity profile. Envisioning success for this program requires the highest level of service, ensuring that we operate efficient, agile, high-quality testing and security assessment services that are cost-effective and in compliance with all current regulatory directives and industry standards. We apply this same requirement to each customer and each project.

| Proven Experience With Information Technology Managed Services And Cybersecurity Assessment Services [RFP 4.2] | | |
|---|---|---|
| **Michigan Economic Development Corporation** | **Detroit Wayne Integrated Health Network** | **Kansas Office of Information Technology Services** |
| Providing Cybersecurity Compliance Consulting Service | Provide Comprehensive Cybersecurity Risk Assessments | Provide Information Security Officer Services |
| **Connect for Health Colorado** | **Lansing Board of Water** | **Department of Interior (DOI)** |
| Providing Chief Information Security Officer Information Technology and Security Services | Provided Penetration Testing and Digital Forensics to | Recently awarded a $25+ million BPA contract offering comprehensive cybersecurity services to federal agencies |
| **Jacksonville Aviation Authority** | **Fort Wayne–Allen County Airport Authority** | **Nevada Affordable Housing Assistance Corporation** |
| Provider Network Penetration Testing | Completed an IT Security Assessment | Provided External Network, Web Application Vulnerability Scanning, and Penetration Testing |
| **Department of the Treasury Office of the Inspector General** | **Department of Agriculture Office of the Chief Information Officer** | **U.S. AbilityOne Commission** |
| Awarded a multiyear Cybersecurity Assessment contract | Completed a $10 million nationwide BPA for Cybersecurity Assessments and Penetration Testing | Completed a multiyear contract providing Cybersecurity Audit Analysis Services |

Point of Contact Details

**Name:** Lisa Salvador, Vice President **Email:** lisas@globalsolgroup.com
**Telephone:** (248) 291-5440 (office) || (313) 333-0188 (mobile)

As Vice President of Global Solutions Group, Inc., I am fully authorized to negotiate and bind GSG during the period in which the Authority is evaluating proposals. You may contact me at any time.

Regards,

Lisa Salvador

Lisa Salvador, Vice President

## Table of Contents

## Tab 1. GSG Qualifications and Experience [RFP 4.2]

GSG is a privately held corporation founded in 2003 to provide IT support services to government agencies and private sector clients. We operate nationwide from our offices in Oak Park, Michigan. Over the past 20 years our business has grown as we supported four (4) core competencies across multiple business sectors: Cybersecurity, IT Services, Document/Data Management and Physical Security.

As our IT consulting business grew, we recognized that several of our clients were not satisfied with their existing information security services, so we started placing IT security professionals with those clients. That experience has allowed us to expand our IT services to include cybersecurity consulting. We have since added penetration testing, cybersecurity audits, and assessments as key facets of our business.

Our cybersecurity expertise has led to major multiyear contracts with the AbilityOne Commission as well as a multiyear, multimillion-dollar contract to provide operational assessment and penetration testing to all offices and agencies under the purview of the USDA nationwide. GSG was awarded a major cybersecurity assessment contract with the U.S. Department of the Treasury, Office of the Inspector General.

### GSG's Four Core Competencies

#### Cybersecurity

- Penetration Testing
- Policy and Procedure Development
- Risk Assessment
- Security Audits
- Information Assurance
- Social Engineering Security Compliance
- Incident Response Planning
- Operational Continuity Planning
- Education and Training
- Security Engineering
- Security Hardware and Software
- Security Information and Event Management
- Payment Card Industry Assessment
- Next-generation Firewalls

#### IT Services

- Cloud Hosting
- Licensing, Implementation, and Renewal Support
- IT Support
- Help Desk
- Backup/Disaster Recovery
- Database Management
- SQL
- SharePoint
- IT Managed Services
- Telephony
- IT Staffing
- Network Architecting and Administration
- Hardware

#### Document/Data Management

- Digital Transformation
- Enterprise Document Management Solutions
- Laserfiche
- OpenText
- Enterprise Records Management
- Enterprise Content Management
- Case Management
- Workflow Management
- Document Imaging System and Services
- Document Digitization
- Customer Relationship Management Systems

#### Physical Security

- Security Cameras/CCTV
- Entry Systems
- PIV, Access Control, and Personal Identification Systems
- Proprietary alerteerTM Security Monitoring Software

Our cybersecurity expertise has led to major multiyear contracts with the AbilityOne Commission as well as a multiyear, multimillion-dollar contract to provide operational assessment and penetration testing to all offices and agencies under the purview of the USDA nationwide. GSG was awarded a major cybersecurity assessment contract with the U.S. Department of the Treasury, Office of the Inspector General.

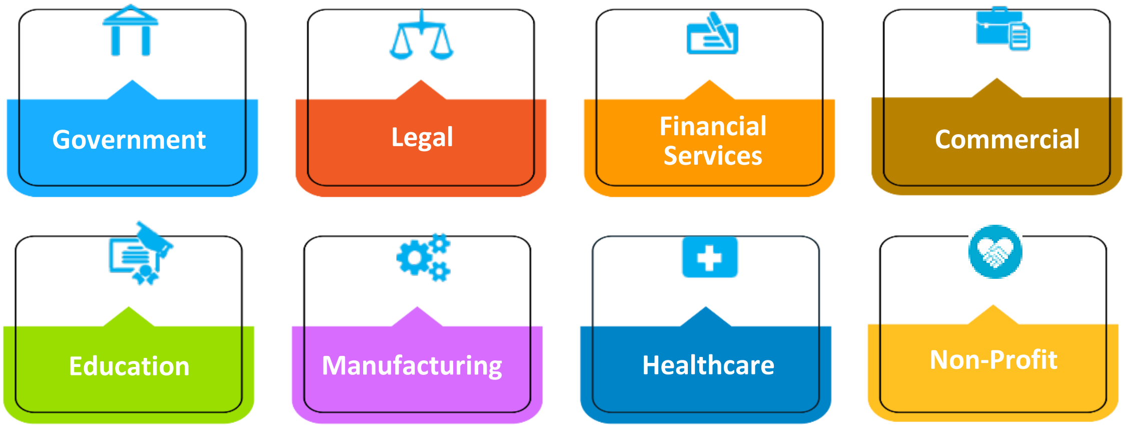
**GSG has provided Cybersecurity Assessments and Penetration Testing for over:**

- 3,500 Offices and Agencies Nationwide
- 100,000 End Points
- 120,000 Workstations
- 200,000 IPs

GSG's cybersecurity team has successfully completed more than 1,000 projects including penetration testing, cybersecurity assessments, audits, vulnerability assessment, web application security assessment, risk assessments, etc. We have experience and expertise with industry standards and best practices including the NIST Cybersecurity Framework, Federal Risk and Authorization Management Program (FedRAMP), Payment Card Industry Data Security Standard (PCI–DSS), Open Web Application Security Project (OWASP), Center for Internet Security Critical Security Controls (CSC) for Effective Cyber Defense, and various others.

We are agile in adjusting our approach to meet the specific needs of each client — whether it is a commercial operation, a state agency, or an entire Cabinet-level department with locations across the nation.

## Sectors We Serve



Government
Legal
Financial Services
Commercial
Education
Manufacturing
Healthcare
Non-Profit

# GSG is Uniquely Positioned to Fulfil MMSA's Requirements

The following table outlines how GSG differentiates us from other consultants:

| | | |
|---|---|---|
| **TEAM EXPERTISE:**<br>INDUSTRY EXPERIENCE<br>+<br>PROVEN PERFORMANCE | **GSG has experience with:**<br>♦ Long-term, complex security assessments<br>♦ Fixing vulnerabilities to improve compliance with regulatory requirements or security standards such as HIPAA, PCI DSS, or ISO 27001/27002<br>♦ **Strong knowledge base of the industry due to work on multiple projects**<br>♦ Improved and more reliable measures of confidence in cybersecurity requirements<br>♦ Oversight of contract performance and quality assurance using industry standard techniques. | **With 10 years' experience in cybersecurity and 1000+ completed projects, GSG is capable of managing and meeting the demands for MMSA's required cybersecurity services.**<br>♦ GSG will identify exposures in your application configurations and network infrastructure and using proven process, industry standards resolve those issues.<br>♦ GSG understands the importance of IP, sensitive and confidential data.<br>♦ Highlights real risks of an actual hacker successfully breaching your defenses. |
| **HIGHLY QUALIFIED STAFF** | Our key personnel:<br>♦ Average of **15 years** of experience in IT security support<br>♦ Have worked together as a team on over 40+ assignments<br>♦ Have performed hundreds of web application assessments and network penetration tests. | ♦ The same Key Staff proposed for MMSA recently implemented continuous monitoring Configuration Baseline standards enterprise-wide for 2,000 endpoints and servers for the Department of Labor.<br>*This showcases our ability to work large projects, under tight timelines and deliver a timely work product for our client.* |
| **HIGHEST QUALITY SERVICE** | ♦ With an approach tailored to meet the Authority's requirements, our team utilizes industry best practices, bleeding-edge technology, and first-rate research to understand, anticipate, and protect against even the most advanced intrusion attempts | ♦ GSG will deliver an IT ecosystem that is hardened against attacks, ensuring continuity of uninterrupted services and security of data that meets all cybersecurity standards. |

## SNAPSHOT OF GSG PROJECTS SIMILAR AND RELEVANT TO MMSA

### LARGE FEDERAL CONTRACTS

| | | |
|---|---|---|
| DOI | $25+M | Cybersecurity Services |
| USDA | $10M | Cybersecurity Assessments and Penetration Testing |
| DOT | $1.9 M | Cybersecurity Assessment Service Support |

### PROJECTS SIMILAR IN SIZE AND SCOPE

| | |
|---|---|
| Fort Wayne–Allen Co. Airport Auth. | IT Security Assessment |
| Jacksonville Aviation Authority | Network Penetration Testing |
| City of New Orleans | Cyber Services |
| City of San Jose | Cyber Products and Services |
| Maricopa County | Cyber Penetration Testing Services |
| NV Affordable Housing Assist. Corp. | Network Penetration |
| Maricopa County | Cyber Penetration Testing Services |

## Snapshot of GSG projects Similar and Relevant to MMSA

| | | |
|---|---|---|
| | City of Sunnyvale | IT Strategic Planning, Process Redesign, Technical Support Services |

GSG offers twenty years of lessons learned from providing directly relevant work performing on large-scale city, state, and federal government contracts, as well as on projects for a variety of commercial and non-commercial clients. Through our team's experience in IT services, including our involvement in government, public services, account administration, and data management we ensure the reduction of risk and the provision of timely, cost-effective services to the satisfaction of all stakeholders.

Our team has provided **penetration testing, risk assessment, cybersecurity assessment, vulnerability assessment, threat management, security auditing, security operations, and other cybersecurity services** for various other government agencies and private sector businesses and organizations, including:

| Work Performed | Customer |
|---|---|
| **Large Federal Contracts** | |
| $25M Cybersecurity Services | Department of Interior |
| $1.9M Cybersecurity Assessment Support | Department of Treasury |
| $9.8M Penetration Testing, Web Security | Department of Agriculture |
| **Other Cyber-Related Contracts** | |
| Network Disaster Recovery Plan | Suburban Mobility Authority for Regional Transportation |
| Cybersecurity Consulting | National Cooperative Purchasing Alliance |
| Cybersecurity Services | Maricopa County |
| | Golden Gate Bridge Highway and Transportation District |
| | Commonwealth of Massachusetts |
| | State of New Mexico Human Services Department |
| | City of New Orleans |
| | Michigan Economic Development Corporation |
| | Department of the Interior |
| Digital Forensic Examinations | Lansing Board of Water and Light |
| Forensic Investigation | Kansas Board of Tax Appeals |
| Information Security Monitoring | City of Sunnyvale |
| Information Security System Audit | Johnson County Community College |
| Internal and External Network Testing | Housing Authority of the Birmingham District |
| IT and Security Consulting and Services | Connect for Health Colorado |
| IT Cybersecurity Services | San Diego County Regional Airport Authority |
| IT Forensic Investigation | Kansas Department of Corrections |
| IT Infrastructure Analysis and Updates | Medical College of Wisconsin |
| IT Infrastructure Security Review | U.S. AbilityOne Commission |
| IT Network Architecture Assessment | City of Chicago Department of Assets Information and Services |
| IT Environment Comprehensive Review | Regional Water Resource Agency |
| IT Security Assessment | Prince George's Community College |
| | Lone Star College |
| | Department of Agriculture |
| IT Security Consulting | Kansas State |

| | |
|---|---|
| IT Support and Vulnerability Testing | City of Grand Rapids |
| Long-Range Technology Plan | Capital Area Transportation Authority |
| Network Penetration Assessment | Nevada Affordable Housing Assistance Corporation |
| Network Penetration Network Testing | Fort Wayne–Allen County Airport Authority |
| | Jacksonville Aviation Authority |
| Penetration Testing | Department of Agriculture |
| | Virginia Retirement System |
| | Grand Valley State University |
| Security Assessment | Kansas Department of Health and Environment |
| | Port Authority of Allegheny County |
| Security Audits/ Computer Risk Assessment | Detroit Wayne Integrated Health |
| Security Information/ Event Management | Univ. of Michigan School of Medicine |
| Security Specialist Support | Maryland State Department of Education |
| Systems Security Services | Department of the Treasury |
| Threat Modeling, Vulnerability Assessment | Call Tower, Inc. |
| Upgrade IT Infrastructure | Montana State University |
| Wireless Penetration Testing | U.S. Department of Agriculture |

### *a) Accolades from GSG's Clients*

GSG has received the following accolades from multiple clients:

| | | |
|---|---|---|
| Douglas Nash<br>Assistant CIO<br>APHIS Marketing and Regulatory Programs Business Services | APHIS | Thanks for your help with the penetration testing and follow-up analysis. Your team did a great job working with our two agencies. |
| Joseph Binns<br>Director, Information Security Office, USDA<br>Food, Nutrition, and Consumer Services | USDA | GSG was a highly independent team, who required very minimal guidance from USDA and provided outstanding output. These facts allowed for less oversight, which allowed Government assets to be utilized elsewhere which is a cost savings and a benefit to the Government. All in all, fantastic job. |
| Victor J Cernius<br>Director of Operations<br>Regional Water Resource Agency | RWRA | GSG, Great job on the presentation today and a wonderful job from start to finish on this. The whole effort took longer than anticipated, but we certainly appreciate all of your time and effort to deliver the package that you did. We understand this was not an easy task. |
| Greg Glover | NEVADA HARDEST HIT FUND | I do want to say that it has been a pleasure working with GSG Inc on this project and look forward to working with your organization in the future. |

| | | |
|---|---|---|
| Info. Tech. System Mgr.<br>Nevada Affordable Housing Assistance Corp | | |
| Kasey Koch<br>Contracting Officer<br>USDA Office of Information Security | | Quality Control was exceptional. Reports were carefully reviewed in full and were flawless in presentation and content. |
| Randy Diehl<br>MIS Director<br>Maryland State<br>Depart. of Education | | I really enjoyed working with you. What you were able to put together for us in such a short period of time was amazing. Please take care and be safe. |
| Kimberly Carson<br>Lead Contract Specialist<br>GSA Region 4 | | Global Solutions Group is customer focused and engaged in the activities of the Agency. They were very receptive and adaptable to organizational changes. Global Solutions Group has maintained open communications with the Contracting Team. |
| Joelene (Jody) Allen<br>Executive Director<br>Kansas Board of Tax Appeals | | Global Solutions Group, Inc. (GSG) rescued our state agency when our system was attacked by a Trickbot trojan. Once our agency contacted GSG; they were on on-sight quickly and started the process of removing the trojan. While working on the source hit by the trojan, Global diligently ran scans on all servers and PCs to assure the trojan had not attacked any other part of our system. GSG's expertise, professionalism, and diligence kept our entire system in tack.'<br>'Since then, our agency has had four additional contracts with GSG, including one that updated our entire server system. With GSG's expertise, the agency was able to go down to three servers versus the eleven servers that were currently being used. 'GSG will always be our 'go-to;' as they provided excellent service at a very reasonable cost.' |

## Tab 2. Technical Approach to Scope of Services [RFP 4.3]

GSG operates at the highest level of efficiency with certified practices in CMMI L3, ITIL, ISO 9001:2008, ISO 20000, and ISO 27001. We focus on a proactive, responsive approach, and conduct penetration testing service delivery model for Continual Service Improvement (CSI).

**Our goal is to exceed service-level targets.**

GSG provides a seamless transition and continuity of service delivery based upon our experience of processes, procedures, tools, and technologies. We provide the Authority with a better Return on Investment (ROI) by providing high availability, high quality, high reliability, high security, high performance, and efficient operations. **We have eight goals to best support Authority:**

1. **Evolve the current architecture and processes** to enable rapid, affordable, secure delivery, and lifecycle support of IT services that meet the operational needs of the Authority.
2. Achieve **high availability and reliability** governed by properly architecting the solutions, proactive monitoring, and effective change management.
3. Ensure **maintainability** to deal with the introduction and reversal of change with effective change management.
4. Ensure **sustainability** through technology refresh, performance management, and capacity planning.
5. Provide **scalability** to proactively meet changing requirements and mission objectives.
6. Provide **secure IT infrastructure** by following the Authority standards, processes, and technologies.
7. Reduce the **cost** of operating and maintaining the current technical environment while meeting or exceeding performance targets.
8. Incorporate the **innovative capabilities** we gained through CMMI and ISO process-based development and quality assurance.

GSG's approach to performing the technical areas that are listed in **Scope of Services** is explained in detail in subsequent sections. The technical approach and methodologies are based on our collective experience operating within large infrastructure environments, utilizing technology tools to eliminate weaknesses in highly regulated information security architecture environments.

Our approach includes deployment of enterprise-level strategies to promote lower levels of redundancy, while sustaining or exceeding overall job performance. GSG has an experienced team, expertise, and proven processes to manage all the tasks listed in **Scope of Services**, offering a collaborative partnership that ensures lowered costs with increased quality.

## *a) Information Technology Management Services* *[RFP 2.1]*

### *(A) Management of Firewalls, Anti-Virus, Anti-Malware, and Threat Identification*

GSG will proactively manage and protect against cyber threats, which helps in reducing the risk of data breaches, financial losses, and reputational damage.

| | | |
|---|---|---|
| GSG's IT management services related to **Firewalls** typically involve: | **Firewall Configuration and Deployment** | We will set up and configure firewalls to suit the Authority security requirements and network architecture. |
| | **Firewall Monitoring** | GSG will continuously monitor firewall logs and traffic patterns to identify potential security breaches or anomalies. |
| | **Firewall Rule Management** | We regularly review and update firewall rules to ensure they are up-to-date and align with the organization's security policies. |
| | **Intrusion Detection/Prevention Systems (IDS/IPS) Integration** | GSG will integrate intrusion detection and prevention systems with firewalls to detect and block suspicious activities. |

| | | |
|---|---|---|
| GSG's IT management services related to **Anti-Virus and Anti-Malware** typically include: | **Anti-virus Deployment** | GSG will install and configure anti-virus software on all endpoints, servers, and network devices. |
| | **Regular Updates** | We ensure that anti-virus and anti-malware software is regularly updated with the latest virus definitions and security patches. |
| | **Real-time Monitoring** | GSG will monitor systems in real-time to detect and respond to malware infections promptly. |
| | **Quarantine and Remediation** | We will isolate infected systems and performing necessary actions to clean and restore them to a secure state. |

| | | |
|---|---|---|
| GSG's IT management services related to **Threat Identification** typically include: | **Security Information and Event Management (SIEM)** | GSG will collect and analyze security event data from various sources to identify potential security incidents. |
| | **Threat Intelligence** | We stay up to date with the latest threat intelligence to understand emerging cyber threats and vulnerabilities. |
| | **Vulnerability Assessment** | GSG will conduct regular scans and assessments to identify weaknesses in the IT infrastructure that could be exploited by attackers. |
| | **Penetration Testing** | We will simulate real-world attacks to assess the effectiveness of existing security measures and identify areas of improvement |

.

### *(B) Proactive Monitoring and Alerts*

Our Proactive monitoring involves continuously observing the health, performance, and security of an Authority's IT infrastructure and applications. It typically involves the use of specialized software tools that track various metrics, such as server performance, network activity, application response times, and security events. By monitoring these metrics in real-time, IT professionals can identify potential problems or vulnerabilities before they escalate into major issues.

GSG will detect and address potential problems before they lead to system failures or downtime. This proactive approach helps in reducing downtime and minimizing disruptions to business operations. By monitoring system resources and performance, IT managers identify bottlenecks and optimize configurations, leading to better overall performance.

Our Continuous monitoring allows the resources to identify suspicious activities or security breaches early on, enabling them to respond swiftly and mitigate potential damage. Through Proactive monitoring we provide valuable data and insights, allowing IT managers to make informed decisions about resource allocation, capacity planning, and technology investments.

When the monitoring system detects a potential issue, it sends out notifications or alerts to IT staff, indicating the nature and severity of the problem. GSG will configure the alerts to trigger based on predefined thresholds or unusual events. GSG will investigate the root cause of the issue and take appropriate action to resolve it.

### *(C) On-Site and Remote Support Services*

GSG aims to optimize the organization's IT environment, enhance security, reduce operational downtime, and enable efficient use of technology resources. Our IT operations enhance the productivity and ensure a smooth and secure technology environment.

| | | |
|---|---|---|
| **GSG's**<br>**On-Site Support Services** | **Hardware Maintenance** | GSG will provide maintenance and repair services for physical IT equipment, such as servers, workstations, networking devices, and peripherals. |
| | **Troubleshooting** | GSG's On-site support personnel will address technical issues that cannot be resolved remotely, ensuring prompt resolution and minimal downtime. |
| | **Upgrades and Installations** | They handle the installation of new hardware or software components and perform upgrades to existing systems. |
| | **IT Asset Management** | We manage the lifecycle of IT assets, including procurement, inventory, tracking, and disposal. |
| **GSG's**<br>**Remote Support Services** | **Help Desk Support** | Our IT experts aid and guidance to end-users through phone, email, or chat, resolving software-related issues, password resets, and general IT inquiries. |
| | **Remote Monitoring and Management (RMM)** | GSG's IT teams will use specialized tools to monitor and manage networks, servers, and endpoints remotely, detecting and addressing potential problems proactively. |
| | **Software Updates and Patch Management** | We regularly apply software updates and security patches to ensure systems are up to date and protected against vulnerabilities. |
| | **Remote Troubleshooting** | Our IT technicians remotely diagnose and resolve technical problems on users' computers or devices |

.

## *(D) Private, Hybrid, and Public Cloud Options*

GSG's private, hybrid, and public cloud options allow us to choose the best cloud model that aligns with specific requirements, budget, and security considerations.

| | |
|---|---|
| **PRIVATE CLOUD**<br>*Through the Private Cloud environment, we offer greater control, security, and customization. It can be tailored to meet the specific needs of the Client, comply with regulations, and address any security concerns related to sensitive data.* | • Designing and setting up the private cloud infrastructure.<br>• Managing and monitoring the private cloud environment.<br>• Security services, such as access controls, encryption, and threat detection.<br>• Regular maintenance and updates to ensure optimal performance. |
| **HYBRID CLOUD**<br>*With hybrid cloud, we offer flexibility and scalability, by utilizing the public cloud for less sensitive tasks while keeping critical data and applications in the private cloud.* | • Integrating and managing both private and public cloud resources.<br>• Data synchronization and migration between the two environments.<br>• Implementing a secure and efficient communication channel between clouds.<br>• Hybrid cloud optimization and cost management |
| **PUBLIC CLOUD**<br>*By utilizing the public cloud, GSG will provide scalability, cost-effectiveness, and ease of use.* | • Selecting appropriate public cloud providers /services.<br>• Deploying and managing applications on the public cloud.<br>• Ensuring data security and compliance in a shared environment.<br>• Optimizing cloud resources to control costs. |

## *(E) On-Call Infrastructure Professionals*

GSG's On-Call Infrastructure Professionals are available to provide support and assistance on an as-needed basis, often outside of regular business hours. Our professionals may be called upon during emergencies, system outages, or to manage critical issues that require immediate attention. They ensure that the IT infrastructure remains operational and will quickly respond to unexpected situations that may arise. They focus on core activities leading to improved efficiency, reduced downtime, and enhanced overall IT performance.

The key responsibilities of on-call infrastructure professionals include:

| | |
|---|---|
| **Incident Response** | Our incident response team are the first point of contact when critical incidents occur outside of regular business hours. They will quickly diagnose and resolve issues to minimize downtime and service disruptions. |
| **Monitoring and Alerts** | GSG's on-call professionals continuously monitor infrastructure and services using various tools to detect any anomalies or performance degradation. They respond promptly to alerts and notifications. |
| **Troubleshooting** | When incidents occur, our on-call engineers will perform root cause analysis and troubleshoot problems to find the most effective solutions. |
| **Escalation** | If a problem requires specialized expertise or falls outside the on-call engineer's scope, GSG will escalate the issue to the appropriate team or senior personnel. |
| **Documentation** | GSG's resources will maintain detailed documentation of incidents, resolutions, actions taken, which is valuable for future reference. |
| **Preventive Maintenance** | Our on-call infrastructure professionals also engage in proactive measures to prevent potential issues. This includes regular |

| | |
|---|---|
| | maintenance tasks and implementing best practices for system stability. |
| **Collaboration** | Our certified experts will work closely with other teams, such as development, network operations, and security, to ensure a cohesive and well-coordinated response to incidents. |
| **Post-Incident Analysis** | After resolving incidents, GSG will participate in post-mortem discussions to analyze the root cause and implement measures to prevent similar issues in the future |

## *b) Cybersecurity Assessment Services* *[RFP 2.1]*

### (A) Independent View of Current Information Technology Security Measures

GSG provides a comprehensive report with findings, recommendations, and a roadmap for improving the Authority's security posture. We utilize the following key components for cybersecurity assessment services.

| | |
|---|---|
| **Vulnerability Assessment** | Our assessment involves scanning the network, systems, and applications to identify known vulnerabilities. Vulnerability scanners help to discover weaknesses that malicious actors could exploit. |
| **Penetration Testing (Pen Testing)** | GSG’s Pen testers, attempt to simulate real-world attacks on an Client's systems and networks. They try to exploit vulnerabilities to assess how well the existing security measures hold up and where improvements are needed. |
| **Risk Assessment** | Our risk assessment helps in identifying potential threats and their potential impact on an organization's assets. It also evaluates the likelihood of those threats occurring. |
| **Security Policy and Procedure Review** | We evaluate existing security policies and procedures to ensure they align with industry best practices and regulatory requirements. |
| **Security Awareness Training** | GSG will assess the level of security awareness among employees and conduct training sessions to educate them about various security risks and best practices. |
| **Incident Response Preparedness** | GSG will assess the Client’s preparedness to respond to cybersecurity incidents effectively. This includes reviewing incident response plans, protocols, and coordination among stakeholders. |
| **Data Protection and Privacy Assessment** | GSG evaluates the Client's data protection practices and compliance with relevant privacy regulations. |
| **Network Security Assessment** | We analyze network architecture, firewall configurations, and other security measures to identify potential weaknesses. |
| **Web Application Security Assessment** | GSG will review the security of web applications to identify vulnerabilities like SQL injection, cross-site scripting (XSS), etc. |
| **Physical Security Assessment** | GSG will evaluate physical security measures such as access controls, surveillance systems, and data center security. |
| **Compliance Assessment** | We ensure that the Client adheres to relevant industry standards (e.g., ISO 27001) and regulatory requirements (e.g., GDPR, HIPAA). |

## (B) Recommendations for Modified Information Security Measures based upon Stated Priorities and Identified Vulnerabilities

Our Cybersecurity professionals will perform tailored assessments and will provide specific recommendations critical for achieving robust security. We will continuously reassess and adapt security measures based on emerging threats and changing business priorities. GSG's general recommendations for cybersecurity assessment services and modifying information security measures based on stated priorities and identified vulnerabilities are as follows:

| | |
|---|---|
| **Prioritizing Security Measures** | GSG will align security measures with the Client's overall goals and objectives by considering the criticality of assets and data, focusing on protecting the most valuable and sensitive information first. We will assess the potential impact of a security breach and prioritize based on the severity of consequences. |
| **Conducting Risk Assessment** | GSG will / evaluate potential risks, threats, and vulnerabilities in the Client's information systems and networks. Will analyze the likelihood of an attack and the potential impact on the Client if a vulnerability is exploited. The risk assessment will be utilized to prioritize security efforts and allocate resources effectively. |
| **Implementing a Layered Defense Strategy** | GSG will deploy multiple layers of security measures to create a robust defense against various attack vectors by considering using a defense-in-depth approach that includes firewalls, intrusion detection/prevention systems, access controls, encryption, etc. |
| **Performing Regular Vulnerability Assessments and Penetration Testing** | We will conduct periodic vulnerability assessments and penetration testing to identify weaknesses in Client's systems and will use these tests to gain insights into potential threats and address vulnerabilities before malicious actors exploit them. |
| **Employee Training and Awareness** | We will educate the staff about cybersecurity best practices, social engineering threats, and how to recognize potential phishing attempts as employees play a crucial role in safeguarding the organization's data and systems. |
| **Secure Software Development** | GSG will prioritize secure software development practices to reduce the likelihood of introducing vulnerabilities in applications. Implement code reviews, use secure coding guidelines, and conduct security testing during the development lifecycle. |
| **Incident Response and Recovery Plan** | GSG will establish a comprehensive incident response plan to manage security breaches promptly and effectively. We will practice incident response scenarios through simulations and exercises to ensure preparedness. |
| **Continuous Monitoring and Auditing** | Our certified experts will implement continuous monitoring and auditing of the Client's systems to detect any suspicious activities/ unauthorized access. Use security information and event management tools to centralize log analysis, generate real-time alerts. |
| **Compliance and Regulatory Adherence** | GSG will stay up to date with changes in the regulatory landscape to avoid potential legal and financial consequences ensuring that the Client's security measures comply with relevant industry standards and regulations. |
| **Regular Review and Adaptation** | We will regularly review, and update security measures based on new threats and changing priorities |

## (C) Recommendations for Improving Short-Term and Long-Term Planning to Increase Information Technology Security

GSG's **Short Term Planning** to enhance information technology security is as follows:

| | |
|---|---|
| **Threat Assessment** | GSG will conduct a thorough assessment of potential cybersecurity threats that your organization may face. Understand the latest attack vectors, vulnerabilities, and tactics used by cybercriminals. |
| **Risk Analysis** | We identify critical assets, data, and systems that need protection the most. Perform a risk analysis to prioritize security efforts and allocate resources effectively. |
| **Employee Training** | We will educate all employees about cybersecurity best practices, including how to recognize and avoid common security threats like phishing attacks or social engineering. |
| **Patch Management** | GSG ensures that all software, operating systems, and applications are regularly updated with the latest security patches and fixes. |
| **Access Control** | GSG will implement strong access controls and least privilege principles to limit user access to sensitive data and systems. |
| **Incident Response Plan** | We develop a clear and well-documented incident response plan to manage security breaches effectively when they occur. |
| **Encryption and Authentication** | GSG uses encryption for data in transit and at rest. Implement multi-factor authentication (MFA) to add an extra layer of security to user accounts. |
| **Security Monitoring** | We set up continuous monitoring and auditing of your IT infrastructure to detect suspicious activities/ potential security breaches in real-time. |
| **Backup and Recovery** | Regularly back up critical data and test the restoration process is performed to ensure data recovery in case of a cyber incident. |

GSG's **Long-Term Planning** to enhance information technology security is as follows:

| | |
|---|---|
| **Security Governance** | GSG will establish a clear security governance framework that includes policies, standards, and procedures for the organization. |
| **Security Awareness Program** | GSG will develop an ongoing security awareness program to keep employees informed about the latest threats and best practices. |
| **Security Culture** | We will foster a security-first culture throughout the organization, where every employee understands their role in maintaining cybersecurity. |
| **Penetration Testing** | GSG conducts regular penetration testing and vulnerability assessments to identify weaknesses in your security infrastructure. |
| **Security Architecture Review** | GSG will periodically review the Client's IT security architecture to ensure it aligns with industry best practices and standards. |
| **Threat Intelligence** | GSG utilizes threat intelligence services to stay updated on emerging threats and tactics used by cyber attackers. |

| | |
|---|---|
| **Continuous Improvement** | We create a process of continuous improvement for your cybersecurity measures, considering lessons learned from past incidents. |
| **Regulatory Compliance** | GSG will stay abreast of relevant cybersecurity regulations and ensure that your organization remains compliant. |
| **Red Team Exercises** | We run red team exercises to simulate real-world attacks and test your organization's response capabilities. |
| **Invest in Technology** | GSG invests in advanced cybersecurity technologies, such as Intrusion Detection Systems (IDS), Security Information And Event Management (SIEM) solutions, and endpoint protection platforms. |

### *(D) Recommendations for Information Security Best Practices*

GSG’s recommendations for information security best practices for cybersecurity assessment services are as follows:

| | |
|---|---|
| **Use Standard Frameworks** | GSG utilizes well-established cybersecurity frameworks such as NIST Cybersecurity Framework, ISO/IEC 27001, or CIS Critical Security Controls as a basis for conducting assessments. These frameworks provide comprehensive guidelines for evaluating security posture. |
| **Engage Experienced Professionals** | We ensure that the cybersecurity assessment team consists of experienced and skilled professionals with expertise in various domains of information security. Our Certified professionals (e.g., CISSP, CISA, CISM) will bring valuable insights and knowledge to the assessment. |
| **Conduct Risk Assessments** | GSG will incorporate risk assessment methodologies to identify and prioritize potential threats based on their impact and likelihood. This enables the organization to allocate resources effectively to address critical risks first. |
| **Perform Vulnerability Assessments** | We conduct regular vulnerability assessments to identify weaknesses and vulnerabilities in the organization's IT systems, networks, and applications. |
| **Penetration Testing** | GSG performs ethical hacking exercises, such as penetration testing, to simulate real-world attacks and discover potential weaknesses that may not be evident in other assessments. |
| **Review Access Controls** | GSG will assess the effectiveness of access controls, both physical and logical, to ensure that only authorized individuals can access sensitive data and resources. |
| **Review Incident Response Plans** | We evaluate the Client's incident response plans and procedures to identify areas for improvement and to ensure a prompt and effective response to security incidents. |
| **Secure Data Handling** | GSG will assess how sensitive data is collected, stored, processed, and transmitted to ensure compliance with data protection regulations and industry best practices. |
| **Review Employee Security Awareness** | GSG evaluates the Client's security awareness training programs to ensure that employees are knowledgeable about security risks and best practices. |

| | |
|---|---|
| **Document Findings and Recommendations** | We document all findings and provide actionable recommendations for addressing identified security gaps/ vulnerabilities. |
| **Continuously Improve** | GSG will regularly reassess the Client's security posture to adapt to evolving threats and technologies. |
| **Maintain Confidentiality** | We ensure that all data collected during the assessment remains confidential and is managed securely to avoid potential leaks or misuse. |

## (*E*) Assistance with Implementation of Sections 2(a)(2)(B) to 2(a)(2)(D)

Since information security is an ongoing process, GSG provides a proactive approach to address new and evolving threats. We will regularly review and update the Client's security measures to stay ahead of potential risks and vulnerabilities. Below specified are key steps and best practices for information security implementation:

| | |
|---|---|
| **Risk Assessment** | GSG will perform a thorough risk assessment to identify potential vulnerabilities and threats to the Client's information assets as understanding the risks allows the Client to prioritize security efforts effectively. |
| **Security Policies and Procedures** | We will develop comprehensive information security policies and procedures that address various aspects of security, such as access control, data classification, incident response, and acceptable use. Make sure these policies are regularly updated and communicated to all employees. |
| **Access Control** | GSG will implement strong access controls to limit access to sensitive information only to authorized personnel. This includes using strong passwords, multi-factor authentication, and least privilege principles. |
| **Data Encryption** | We will encrypt sensitive data, both in transit and at rest as encryption ensures that even if data is intercepted or stolen, it remains unreadable without the appropriate decryption keys. |
| **Employee Training and Awareness** | We train employees on information security best practices, potential risks, and their roles and responsibilities in maintaining security. Will regularly conduct security awareness programs to foster a security-conscious culture within the organization. |
| **Regular Security Updates and Patch Management** | GSG will keep all software, operating systems, and applications up to date with the latest security patches and updates. Since vulnerabilities in software are often patched by vendors, and failing to apply updates could leave systems exposed to attacks. |
| **Network Security** | We will implement firewalls, intrusion detection/prevention systems, and secure configurations to protect the Client's network from unauthorized access and potential cyber threats. |
| **Incident Response Plan** | We will develop a well-defined incident response plan that outlines the steps to be taken in case of a security breach. Regularly test and update this plan to ensure its effectiveness. |
| **Regular Auditing and Testing** | We will conduct periodic security audits and penetration testing to identify weaknesses and gaps in the Client's security posture. Regular testing helps you stay one step ahead of potential attackers. |

| | |
|---|---|
| **Mobile Device Security** | GSG will implement Mobile Device Management (MDM) solutions and enforce security policies for mobile devices used within the organization. |
| **Backup and Disaster Recovery** | We regularly back up critical data and have a disaster recovery plan in place to ensure business continuity in case of data loss or system failure. |
| **Compliance** | We ensure that GSG complies with relevant data protection and privacy regulations and standards, such as GDPR, HIPAA, PCI DSS, etc. |

**GSG's cybersecurity personnel have successfully completed over 1,000 projects over the past 10 years.**

## Tab 3. Other Information Required Response

### a) *Mandatory Qualifications* *[RFP 4.b]*

GSG manages the delivery of cybersecurity services for providing and executing the agreed-upon cybersecurity solutions. We provide the services by adhering to high ethical standards, meeting industry best practices, and maintaining a level of professionalism in all interactions.

GSG will assign a dedicated single point of contact for the Authority (**Vicki Shah, Project Manager**) and she will be responsible for the direction and supervision of services provided. We ensure that the assigned point of contact will not the changed without approval from the agency.

GSG agrees that we will not subcontract duties under its contract with the Authority or a participating Public Agency without the approval of the Authority or the participating Public Agency.

GSG ensures that we keep informed about the updates of all progress, status and pending matters to the Authority.

Our Security Program Assessment provides an analysis of the effectiveness of a company's security controls based upon compliance with identified industry standards, regulations, and statutes, such as FERPA, PCI-DSS 3.2.1, GLBA Safeguards Rule, GDPR (the European Union privacy standard), HIPAA, NIST Cyber Security Framework, CIS CSC 20 Security Controls, NIST SP800-53r4, NIST SP800-171r1 and NIST Risk Management Framework (RMF).

GSG will assess your security environment to ensure that you follow each regulation that governs your industry which includes review of current documentation, policies and practices, interviews with key personnel comparisons against "best practices." In performing cybersecurity services, our team can examine security elements including:

- Security policies, standards, and guidelines frameworks
- Security organization and infrastructure
- Security asset classifications
- Personnel security and training
- Physical and environmental security
- Network, communications, and operations management
- Telecommunications security
- Systems development and maintenance
- Security administration and access control
- Anti-virus protection
- Incident response identification and response
- Business continuity planning
- Legal compliance
- Privacy

In Security Technology Assessment we perform a high-level security review of the external security boundary along with selected key areas and systems to determine potential vulnerabilities and risks where primary systems and areas of interest include:

- Internet connectivity
- Remote access
- Business partner connections
- Critical internal network infrastructure
- Application security infrastructure

The experience of 40+ GSG cybersecurity initiatives is listed in the following table.
Some details have been withheld because of its nature.

## State Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | **Michigan Economic Development Corporation** | MEDC<br>MICHIGAN ECONOMIC DEVELOPMENT CORPORATION | Cybersecurity Technical Services | Provided cybersecurity technical services and a full range of cybersecurity compliance services including gap analyses, POAMs, SPPRs, and remediation. Assisted in applying NIST Special Publication 800-171 required for meeting DFARS 252.204-7012 requirements, and CMMC compliancy for all DoD and DHS contracts. |
| 2 | **Virginia Retirement System** | VRS Virginia Retirement System | Penetration Testing Services | Internal/External penetration testing services which included: Source Code Review, Wireless Network Penetration Testing, Social Engineering, Physical Social Engineering. Specialized Security Assessments for Firewall and Routers, Database Architecture, Active Directory and Azure Active Directory, and Telecommunications. |
| 3 | **Kansas State**<br>*Office of Information Technology Services* | Kansas<br>Office of Information Technology Services | IT Security Consulting | Provided an Information Security Officer who advised senior management on risk levels and security posture, help establish a cybersecurity risk management program. Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. |
| 4 | **Nevada Affordable Housing Assistance Corporation** | NEVADA HARDEST HIT FUND<br>NEVADA AFFORDABLE HOUSING ASSISTANCE CORPORATION | Internal and External Network Penetration Assessment | Performed an internal and external network penetration assessment to verify that the security controls implemented by networks infrastructure and supporting systems provided an adequate level of protection. Our team used a broad range of commercial and public tools from our Virtual Security Test Center (VSTC). |
| 5 | **Kansas Board of Tax Appeals** | Kansas Board of Tax Appeals | Forensic Investigation and IT Environment Evaluation | Evaluated IT environment to determine the extent of a malware infection. Conducted a forensic investigation to determine what data had been exposed, and re-imaged infected workstations. Ensured that all workstations and servers were patched, and the antivirus was operated correctly with latest versions of the signature files and scan engine. |
| 6 | **Kansas Department c Corrections** | Kansas<br>Department of Corrections | IT Forensic Investigation | Conducted a forensic investigation of one server. Tracked file permission tasks using logs and determined the user ID that changed file permissions on the server, authorizing access to restricted files. |
| 7 | **Commonwealth of Massachusetts** | COMMONWEALTH OF MASSACHUSETTS | Cybersecurity Services | Data and cybersecurity services. PCI-related services with a full range of audit, penetration tests, reviews, and validation of compliance with legal, regulatory and policy requirements. Also performed data breach investigation, remediation, and security of confidential information. |

| | | | | |
|---|---|---|---|---|
| 8 | **Kansas**<br>*Department of Health and Environment* | | Security Assessment | Provides application security assessment. Utilized various tools and methodologies to identify any potential vulnerabilities within the application and tests how it responds to both manual and automated attacks. |

## Transportation Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | **Suburban Mobility Authority for Regional Transportation** | | Cloud Based Email Security | Teamed with Trellix to provide email security for 500 users. Features included pre/post-delivery detection, anti-virus and malware scanning and anti-phishing support. |
| 2 | **Suburban Mobility Authority for Regional Transportation** | | Computer Network Disaster Recovery Plan | Developed a computer network disaster recovery plan. Reviewed the current network, identified mission critical applications should an operations disaster occur. The Disaster Recovery plan that included multiple locations, two data centers with cloud recovery functionality. |
| 3 | **Detroit Transportation Corporation – People Mover** | | Document Scanning and Laserfiche Software services | Digitized all the old maps (including maps up to 60" wide and varying lengths), plans, contracts, and other records for DTC. Performed document preparation, records inventory for off-site for permanent archival, scanning, indexing, and conducting OCR and metadata operations on backlogged documents. |
| 4 | **San Diego County Regional Airport Authority** | | On-Call IT Cybersecurity Services | Data breach incident investigation and response, vulnerability assessment, penetration testing, critical controls assessment and compliance testing, business and operation risk assessment, documentation services, network systems, and application services. |
| 5 | **Jacksonville Aviation Authority** | | External And Internal Network Penetration Network Testing<br>*Supporting 4 Airports* | Network penetration testing encompassed 25 secure VLANs containing sensitive systems and data and 95 general purpose/non-security sensitive VLANS. Test integrated with the FAA Cybersecurity Strategy, TSA security requirements and PCI-DSS and Criminal Justice Information System Security Policies. |
| 6 | **Fort Wayne–Allen County Airport Authority** | | External And Internal Network Penetration Network Testing | Performed extensive IT internal and external network security assessment, reviewed of network device configurations, application and wireless penetration testing. Vulnerabilities were identified and resolved in accordance with industry best practices. |

| | | | | |
|---|---|---|---|---|
| 7 | **Capital Area Transportation Authority** | CATA | Long-Range Technology Plan | Created a Long-Range Technology Plan and the development of multiple long-term and risk assessment strategies. |
| 8 | **Port Authority of Allegheny County** | Port Authority | Security Assessment and Business Process, Infrastructure Consultation | Provided business process, infrastructure, and security assessment. Reviewed/Assessed and current IT services including IT financial, existing IT software/system design. Made system upgrade recommendations for infrastructure to streamline business processes. |

## Federal Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | **U.S. AbilityOne Commission** | U.S. AbilityOne COMMISSION | IT Infrastructure Review of Security Features | Provided reviews and appropriate tests of security features, practices, and policies for the hardware and software that make up AbilityOne's IT infrastructure. Analyzed and evaluated data for conformance to all standards. After examination and analysis, our team delivered final presentations and FISMA reports. |
| 2 | **U.S. Department of Agriculture**<br>*Security Operations Center* | USDA | Penetration Tests | Penetration tests that include probing each host's Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports using a port scanner and determined network services are being provided by each host, and by scanning each host's available network services for known, remotely exploitable vulnerabilities. |
| 3 | **U.S. Department of Agriculture**<br>*National Institute of Food & Agriculture* | NIFA | IT Security Assessments | Performed security assessments including perimeter security, network security, web security, host security, policy, procedures, and training including user awareness training. Security Operations Center standard operating procedures. |
| 4 | **U.S. Department of Agriculture**<br>*Security Operations Center* | USDA | Wireless Penetration Testing | Conducted internal/external, wireless penetration testing at 18 USDA agencies across the country. Tests included: passive/ active reconnaissance, running exploits, spoofing, password cracking, misconfiguration, data *insertion*, router/ device exploitation. |

| | | | | |
|---|---|---|---|---|
| 5 | **Department of the Treasury**<br>*Office of the Inspector General (OIG)* | | Systems Security Services | Conducted a comprehensive cybersecurity assessment, document findings in a POA&M, and assisted with implementation of Government approved mitigations that would further bolster OIG's cyber hygiene in accordance with Treasury policies, NIST, CNSSI and RMF. |
| 6 | **Department of the Interior**<br>*Interior Business Center* | | Cybersecurity Testing, Forensics and Penetration Testing | Supported six civilian agencies under this contract. Technical Testing and Penetration Testing, Forensics, Insider Threat Assessment, Security Policy, Plans and Documentation Development, and Testing, RMP Development and Integration and A&A Services. |

## Local Government Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | **Detroit Wayne Integrated Health Network (DWIHN)** | | Security Audits and Computer Risk Assessment | Provided vCISO services to manage existing and continuing security audits, as well as to complete and deliver a full Risk Assessment and risk assessment report. Provided in-depth review of current information security posture. Results included recommendations and changes to secure network, full risk assessment to become fully compliant with all system requirements. |
| 2 | **City of Grand Rapids** | | IT Support and Vulnerability Testing | GSG provides two categories of services for IT support, CISO as a Service (CISOaaS) and Penetration and Vulnerability Testing. |
| 3 | **City of Inkster** | | Laserfiche Implementation and Support Services | GSG provides Laserfiche Implementation, Support, licenses, and maintenance services. We are storing all data into the Laserfiche repository and provide forms, reports, and workflow as per the City's requirement. |
| 4 | **City of Farmington Hills** | | Laserfiche – Server and Software Licenses | We provided support and maintenance of the Laserfiche system implementation for the City of Farmington Hills, including Workflows, Forms, and other modules, as well as the Premium Laserfiche Software Assurance Plan (LSAP). |
| 5 | **City of Southfield** | | Laserfiche Professional Services | Our team converted physical HR forms into electronic forms using the Laserfiche Forms System, including multilevel review and approved workflow. |

| | | | |
|---|---|---|---|
| 6 | **City of Livonia** | Document Management Services | GSG provides Laserfiche Document Management Services to various departments within City of Livonia like Clerk, Police, Building, Permit, Housing, IT, HR, etc. All departments are storing information in Laserfiche for faster retrieval and sharing. |
| 7 | **Washtenaw County** | Maps and Plans Scanning Services | Provided scanning and indexing services for maps and drawings for electronic storage. Organized, indexed the documents on the hard drive for import into On-Base. |
| 8 | **County of Ottawa** | Microfilm Document Scanning and Conversion | Provided digitizing services for 16mm microfilm cartridges containing public and confidential court records. Provided with scanning, indexing, and conversion of microfilm (16mm) cartridges of court files. |
| 9 | **City of Dexter** | Document Scanning | Provided document digitalization. Provided services which included transport, preparation, scanning, indexing, and OCR were provided for all the records. |
| 10 | **Macomb Township, Michigan Fire Department** | Large Format Plan Scanning | Provided large format plan scanning services. Digitized large plans, color documents with 300 DPI, OCR, indexing, folder structure, file naming services, and given them in PDF and Tiff image format. |
| 11 | **City of Chicago Department of Assets Information and Services** | Assessment of the City's IT Network Architecture | Teamed with Google \| Mandiant to review and perform assessment of the City's IT network architecture including Network Services – Active Security Assessment and Network Architecture Review. |
| 12 | **Boston Public Health Commission** | Cybersecurity Vulnerability Assessment | Cybersecurity vulnerability network assessment of the BPHC's network which included penetration testing, internal/external perimeter testing, User Privilege Escalation, Segmentation Testing, Wireless Scanning, Applications, Database Assessment, Brute Force Attack, Social Engineering, Phishing/spear phishing Attacks, Employee Impersonation, and Pretexting. |

| | | | | |
|---|---|---|---|---|
| 13 | **Maricopa County** | | Cybersecurity Penetration Testing Services | Cybersecurity penetration testing services. Deliverables included: executive-level reports, assessment methodologies, identified vulnerabilities, recommendations for corrective action, and formal responses to system developer/vendor. Assessment covered workstations, laptops, tablets, and mobile computer devices, servers, data centers, web applications, wireless networks. |
| 14 | **Connect for Health Colorado** | | IT And Security Consulting and Services | IT and security consulting and services to augment C4HCO's existing staff. Provides a Chief Information Security Officer (CISO), cybersecurity analysis/consulting, network security engineering, penetration testing, cloud security support, forensic analysis, blue/red team exercises, and other requirements on a call order basis. |
| 15 | **City of San Jose** | | Advanced Cybersecurity Services | Provided as-needed supplemental advanced cybersecurity services to improve the City's security profile. |
| 15 | **City of New Orleans** | | Cybersecurity Services and Enterprise Services | Provided Cybersecurity Services and enterprise services including multiple, specific technology and cybersecurity products that are core components of the City's enterprise information infrastructure. Services included: Penetration Testing, Endpoint/Network Detection and Response, Email Security, and Multifactor authentication. |
| 17 | **City of Sunnyvale** | | Information Security Monitoring | Services for planning, implementing, and monitoring information security including: security audits, risk assessments, project management, implementation of security tools like intrusion detection, anti-virus, malware protection, and other tools. Services include VCISO, Security Information and Event Management and SOC. |
| 18 | **Housing Authority of the Birmingham District** | | Information Security and Internal/External Network Testing | Provided information security and computer equipment, including tests of the internal network, external network, wireless network, physical access controls, remote access external partners, social engineering vulnerability, internet usage, and host-based security. |

## Commercial Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | Call Tower, Inc. | calltower<br>Stay Connected. Stay Ahead. | Threat Modeling, Vulnerability Assessments | Provided threat modeling, vulnerability assessments, and network and web application penetration testing for CallTower. This assessment was conducted to validate those reasonable controls were in place to comply with industry best practices and to confirm that access to CallTower's IT environment does not compromise system confidentiality, integrity, or availability of other resources |
| 2 | ULB LLC | ULB<br>UNIVERSAL LOAD BANKS | Laserfiche ECM | GSG helped develop and implement a bi-directional integration of Laserfiche with Quick Books (Accounting Software). Which made our tasks of finding vendor invoices easier from Laserfiche and saving statements/documents that are generated into Laserfiche. |

## Educational Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | **Grand Valley State University** | GRAND VALLEY STATE UNIVERSITY | Penetration Testing | GSG recently awarded a contract to provide penetration testing, including pen testing for PCI DSS v4.0 compliance. |
| 2 | **Univ. of Michigan School of Medicine**<br>*University of Michigan Hospitals* | MICHIGAN MEDICINE<br>UNIVERSITY OF MICHIGAN | Security Information and Event Management (SIEM) | Provided leadership for a Security Information and Event Management (SIEM) project. GSG identified, evaluated, and recommended a solution that could be implemented across the University of Michigan Campus computer system. |
| 3 | **Oakland County Academy of Media and Technology** | OCA | Site Assessment and Managed Services | Provided IT Managed Services, including server and other related IT infrastructure such as firewalls, routers, switches, network cable installation, and various other support services 24/7. |
| 4 | **Grand Rapids Community College** | GRCC<br>GRAND RAPIDS COMMUNITY COLLEGE | Microfiche Conversion | GSG digitized approximately 55,000 microfiche jackets containing student records. We provided transportation, microfiche scanning, and indexing at the jacket level and field level. Additionally, our team performed post-scanning services and ensured the quick access to digitized documents. |
| 5 | **Montana State University** | MSU | Upgrade IT Infrastructure | Consulting services to upgrade outdated IT infrastructure. Supported the implementation of a Cisco HyperFlex system with Cisco 10-Gig Ethernet switches and 4-node cluster sizes which was then integrated into the existing environments utilizing Cisco UCS Management. |

| | | | | |
|---|---|---|---|---|
| 6 | **Johnson County Community College** | | Information Security System Audit | Provided information security and incident management professional auditor services. Report included plan for improving the Information Security Incident Management processes, recommendations for areas of improvement, defined objectives, overall security prioritizations. |
| 7 | **Prince George's Community College** | | IT Security Assessment and IT Security Services | Consultant for a variety IT Security Assessment and IT Security Services which include vCISO, vSOC, for IT Security Assessment and IT Security Services, Data Breach Analysis and Remediation, IT Security Planning, Network Infrastructure Design and Penetration Testing. |
| 8 | **Medical College of Wisconsin** | | IT Infrastructure Analysis and Updates | Provided IT infrastructure engineering personnel to assess the College's IT network and to roadmap future improvements. Our team implemented an Endpoint Detection and Response system. |
| 9 | **Maryland State Department of Education** | | Security Specialist Support | Providing Security Specialist Support to perform the following duties: Support the control assessment, reporting, and monitoring processes. Assist updating the Business Continuity and Contingency Plan, evaluate current security posture, and recommend remediation. |
| 10 | **Lone Star College** | | IT Security Assessment Services | Provided IT security assessment services for Email Security, Firewall Audits/Scans, Network Security Assessment (Internal and External), Telephone Vulnerability Assessment, Penetration Testing, |

## Utility Cybersecurity Contracts

| | | | | |
|---|---|---|---|---|
| 1 | **Golden Gate Bridge Highway and Transportation District** | | Cybersecurity Professional and Security Services | Aligned business and cybersecurity IT objectives, developed IT strategy and identified current/future states, created the overall solution to improve the current environment with state-of-the-art plans for designs, integration plans, prepared implementation plans with insight into integration/ configuration/testing. |
| 2 | **State of New Mexico Human Services Department** | | Cybersecurity Services | Developing a System Security Plan (SSP), Information System Risk Assessment (ISRA), POA&M, and other federally mandated security documents for Federal Agency compliance. Provided security analysis, information systems audit, software management. Assessed current security artifacts for completeness; identified deficiencies and recommend improvements. |
| 3 | **National Cooperative Purchasing Alliance** | | Cybersecurity Consulting | Provided cybersecurity solutions, malware, ransomware protection, other related products and services for Region 14 Education Services Center (ESC) and all NCPA participating entities. |

| | | | | |
|---|---|---|---|---|
| 4 | **Lansing Board of Water and Light** | LANSING BWL<br>Hometown People. Hometown Power. | Digital Forensic Examinations | Provided digital forensic examinations to identify any undetected compromising indicators. Provided remediation for detected malware. Tested and made recommendations for weaknesses. |
| 5 | **Regional Water Resource Agency** | RWRA | Created Comprehensive Review of the Current IT Operating Environment | Created the Cyber Resilience Program (CRP), a comprehensive review of the current IT operating environment, to improve overall technology security posture. Analyzed, reviewed, assessed, and created cyber security recommendations. Performed an exploration, detailed mapping, and risk-assessment of networked Operational Technology (OT) systems including SCADA Controls, Telemetry, RWRA-managed networking devices and ancillary connections. |

## b) *Administrative Component* *[RFP 4.c]*

### Understanding of Work Required

GSG understands that the Authority is seeking a qualified contractor who can offer cybersecurity assessment services as well as information technology management services to the Authority or participating Public Agencies, or both.

***For detailed technical approach please refer to section "Tab 2. Technical Approach to Scope of Services".***

### Detailed Expenditure

Our proposed billing rate includes pay and benefit towards holiday, vacation, and various health insurance to attract and retain skilled and experienced talent. However, our proposed cost doesn't include any onsite travel-related cost, software license, hardware, equipment, network device or any other item that is specifically required for this project and it will be an additional cost as an actual cost.

## c) *Technical Component* *[RFP 4.d]*

### 3.c.1 GSG Sole Point of Contact and Other Personnel [RFP 4.d.1]

Our team will be overseen by our **Project Manager, Ms. Vicki Shah**, who has over 15 years managing complex IT and cybersecurity projects for both the public and private sector. Ms. Shah will be the sole point of contact while the assessment is ongoing.

The Project Manager manages and supervises personnel involved in all aspects of the project activity, including organizing and assigning responsibilities to subordinates and overseeing the successful completion of all assigned tasks.

Ms. Shah will generate and update technical and financial reports. She will also perform the day-to-day management of overall contract support operations. She has managed contracts wherein GSG's staff have performed over 300 penetration tests, vulnerability assessments, and web application assessments.

Summary of Key Project Resources

| | Name | Position | Yrs. Exp | Partial Certification Summary |
|---|---|---|---|---|
| **Project Team** | **Vicki Shah, PMP**<br>*(Sole Point of Contact)* | Project Manager | 15+ | PMP |
| | **Vatsal Shah** | Cybersecurity Technical Lead/Assessor/Tester | 20+ | PCIP, CCSK, CISA, CEH, TL, CISSP, CISSP-ISSAP, GWAPT, OP |
| | **Kumar Setty** | Cybersecurity Assessor | 15+ | CISSP, CISA, CCSK, ITIL, PCIP, AWS, HCISSP |
| | **Rubin Mehta** | Incident Response Analyst | 10+ | CEH, CCNA, CCSP, Security+, CSE, ESM/SIM |
| | **Vishal Dave** | Sr. Network and System Administrator | 23+ | CCNA, MCP, MCAF, MAA |

GSG maintains a pool of extraordinary cybersecurity professionals. The quality of our team is peerless, having executed various programs of similar scope and complexity. **Each of our proposed personnel has 10+ years of experience in providing cybersecurity and related services.**

**GSG requires one or more of the following certifications or their equivalent for personnel implementing cybersecurity services**
*(not including account/project management and sales personnel)*

| | | | |
|---|---|---|---|
| CAP | Certified Authorization Professional | PFI | PCI Forensic Investigators |
| CCIP | Certified Core Impact Professional | ISSAP | Infor. Systems Security Arch. Professional |
| CCSK | Certificate of Cloud Security Knowledge | GSEC | GIAC Security Essentials |
| CGEIT | Certified in Governance of Enterprise IT | GCIH | GIAC Certified Incident Handler |
| CHSE | Certified HIPAA Security Expert | GPEN | GIAC Penetration Tester |
| CISA | Certified Information Systems Auditor | GCIA | GIAC Certified Intrusion Analyst |
| CISM | Certified Information Security Manager | GWAPT | GIAC Web App Penetration Tester |
| CEH | Certified Ethical Hacker | GCFE | GIAC Certified Forensic Examiner |
| CISSP | Certified Information Systems Security Professional | GCFA | GIAC Certified Forensic Analyst |
| | | SANS 508 | Advanced Forensics |
| CRISC | Certified in Risk and Information Systems Control | SANS 572 | Advanced Network Forensics |
| CSX | Cybersecurity Nexus | | |
| CSX–P | CSX Cybersecurity Practitioner Certification | | |
| PCIP | Payment Card Industry Professional | | |

GSG's cybersecurity personnels have successfully completed **more than 1,000+ projects** over the past **10 years.**

*The following table summarizes our experience.*

| Cybersecurity Projects | *Projects 2013-2023*<br>Federal | <br>State/Local | *Partial Customer List* |
|---|---|---|---|
| Penetration Testing | ★ | ★ | - Department of Agriculture<br>- AbilityOne Commission<br>- Department of Treasury<br>- Department of Interior<br>- State of Kansas<br>- Jacksonville Aviation Authority<br>- Ft Wayne–Allen County Airport Auth.<br>- San Diego County Regional Airport Authority |
| Assessments | ★ | ★ | |
| Vulnerability Assessments | ★ | ★ | |
| Web Application Security Assessments | ★ | ★ | |
| Cybersecurity Audits | ★ | ★ | |
| Risk Assessments | ★ | ★ | |

| IT and Cybersecurity Technology Projects | *Projects 2013-2023*<br>Federal | <br>State/Local | *Partial Customer List* |
|---|---|---|---|
| HPE | | ★ | - U.S. Department of Interior<br>- U.S. Department of Energy Office of the Inspector General<br>- U.S. Defense Logistics Agency<br>- State of New Mexico Human Services Department<br>- Mercedes Benz Financial<br>- City of San Jose, California<br>- City of New Orleans<br>- City of Sunnyvale<br>- Michigan Economic Development Corporation |
| Micro Focus | ★ | ★ | |
| Splunk | | ★ | |
| IBM | | ★ | |
| Palo Alto | | ★ | |
| Fortinet | | ★ | |
| Cisco | ★ | | |
| AWS | ★ | | |
| Azure | ★ | | |

| | *Projects 2013-2023* | *Partial Customer List* |
|---|---|---|

| Cybersecurity Framework and Controls Projects | Federal | State/Local |
|---|---|---|
| NIST Cybersecurity Framework | ★ | ★ |
| Federal Risk and Authorization Management Program | ★ | ★ |
| Payment Card Industry Data Security Standard (PCI–DSS) | ★ | ★ |
| Open Web Application Security Project (OWASP) | ★ | ★ |
| Center for Internet Security Critical Security Controls for Effective Cyber Defense | ★ | ★ |

- U.S. Department of Agriculture
- U.S. Department of Treasury
- U.S. AbilityOne Commission
- Jacksonville Aviation Authority
- Golden Gate Bridge and Highway District
- Port Authority of Allegheny
- Johnson County Community College
- Prince George's Community College

**This section highlights our team's work experience, credentials, and demonstrates the relevance to the Authority's cybersecurity requirements.**

| *Name* | *Position* | *Yrs. Exp* | *Partial Certification Summary* |
|---|---|---|---|
| **Vicki Shah, PMP** | Project Manager | 15+ | PMP |

- 15+ years on Global Solutions Group's Contract and Project Manager for large IT programs, including those for city, state, local, and federal government agencies.
- **PMP certified.**
- Recently completed working as Contract and Project Manager for our contract for Federal Information Security Management Act of 2014 (FISMA) Analysis Services for the U.S. AbilityOne Commission.
- Managed a multiyear, $10 million U.S. Department of Agriculture Operational Security Assessment Program BPA contract.
- PMI, procurement/contract management, process improvement, and stakeholder management and collaboration.
- Coordinated and overseen our multiple engagements for the State of Kansas, including our contract for providing CISO support personnel.

| | | | |
|---|---|---|---|
| **Vatsal Shah** | Cybersecurity Technical Lead/ Assessor/Tester | 20+ | PCIP, CCSK, CISA, CEH, TL, CISSP, CISSP-ISSAP, GWAPT, OP |

- Specialty skills involve vulnerability assessment, penetration testing, internal and external assessment, auditing, incident response management, with focus on secure network architecture, 802.11x (Wi-Fi), web application portals, SCADA, Process Control Networks (PCNS), Programmable Logic Controllers (PLCs), physical security, database, application security, and regulatory compliance.
- Technical skills in network technologies, operating system platforms, and IT infrastructure security controls. He has tested Industrial Control Systems (ICS) including Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS) for the Lansing Board of Water and Light.

- Performed over 100 web application assessments and Red Team network penetration tests for government, private sector, and non-profit organizations. He has also designed and analyzed secure network architecture including Virtual Private Networks (VPNs), cryptographic systems, firewalls and access control mechanisms, identity management, 802.11x enterprise wireless, and multiple-tier web application and e-commerce architectures.
- Performed penetration testing on all new enterprise applications being deployed into the environment and existing applications that have gone through a significant upgrade for Lansing Board of Water and Light.

| | | | |
|---|---|---|---|
| **Kumar Setty** | Cybersecurity Assessor | 15+ | CISSP, CISA, CCSK, ITIL, PCIP, AWS, HCISSP |

- 15+ years of experience in providing penetration testing in multiple sectors including university, healthcare, finance, and technology sectors.
- MS Software Engineering. Certifications: CISSP, CISA, CCSK, ITIL v3, PCIP, AWS, HCISPP.
- Developing and implementing security, privacy, and breach management programs with expertise in vulnerability assessment and penetration testing. In-depth knowledge of security assessments of databases, EHR/EMR, SAP, Oracle Financials, and other ERPs.
- Eight years of experience in performing security and privacy risk assessments and audits. Well-versed in HITRUST SOC 1/2/3, FFIEC, NIST, COBIT, HIPAA, PCI-DSS, SEI-CMM methodology, IT QA methods, and ISO security standards with vast understanding of threat modeling using frameworks such as Octave Allegro and MITRE ATT&CK.

| | | | |
|---|---|---|---|
| **Rubin Mehta** | Incident Response Analyst | 10+ | CEH, CCNA, CCSP, Security+, CSE, ESM/SIM |

- 10+ years of experience in experience in network security, data networking, and information technology.
- MS, Engineering in Computer Networks. Certifications: CEH, CCNA, CCSP, CSE ESM/SIM, CISSP in progress.
- Arc Sight: Advanced Integrator/Administrator, ESM/SIM.
- Knowledge in security architecture, engineering, operations, and managed security services.
- Currently serving as cybersecurity SME performing security assessments on of web servers and applications, in addition to penetration testing in accordance with federal regulations and industry best practices.

| | | | |
|---|---|---|---|
| **Vishal Dave** | Sr. Network and System Administrator | 23+ | CCNA, MCP, MCAF, MAA |

- 23+ years of experience involving Network Administration with multiple organizations.

- Bachelors in computer application, Certifications/Training: CCNA, MCP, MCAF, MAA, Training Hardware, and Network Engineer.
- Experienced with configure SonicWALL firewall, Cisco Switch, Vonage, Routers, FortiGate Firewall, Network processing, centralized and distributive network connection, Installing, configuring, and administering network technologies, IIS, SSL, Web Hosting, SQL, My SQL, PHP Website Configuration, Ample knowledge in Windows 98\ Me\XP \2000\2008\2010\2003 Server\2008 Server\2016 Server\2019 Server.
- Active directory management, NTFS security, disk quota management, Diagnostic and trouble-shoot various problems in PCs, network, servers, routers, switches.
- Networking, LAN, and WAN trouble shooting. Network Auditing, Knowledge of configuration and maintenance, Routing, Microsoft AD Configuration, Computer assembling and maintenance.
- Troubleshooting hardware and software problems, Installing, and configuring the peripherals, components, and drivers.
- Installing software and application to user standards.

### 3.c.2 Adequacy of Personnel to Handle Communications with the Authority or Public Agency [RFP 4.d.2]

Communication is an essential component of a Project's success. GSG focuses upon formal and informal communications between our Project Manager and Authority representatives. Regular customer communication (both scheduled and spontaneous) is a critical project management element in our management approach, since establishing an atmosphere of cooperation, coupled with communication structure, is crucial to resolving potential unanticipated challenges.

Our specific activities associated with communications include regular meetings, conference calls, and progress reports. Open and effective communication is the cornerstone of project management methodology and our corporate culture. We will collaborate with Authority to discuss and formulate the methods and protocols to be used, define the appropriate roles and responsibilities, and establish communication channels. Key communications include a review of the work plan, key dependencies, project risks, action items, and next steps and well as ongoing status reports.

### 3.c.3 Level of Assistance Expected from Authority or Public Agency [RFP 4.d.3]

To perform effective audits and assessments, our team will require additional information from the Client regarding their current security posture as well as cooperation/coordination with our team.

The following are requirements we need from all clients to enable us to execute contracts effectively and efficiently:

1) A minimum of one IT department member with authorization to provide access to our analysts
2) Access to individuals for interviews and social engineering efforts
3) Details of previous assessments and/or audits
4) Any logs regarding security incidents, related event documentation, or problematic issues that have arisen within the organization within the last thirty to sixty days. This should also include any collected traffic information such as documented application performance issues, timeout errors, routing issues or network related issues

5) Allow logical access to the systems, network or computer equipment, which are necessary to perform the evaluations, and protect all assets that may be affected by this service

6) Inventory of network equipment

    a) Desktops/Workstations/Laptops

    b) Routers/Switches

    c) Peripheral Devices (printers, scanners, etc.)

    d) Including wireless

    e) Including mobile devices (smart phones, tablets)

7) List of operating systems in use (Linux, Windows, etc.)

8) Lists of third-party vendors/software

9) All internal and external IP addresses

10) Copy of existing IT Policies and Procedures

11) Copy of existing Business Continuity Plan

12) Assign staff to be the primary and/or secondary point of contact for the Contractor

13) Provide contact lists for both office and non-office hours whenever necessary

14) Timely review and comment within two business days on all interim, draft, and final deliverables, unless mutually agreed upon, based upon the size of deliverable, for a different timeline

15) Provide responses to GSG enquiries within a reasonable time span

16) Timely response to/implementation of remediation recommendations, especially those determined critical

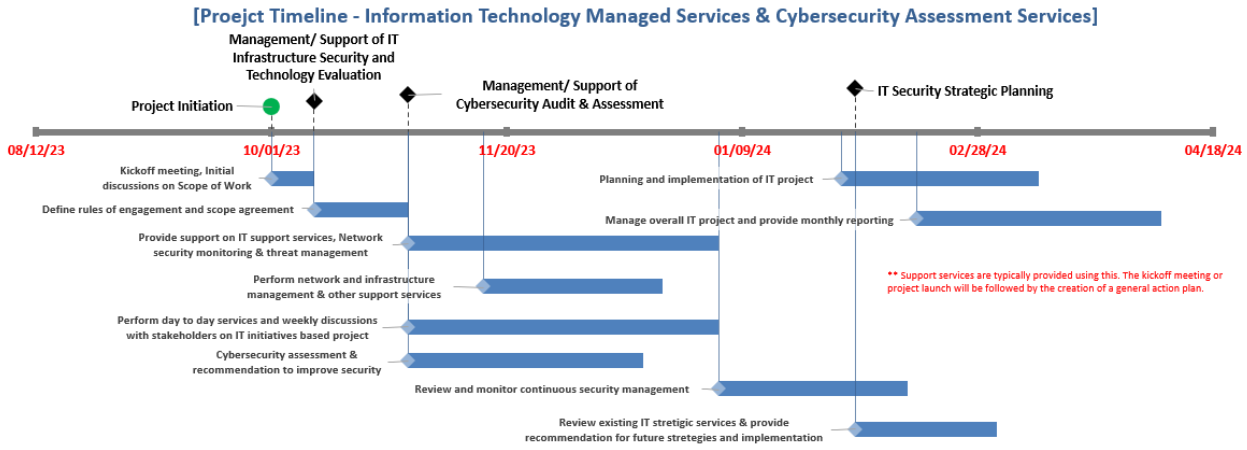
## 3.c.4 Work Plan and Schedule [RFP 4.d.4]

*A sample project work plan for completing scope requirements is provided below:*

**Project Tentative Work Plan Schedule [October 1, 2023, to September 30, 2024]**

| Sr. No. | Task description | Target plan to start project |
|---|---|---|
| **Project Initiation** | | |
| 1 | Kickoff meeting, Initial discussions on Scope of Work | 1 Week after getting the project |
| 2 | Define rules of engagement and scope agreement | 2-4 Weeks |
| **Management/Support of IT Infrastructure Security and Technology Evaluation** | | |
| 3 | Provide support on IT support services, Network security monitoring and threat management | 12-15 weeks |
| 4 | Perform network management, Monthly preventive maintenance etc. [AD-HOC services] | 3-5 weeks |
| 5 | Perform day to day services and weekly discussions with stakeholders on IT initiatives-based project | 3-15 weeks |
| **Management/Support of Cybersecurity Audit and Assessment** | | |
| 6 | Cybersecurity assessment and recommendation to improve security | 5-7 weeks |
| 7 | Review and monitor continuous security management | 4-5 weeks |
| **IT Security Strategic Planning** | | |
| 8 | Review existing IT strategic services and provide recommendation for future strategies and implementation | 3-4 weeks |
| 9 | Planning and implementation of IT project | 4-7 weeks |
| 10 | Manage overall IT project and provide monthly reporting | 3-7 weeks |

The following demonstrates sample schedule for completing scope requirements:



** Support services are typically provided using this. The kickoff meeting or project launch will be followed by the creation of a general action plan.

### 3.c.5 Past Performance [RFP 4.d.5]

The following are the three (3) references for contracts on which GSG has performed similar work:

| Reference | Work Performed | Customer |
|---|---|---|
| Reference ❶ | **Operational Security Assessments, Penetration Testing and Web Security Assessments** | U.S. Department of Agriculture |
| Reference ❷ | **IT Security Support Services** | State of Kansas Office of Information Technology Services |
| Reference ❸ | **Network Penetration Testing** | Jacksonville Aviation Authority |

**Reference #1 Operational Security Assessments, Penetration Testing, and Web Security Assessments**

| | |
|---|---|
| **Organization** | **U.S. Department of Agriculture** |
| **Contact** | Stacey Marshall<br>Contracting Officer's Representative<br>USDA Office of the Chief Information Officer<br>stacey.marshall@usda.gov<br>(816) 823-2752 |

***Description of Services Provided***

GSG conducted Operational Risk Assessments, Penetration Testing, Web Security Assessments with High Value Applications (HVA), and Red Team Assessments for all USDA offices and data centers nationwide. Provided extended assessments for the Office of the Chief Financial Officer and National Finance Center (USDA–NFC), which processes payroll for over 600,000 federal government employees. Our team also performed NIST CSF, NIST SP 800 series, and FISMA/FedRAMP based Vulnerability Assessments and Penetration Testing. GSG's assessments supported agency-level cybersecurity leaders in determining overall risk and provided recommendations for resolution or mitigation.

GSG has provided work for the following USDA offices/agencies:

- Agricultural Marketing Service
- Agricultural Research Service
- Agriculture Security Operations Center/OCIO
- Animal and Plant Health Inspection Service
- Client Technology Services/OCIO
- Conservation Service
- Economic Research Service
- Farm Service Agency
- Food and Nutrition Service
- Food Safety and Inspection Service
- Grain Inspection, Packers, and Stockyards Administration
- National Agricultural Statistics Service
- National Finance Center/OCFO
- National Information Technology Center/OCIO
- National Institute of Food and Agriculture
- Natural Resources
- Office of the Chief Economist
- Risk Management Agency

- Foreign Agricultural Service
- Forest Service

Rural Development

In conducting the security assessments, GSG evaluated the following layers of security and their sub-layers:

| | |
|---|---|
| Perimeter Security | Perimeter Router, Perimeter Firewall, VPN Gateway, Perimeter Intrusion Detection System (IDS) |
| Network Security | Infrastructure Switch, Infrastructure Intrusion Detection System (IDS)/Intrusion Prevention System (IPS), Network Vulnerability Scanning, Mail Guards, Network Access Control |
| Web Security | Web Server Security Configuration, Web Applications Security Configuration, Identification and Authentication, Roles and Permission Sets (inherited and non-inherited), Host Security (based on type of O/S used) |
| Unix/Linux Host Security | Host Vulnerability Scanning, Security Configuration, Data Encryption, Patch Management, File Integrity, Antivirus Protection, Host Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) Protection, Host Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) |
| Windows Host Security | Host Vulnerability Scanning, Security Configuration, Data Encryption, Patch Management, File Integrity, Antivirus |
| Policy, Procedures, and Training | User Awareness Training, Privileged User Awareness Training, Configuration and Change Management, Network Operations Center (NOC) Standard Operating Procedures (SOPs), Security Operations Center (SOC) Standard Operating Procedures (SOPs), Computer Incident Response Team (CIRT) Standard Operating Procedures (SOPs) |
| Multi-Layer Solutions | Network Management Systems, Data Loss Prevention, Security Information and Event Management |
| Incident Response | Identification; Investigation; Remediation |
| Penetration Testing | Open-Source Data Collection; Host Discovery and Port Scanning; Host Exploration; Web Server and Application(s) Discovery; Web Server and Application(s) Exploration; Social Engineering |
| Forensics | Extent of Compromise |

## Reference #2 IT Security Support Services

| | |
|---|---|
| **Organization** | **State of Kansas Office of Information Technology Services** |
| **Contact** | Mr. Nathaniel Kunst, ISO At-Large<br>Nathaniel.Kunst@ks.gov<br>(321) 517-8729 |

***Description of Services Provided***

GSG provides IT Security Support Services as needed to all departments in the State of Kansas government on a task-order basis. Services include, but are not limited to:

a) Security planning, design, and review:
   i) Developing security organizational plans.
   ii) Determining appropriate staffing levels.
   iii) Designing security architectures, including perimeter defense, secure remote access, authentication, VoIP, intrusion detection, and physical security of networks and systems.
   iv) Developing security standards, policy, and procedures.
   v) Developing business continuity and disaster recovery plans.

b) Risk and Security Assessments, penetration, and vulnerability testing:
   i) Networks, (firewalls, routers, remote access, authentication servers).
   ii) Wireless networks.
   iii) Servers (web, email, application, file, and print on all operating systems).
   iv) Security management applications (antivirus, patch management, and desktop security).
   v) Code audit.
   vi) Applications:
      - Security Configuration
      - Patch Management
   vii) Physical network environment.
   viii) Compliance tracking and reporting.
   ix) Social engineering.
   x) Physical Security.

c) Implementation Services for Technical Security Controls:
   i) This includes installation, configuration, and maintenance in the following categories of security technical controls:
      - Network security devices (firewalls, routers, intrusion prevention, load balancers, etc.).
      - Security applications (user and entity behavior analytics, logging, security information and event management, advanced email filtering, etc.).

d) Incident Response:
   i) Emergency Response.
   ii) Crises management planning.
   iii) Incident scoping.
   iv) In-depth analysis including forensic analysis, network traffic analysis, log analysis, and malware analysis.
   v) Damage assessment.
   vi) Remediation, containment, and remediation strategy.

## Reference #3 Network Penetration Testing

| | |
|---|---|
| **Organization** | **Jacksonville Aviation Authority (JAA)** |
| **Contact** | David Johnson, IT Infrastructure Manager<br>david.johnson@flyjacksonville.com<br>(904) 741-3591 |

***Description of Services Provided***

This project consists of external and internal penetration testing of JAA's network with the goal of obtaining access to protected data in four categories: Access Control, Law Enforcement and Criminal Justice Information System Compliance, PCI Compliance, and General Security. Testing was conducted at the four airports under JAA's control:

- Jacksonville International Airport
- Jacksonville Executive at Craig Airport
- Herlong Recreational Airport
- Cecil Airport

Testing consisted of twenty-five secure VLANs containing sensitive systems and data and ninety-five general purpose/non-security sensitive VLANS. All testing was informed by the Federal Aviation Administration (FAA) Cybersecurity Strategy and Transportation Security Administration (TSA) security requirements as well as PCI DSS and CJIS Security Policies.

### 3.c.6 Retention and Disposal of Records [RFP 4.d.6]

GSG has technical policies and procedures in place for authorizing access to electronic protected information to authorized personnel, for example, through access to workstations, transactions, programs, processes, or other mechanisms per Client requirements. Additionally, these technical policies and procedures apply to all personally identifiable information that our personnel may have access to during a work assignment, including information about, concerning, or controlled by our clients.

GSG applies access authorization policies to establish, document, review and modify a user's right of access to a workstation, transaction, program, or process. Access to all confidential information is role-based and limited to the "minimum necessary."

Additionally, all employees are required to sign our corporate non-disclosure agreement (NDA) and any client/contract-specific NDA as required. Employees who have access to any client data systems are required to abide by all client usage policies and procedures, including participating in any required client training programs.

GSG's data retention period is the duration of time that an Client stores various categories of data. Our retention period will depend on the type of data, data retention laws, contractual obligations, and data sensitivity, among other factors.

GSG's best practice for data retention is only to keep data when it's useful. Once the data is no longer useful to the Client objectives, data destruction/ data sanitization will be scheduled.

GSG uses National Institute for Standards and Technology (NIST) created guidelines for data sanitization that applies to all storage devices. The guidelines provide three effective data sanitization methods that protect data from unauthorized access: Clear, purge and destroy.

Clear: In clearing technique GSG use logical methods to sanitize data. Clearing provides a moderate level of data security by overwriting data in storage devices. This can be done by resetting storage devices to factory settings or overwriting with new data.

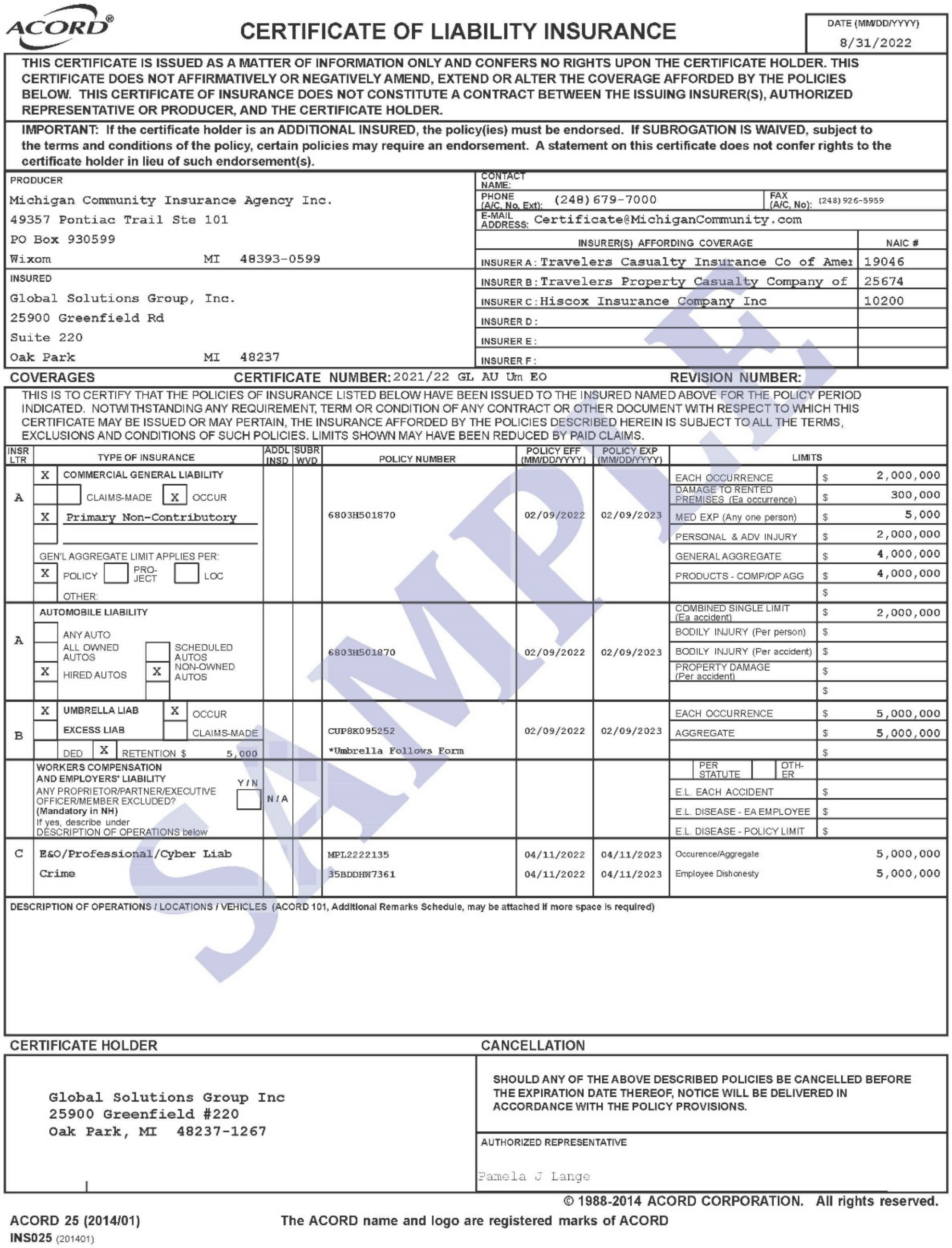
Purge: For purging data we apply physical techniques or technology to render the data unreadable and unrecoverable even within a laboratory environment. Purging data is more effective than clearing and is ideal for handling sensitive data. This method applies techniques such as degaussing and cryptographic shredding to purge large data sets from storage systems.

Destroy: For destruction, GSG involves shredding data and destroying the storage devices as well. This method renders the data unrecoverable and the devices unusable. Techniques used to sanitize data through destruction include incineration, shredding, pulverization, and melting storage devices. Destruction is applied when storage devices are no longer useful and cannot be repaired.

## 3.c.7 Statement of Responder Maintains Comprehensive Liability Insurance and Workers Compensation [RFP 4.d.7]

The following are SAMPLE ACORD files. Upon award, GSG will instruct our insurance carriers to issue ACORDs naming the Client as the Certificate Holder.

### *General and Professional Liability Insurance*



ACORD®

CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 8/31/2022

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

| | | |
|---|---|---|
| PRODUCER<br>Michigan Community Insurance Agency Inc.<br>49357 Pontiac Trail Ste 101<br>PO Box 930599<br>Wixom MI 48393-0599 | CONTACT NAME:<br>PHONE (A/C, No, Ext): (248) 679-7000 FAX (A/C, No): (248) 926-5959<br>E-MAIL ADDRESS: Certificate@MichiganCommunity.com | |
| | INSURER(S) AFFORDING COVERAGE | NAIC # |
| | INSURER A : Travelers Casualty Insurance Co of Amei | 19046 |
| INSURED<br>Global Solutions Group, Inc.<br>25900 Greenfield Rd<br>Suite 220<br>Oak Park MI 48237 | INSURER B : Travelers Property Casualty Company of | 25674 |
| | INSURER C : Hiscox Insurance Company Inc | 10200 |
| | INSURER D : | |
| | INSURER E : | |
| | INSURER F : | |

COVERAGES CERTIFICATE NUMBER: 2021/22 GL AU Um EO REVISION NUMBER:

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

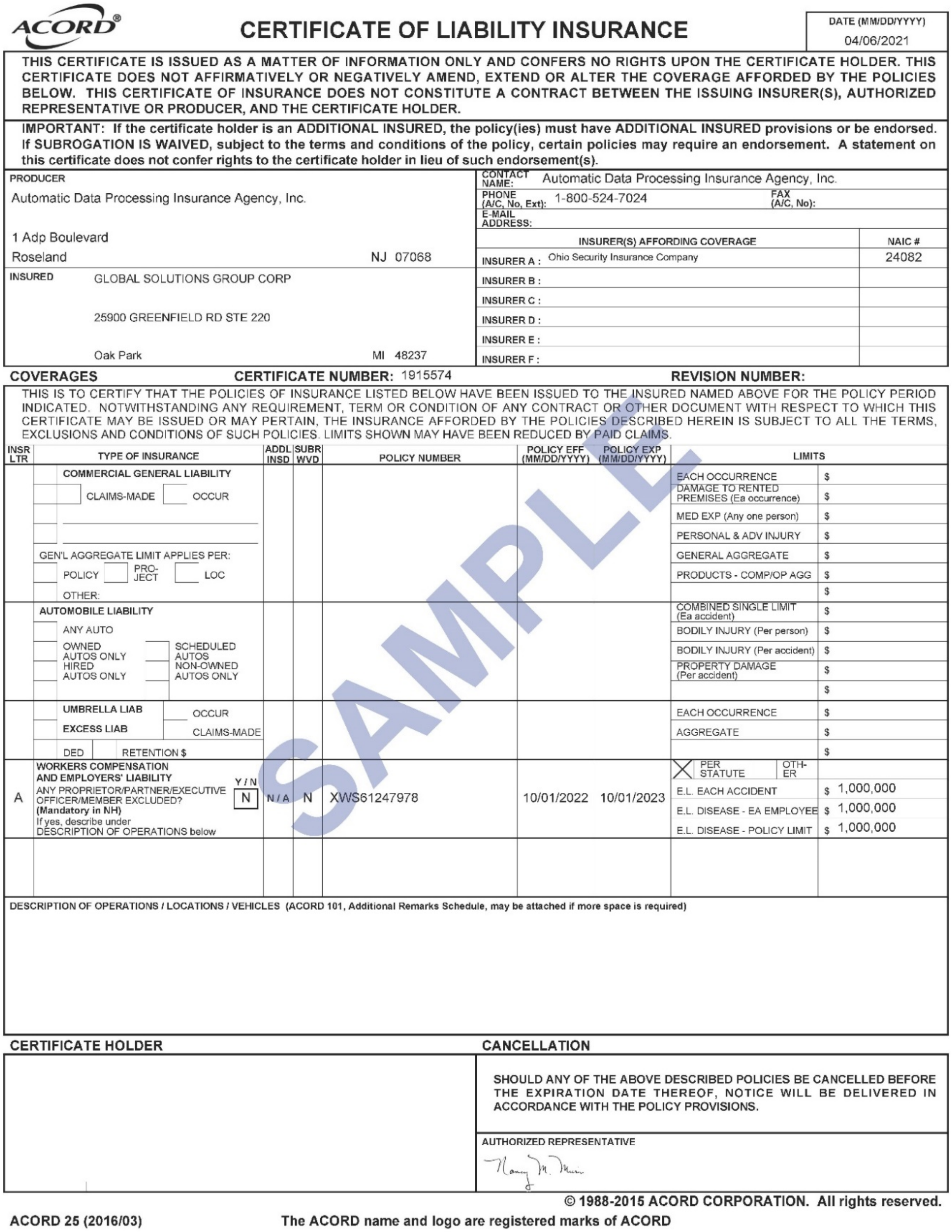
| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| A | ☒ COMMERCIAL GENERAL LIABILITY<br>□ CLAIMS-MADE ☒ OCCUR<br>☒ Primary Non-Contributory<br>GEN'L AGGREGATE LIMIT APPLIES PER:<br>☒ POLICY □ PRO-JECT □ LOC<br>OTHER: | | | 6803H501870 | 02/09/2022 | 02/09/2023 | EACH OCCURRENCE<br>DAMAGE TO RENTED PREMISES (Ea occurrence)<br>MED EXP (Any one person)<br>PERSONAL & ADV INJURY<br>GENERAL AGGREGATE<br>PRODUCTS - COMP/OP AGG | $ 2,000,000<br>$ 300,000<br>$ 5,000<br>$ 2,000,000<br>$ 4,000,000<br>$ 4,000,000<br>$ |
| A | AUTOMOBILE LIABILITY<br>□ ANY AUTO<br>□ ALL OWNED AUTOS □ SCHEDULED AUTOS<br>☒ HIRED AUTOS ☒ NON-OWNED AUTOS | | | 6803H501870 | 02/09/2022 | 02/09/2023 | COMBINED SINGLE LIMIT (Ea accident)<br>BODILY INJURY (Per person)<br>BODILY INJURY (Per accident)<br>PROPERTY DAMAGE (Per accident) | $ 2,000,000<br>$<br>$<br>$<br>$ |
| B | ☒ UMBRELLA LIAB ☒ OCCUR<br>□ EXCESS LIAB □ CLAIMS-MADE<br>□ DED ☒ RETENTION $ 5,000 | | | CUP8K095252<br>*Umbrella Follows Form | 02/09/2022 | 02/09/2023 | EACH OCCURRENCE<br>AGGREGATE | $ 5,000,000<br>$ 5,000,000<br>$ |
| | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y / N<br>ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? □<br>(Mandatory in NH)<br>If yes, describe under DESCRIPTION OF OPERATIONS below | N / A | | | | | □ PER STATUTE □ OTH-ER<br>E.L. EACH ACCIDENT<br>E.L. DISEASE - EA EMPLOYEE<br>E.L. DISEASE - POLICY LIMIT | <br>$<br>$<br>$ |
| C | E&O/Professional/Cyber Liab<br>Crime | | | MPL2222135<br>35BDDHW7361 | 04/11/2022<br>04/11/2022 | 04/11/2023<br>04/11/2023 | Occurence/Aggregate<br>Employee Dishonesty | 5,000,000<br>5,000,000 |

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

| CERTIFICATE HOLDER | CANCELLATION |
|---|---|
| Global Solutions Group Inc<br>25900 Greenfield #220<br>Oak Park, MI 48237-1267 | SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.<br>AUTHORIZED REPRESENTATIVE<br>Pamela J Lange |

ACORD 25 (2014/01)
INS025 (201401)

### *Workers Compensation*



ACORD®

## CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 04/06/2021

**THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.**

**IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).**

| | | |
|---|---|---|
| PRODUCER<br>Automatic Data Processing Insurance Agency, Inc.<br><br>1 Adp Boulevard<br>Roseland NJ 07068 | CONTACT NAME: Automatic Data Processing Insurance Agency, Inc.<br>PHONE (A/C, No, Ext): 1-800-524-7024 FAX (A/C, No):<br>E-MAIL ADDRESS: | |
| | INSURER(S) AFFORDING COVERAGE | NAIC # |
| | INSURER A : Ohio Security Insurance Company | 24082 |
| INSURED GLOBAL SOLUTIONS GROUP CORP<br><br>25900 GREENFIELD RD STE 220<br><br>Oak Park MI 48237 | INSURER B : | |
| | INSURER C : | |
| | INSURER D : | |
| | INSURER E : | |
| | INSURER F : | |

**COVERAGES** **CERTIFICATE NUMBER:** 1915574 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

| INSR LTR | TYPE OF INSURANCE | ADDL INSD | SUBR WVD | POLICY NUMBER | POLICY EFF (MM/DD/YYYY) | POLICY EXP (MM/DD/YYYY) | LIMITS | |
|---|---|---|---|---|---|---|---|---|
| | COMMERCIAL GENERAL LIABILITY | | | | | | EACH OCCURRENCE | $ |
| | □ CLAIMS-MADE □ OCCUR | | | | | | DAMAGE TO RENTED PREMISES (Ea occurrence) | $ |
| | | | | | | | MED EXP (Any one person) | $ |
| | | | | | | | PERSONAL & ADV INJURY | $ |
| | GEN'L AGGREGATE LIMIT APPLIES PER: | | | | | | GENERAL AGGREGATE | $ |
| | □ POLICY □ PRO-JECT □ LOC | | | | | | PRODUCTS - COMP/OP AGG | $ |
| | OTHER: | | | | | | | $ |
| | AUTOMOBILE LIABILITY | | | | | | COMBINED SINGLE LIMIT (Ea accident) | $ |
| | □ ANY AUTO | | | | | | BODILY INJURY (Per person) | $ |
| | □ OWNED AUTOS ONLY □ SCHEDULED AUTOS | | | | | | BODILY INJURY (Per accident) | $ |
| | □ HIRED AUTOS ONLY □ NON-OWNED AUTOS ONLY | | | | | | PROPERTY DAMAGE (Per accident) | $ |
| | | | | | | | | $ |
| | □ UMBRELLA LIAB □ OCCUR | | | | | | EACH OCCURRENCE | $ |
| | □ EXCESS LIAB □ CLAIMS-MADE | | | | | | AGGREGATE | $ |
| | □ DED □ RETENTION $ | | | | | | | $ |
| A | WORKERS COMPENSATION AND EMPLOYERS' LIABILITY Y/N<br>ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? N<br>(Mandatory in NH)<br>If yes, describe under DESCRIPTION OF OPERATIONS below | N/A | N | XWS61247978 | 10/01/2022 | 10/01/2023 | ☒ PER STATUTE □ OTH-ER | |
| | | | | | | | E.L. EACH ACCIDENT | $ 1,000,000 |
| | | | | | | | E.L. DISEASE - EA EMPLOYEE | $ 1,000,000 |
| | | | | | | | E.L. DISEASE - POLICY LIMIT | $ 1,000,000 |
| | | | | | | | | |

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

| CERTIFICATE HOLDER | CANCELLATION |
|---|---|
| | SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.<br><br>AUTHORIZED REPRESENTATIVE |

ACORD 25 (2016/03) The ACORD name and logo are registered marks of ACORD

### 3.c.8 Description of Strategic Relationships [RFP 4.d.8]

We have several strategic partnerships which provide our teams with additional resources, enabling us to provide additional value to our clients.

GSG is a Fortinet Authorized Partner, which enhances our expertise in complete endpoint protection of servers, networks and knowledge of firewalls, switches, security fabric, etc. We are also partnered with Trellix (formerly FireEye and McAfee) providing support for enterprise security and threat intelligence. We have also maintained a partnership with Mandiant (formerly part of FireEye) for providing top-ranked threat intelligence, detection and response support, and Expert-on-Demand services.

GSG is a Micro Focus Business Partner, providing access to the latest software security applications and intelligence through Fortify, as well as other critical tools to build, operate, secure, and analyze the enterprise IT system. We are also part of the Cisco Partner Network, providing us with the latest information in routing, switching, wireless and unified communications technology.

As a member of the IBM PartnerWorld, our team has access to the latest training and knowledge in such areas as Cloud services, security, SIEM, etc. We are also a Microsoft Gold Partner, recognizing our capabilities in providing Microsoft Managed Services as well as Azure Cloud Services, and we are Amazon Web Service (AWS) partners, giving us the ability to support AWS Cloud services. We are a Platinum Certified Value-Added Reseller for Laserfiche, the leading document management and workflow platform.

## Tab 4. Price Quote

The following is our pricing for this requirement.

**NOTE: Due to the formatting requirements of a MS Word Document, we have also provided the pricing as an Excel spreadsheet for clarity.**

| Evaluation of Information Technology Management Services and Cybersecurity Assessment Services | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Milestone Description** | **Number of Devices** | **Monthly Hours** | **Annual Hours** | **Hourly Rate** | **Year 1** | **Year 2** | **Option Year 1** | **Option Year 2** | **Total Cost - 4 Years** |
| Information Technology Management Services | | | | | | | | | |
| **Option A - Small Size Municipal Agency / Department**** | | **50** | **600** | **$75** | **$45,000.00** | **$45,900.00** | **$46,818.00** | **$47,754.36** | **$185,472.36** |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | Up to 25 endpoints / 2 firewalls / 10 network devices | 8 | 96 | | | | | | |
| (B) Proactive monitoring and alerts; | | 10 | 120 | | | | | | |
| (C) On-site and remote support services; | | 15 | 180 | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | 10 | 120 | | | | | | |
| (E) and on-call infrastructure professionals | | 7 | 84 | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Option B - Medium Size Municipal Agency / Department**** | | **100** | **1200** | **$75** | **$90,000.00** | **$91,800.00** | **$93,636.00** | **$95,508.72** | **$370,944.72** |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | Up to 100 endpoints / 3 firewalls / 25 network devices | 16 | 192 | | | | | | |
| (B) Proactive monitoring and alerts; | | 20 | 240 | | | | | | |
| (C) On-site and remote support services; | | 32 | 384 | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | 20 | 240 | | | | | | |
| (E) and on-call infrastructure professionals | | 12 | 144 | | | | | | |
| **Option C - Large Size Municipal Agency / Department**** | | **160** | **1920** | **$75** | **$144,000.00** | **$146,880.00** | **$149,817.60** | **$152,813.95** | **$593,511.55** |
| (A) Management of firewalls, anti-virus, | Up to 250 endpoints / 5 firewalls / 40 | 25 | 300 | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| anti-malware, and threat identification; | network devices | | | | | | | | |
| (B) Proactive monitoring and alerts; | | 24 | 288 | | | | | | |
| (C) On-site and remote support services; | | 45 | 540 | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | 30 | 360 | | | | | | |
| (E) and on-call infrastructure professionals | | 16 | 192 | | | | | | |
| Option D - Extra Large Size Municipal Agency / Department** | | 160 Hours + additional hours as needed | 1920 Hours + additional hours as needed | $75 | As Needed | As Needed | As Needed | As Needed | As Needed |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | Above 250 endpoints / 5 firewalls / 40 network devices | | | | | | | | |
| (B) Proactive monitoring and alerts; | | | | | | | | | |
| (C) On-site and remote | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| support services; | | | | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | | | | | | | | |
| (E) and on-call infrastructure professionals | | | | | | | | | |
| | | | | | | | | | |
| **On-Demand Services***** | | | | | | | | | |
| 1. Consultation (Remote, for onsite - travel charges will be additional) | IT/Network Consulting (Intermediate Level Resource) | - | - | $50 | TBD | TBD | TBD | TBD | TBD |
| | IT/Network Consulting (Senior/SME Level Resource) | - | - | $95 | TBD | TBD | TBD | TBD | TBD |
| 2. Small-scale testing services, as needed, to augment ongoing audits or testing | QA Testing (Intermediate Level Resource) | - | - | $60 | As per scope | As per scope | As per scope | As per scope | As per scope |
| | QA Testing (Senior/SME Level Resource) | - | - | $90 | As per scope | As per scope | As per scope | As per scope | As per scope |
| 3. Ability to use firm during normal business hours | | | | | Yes | Yes | Yes | Yes | Yes |
| Cybersecurity Assessment Services | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Option A - Small Size Municipal Agency / Department**** | | **N/A** | **160** | **$124** | **$19,840.00** | **$20,236.80** | **$20,641.54** | **$21,054.37** | **$81,772.70** |
| (A) Independent view of current information technology security measures; | Up to 200 devices (network and endpoints) | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **Option B - Medium Size Municipal Agency / Department**** | | **N/A** | **240** | **$124** | **$29,760.00** | **$30,355.20** | **$30,962.30** | **$31,581.55** | **$122,659.05** |
| (A) Independent view of current information technology security measures; | Up to 500 devices (network and endpoints) | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **Option C - Large Size Municipal Agency / Department**** | | **N/A** | **480** | **$124** | **$59,520.00** | **$60,710.40** | **$61,924.61** | **$63,163.10** | **$245,318.11** |
| (A) Independent view of current information technology | Up to 1000 devices (network and endpoints) | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| security measures; | | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Option D - Extra Large Size Municipal Agency / Department**** | | **N/A** | **480 Hours + additional hours as needed** | **$124** | **As Needed** | **As Needed** | **As Needed** | **As Needed** | **As Needed** |
| (A) Independent view of current information technology security measures; | Above 1000 devices (network and endpoints) | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information | | | | | | | | | |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **On-Demand Services***** | | | | | | | | | |
| 1. Consultation (Remote, for onsite - travel charges will be additional) | Cybersecurity Consulting (Intermediate Level Resource) | - | - | $85 | TBD | TBD | TBD | TBD | TBD |
| | Cybersecurity Consulting (Senior/SME Level Resource) | - | - | $125 | TBD | TBD | TBD | TBD | TBD |
| 2. Small-scale testing services, as needed, to augment ongoing audits or testing | Cybersecurity Audit (Intermediate Level Resource) | - | - | $90 | As per scope | As per scope | As per scope | As per scope | As per scope |
| | Cybersecurity Audit (Senior/SME Level Resource) | - | - | $124 | As per scope | As per scope | As per scope | As per scope | As per scope |
| 3. Ability to use firm | | | | | Yes | Yes | Yes | Yes | Yes |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| during normal business hours | | | | | | | | | |
| **Optional Cost - Estimated Travel Cost (1 Trip - 3 to 4 days) - If required** | | | | | **TBD** | **TBD** | **TBD** | | **TBD** |
| **Total Cost (Varies based upon selected options)** | | | | | **TBD** | **TBD** | **TBD** | | **TBD** |

**<u>Payment Schedule:</u>**

- IT Management Services - GSG will invoice the appropriate amount monthly.
- Cybersecurity Assessment Services - GSG will accept a 100% services fee invoice upon acceptance of all final deliverables.

**<u>Assumptions:</u>**

** Due to lack of exact assets/network devices information about each Municipal Agency / Department, GSG would like to propose **FOUR Options** for both "Information Technology Management Services" and "Cybersecurity Assessment Services" based upon the size/scope of each Municipal Agency / Department. Each Option for Municipal Agency / Department size included with ceiling limits from numbers of network devices/endpoints. However, if these options are not the best fit then we are open to considering other options as well. Above hours are based upon scope and clarification response provided in RFP and Q&A document. If any of the scope and/or quantities of devices increases, then our effort will be increased appropriately.

**IT Management Services - Hours Break-down**

**Option A -**We have estimated **50 hours** on a monthly basis for a Small agency with specified devices Up to **25 endpoints, 2 firewalls, and 10 network device**s.
**Option B -**We have estimated **100 hours** on a monthly basis for a  Medium agency with specified devices Up to **100 endpoints, 3 firewalls, and 25 network devices.**
**Option C** -We have estimated **160 hours** on a monthly basis for a Large Agency with specified devices Up to  **250 endpoints, 5 firewalls, and 40 network devices.**
**Option D -**We have estimated **160 Hours + additional hours as needed** on a monthly basis for an Extra Large Agency with specified devices  Above **250 endpoints, 5  firewalls, and 40 network devices.**

**Cybersecurity Assessment Services - Hours Break-down**

**Option A -**  We have estimated a one-time effort of **160 hours** for a Small Agency with specified devices Up to a total of **200 devices (network and endpoints)**.
**Option B** -  We have estimated a one-time effort of  **240 hours** for a Medium Agency with specified devices Up to a total of **500 devices (network and endpoints).**
**Option C -**  We have estimated a one-time effort of  **480 hours** for a  Large  Agency with specified devices Up to a total of **1000 devices (network and endpoints).**
**Option D** -  We have estimated a one-time effort of  **480 Hours + additional hours as a needed base** for an Extra Large Agency with specified devices Above **1000 devices (network and endpoints).**

**Note:**

Based upon understanding from RFP and Q&A, GSG proposes an estimated number of hours for different tasks and support categories. Our price will increase prorated if there is an increase in the total number of supported endpoints, servers, network devices, and/or users. If the total number of monthly hours exceeds estimated hours, then it will be charged as an additional cost as per the billable hourly rate.

*** For "On-Demand Services", we are providing hourly rates for "Consultation" OR "Small-scale testing services" on an as-needed basis to augment ongoing audits or testing for Years 1, 2, 3, and 4.  We also agree to provide our resources during normal business hours. All services will be remote. However, if onsite services is required then travel cost will be an additional cost.

As part of our proposed cost for on-site support resources, GSG proposes a local Michigan area resource with as-needed onsite hours monthly. These additional travels to the customer site, however, will incur a comprehensive onsite cost of $150/trip/day/person for any customer within the Detroit Metropolitan Area, and $300/trip/day/person for any customer outside of the Detroit Metropolitan Area but within the State of Michigan. Any onsite trip outside of normal business hours will be charged at 1.5 times the regular bill rate of the appropriate resource.

Our proposed billing rate includes pay and benefits towards holiday, vacation, and various health insurance to attract and retain skilled and experienced talent. However, this above proposed cost doesn't include any onsite travel-related cost, software license,

| |
|---|
| hardware, equipment, network device or any other item that is specifically required for this project and it will be an additional cost as an actual cost. |
| GSG team has large pool of resources based in Michigan for all offered services including IT, Network, and Cybersecurity technical team and we are planning to propose 2-4 resources team for each Municipal Agency / Department depending upon various criteria including scope of work, number of covered assets/endpoints/devices, budget, project schedule, stakeholder availability, etc. Some tasks may be accomplished in parallel depending upon information, systems, and stakeholders' availability. |
| For effective project scheduling, the Client management needs to provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project and all the Client stakeholders should be available as needed to ensure the timeliness and success of this project. |
| The Client will provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project. |
| During this engagement, any vulnerabilities, sensitive data, or configuration data found will not be disclosed except to specify the Client staff. |
| During this effort, GSG will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between the Client and third parties. |
| The Client management will ensure that appropriate personnel are available to meet with the GSG team, as necessary to ensure the success of this project. |
| GSG will not be accountable when delays result from the Client's inability to meet stated prerequisites prior to an engagement, nor when delays result from the Client personnel not being available to provide the required support for the success of this project. |
| The proposal will be valid for 90 days. |

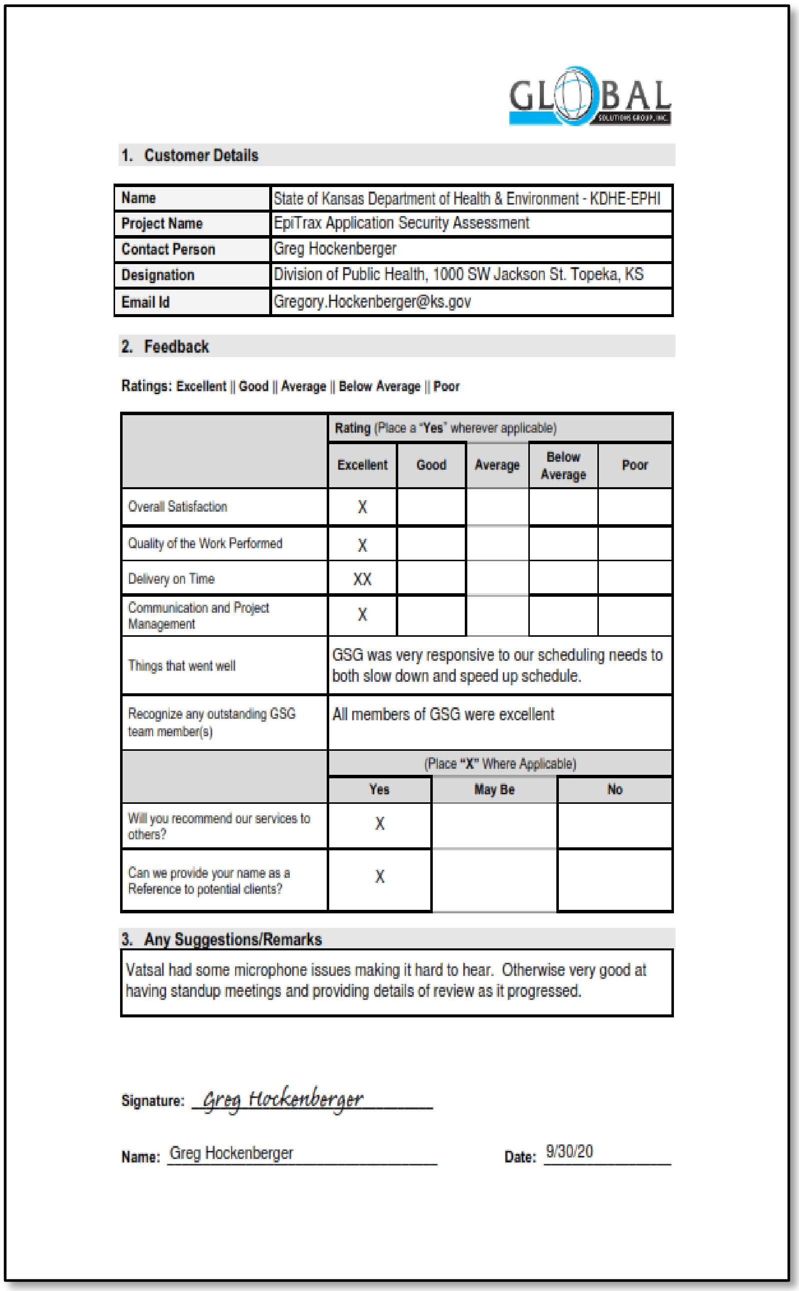
## Tab 5. Performance Reviews

Past performance is an indicator of future performance. Our stellar performance on our contracts is recognized by our customers who acknowledge our outstanding contract performance in written customer reviews. Below is just a subset of our customer reviews from multiple clients.

### *a) State and Local Performance Assessments*

### 5.a.1 State of Kansas Department of Health & Environment

**Synopsis: Excellent in all categories**



**1. Customer Details**

| | |
|---|---|
| **Name** | State of Kansas Department of Health & Environment - KDHE-EPHI |
| **Project Name** | EpiTrax Application Security Assessment |
| **Contact Person** | Greg Hockenberger |
| **Designation** | Division of Public Health, 1000 SW Jackson St. Topeka, KS |
| **Email Id** | Gregory.Hockenberger@ks.gov |

**2. Feedback**

**Ratings: Excellent || Good || Average || Below Average || Poor**

| | **Rating** (Place a "**Yes**" wherever applicable) | | | | |
|---|---|---|---|---|---|
| | **Excellent** | **Good** | **Average** | **Below Average** | **Poor** |
| Overall Satisfaction | X | | | | |
| Quality of the Work Performed | X | | | | |
| Delivery on Time | XX | | | | |
| Communication and Project Management | X | | | | |
| Things that went well | GSG was very responsive to our scheduling needs to both slow down and speed up schedule. | | | | |
| Recognize any outstanding GSG team member(s) | All members of GSG were excellent | | | | |

| | (Place "**X**" Where Applicable) | | |
|---|---|---|---|
| | **Yes** | **May Be** | **No** |
| Will you recommend our services to others? | X | | |
| Can we provide your name as a Reference to potential clients? | X | | |

**3. Any Suggestions/Remarks**

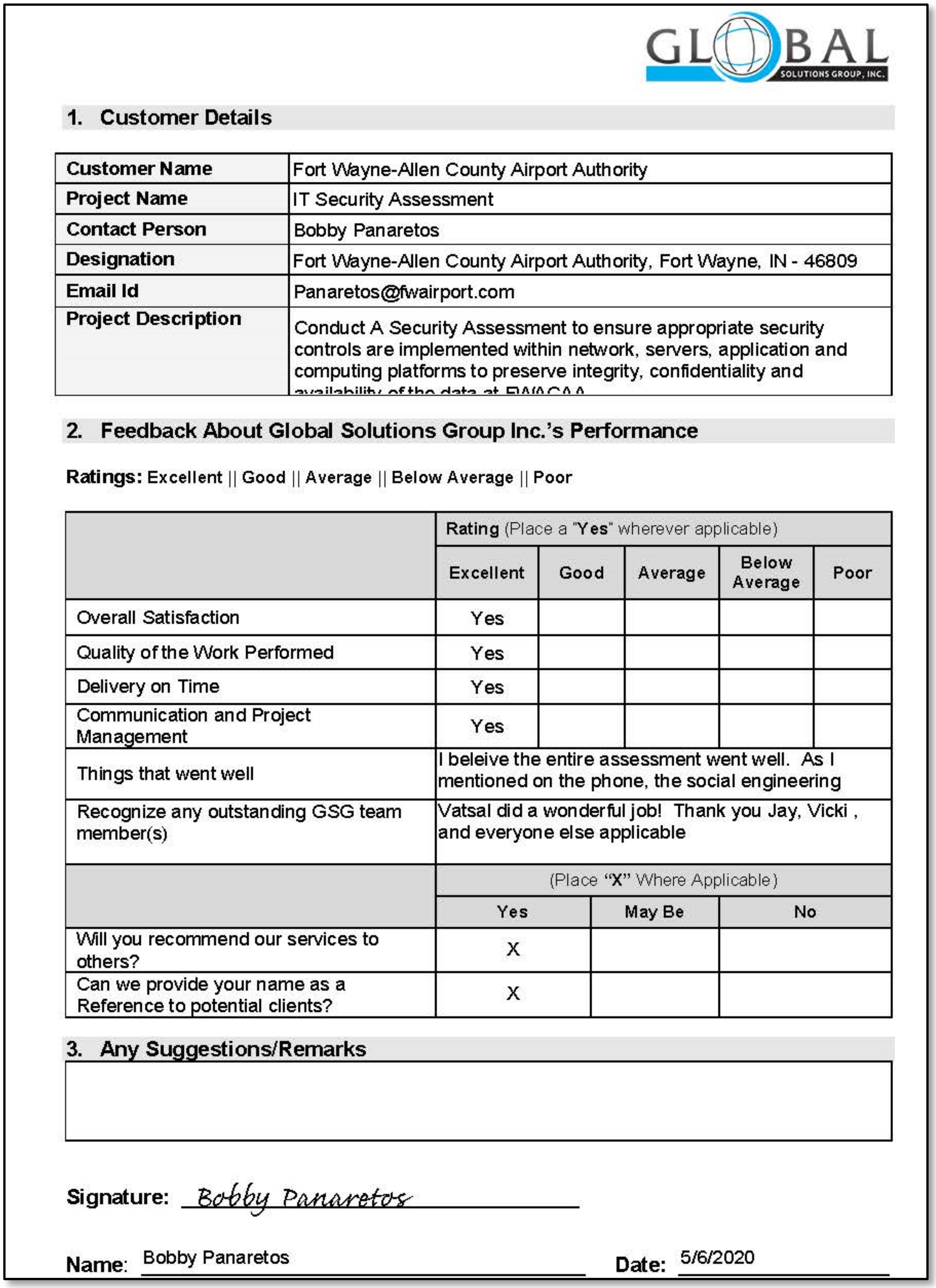
Vatsal had some microphone issues making it hard to hear. Otherwise very good at having standup meetings and providing details of review as it progressed.

**Signature:** Greg Hockenberger

**Name:** Greg Hockenberger **Date:** 9/30/20

## 5.a.2 Fort Wayne–Allen County Airport Authority

**Synopsis: Excellent in all categories**



### 1. Customer Details

| | |
|---|---|
| **Customer Name** | Fort Wayne-Allen County Airport Authority |
| **Project Name** | IT Security Assessment |
| **Contact Person** | Bobby Panaretos |
| **Designation** | Fort Wayne-Allen County Airport Authority, Fort Wayne, IN - 46809 |
| **Email Id** | Panaretos@fwairport.com |
| **Project Description** | Conduct A Security Assessment to ensure appropriate security controls are implemented within network, servers, application and computing platforms to preserve integrity, confidentiality and availability of the data at FWACAA |

### 2. Feedback About Global Solutions Group Inc.'s Performance

**Ratings:** Excellent || Good || Average || Below Average || Poor

| | **Rating** (Place a "**Yes**" wherever applicable) | | | | |
|---|---|---|---|---|---|
| | Excellent | Good | Average | Below Average | Poor |
| Overall Satisfaction | Yes | | | | |
| Quality of the Work Performed | Yes | | | | |
| Delivery on Time | Yes | | | | |
| Communication and Project Management | Yes | | | | |
| Things that went well | I beleive the entire assessment went well. As I mentioned on the phone, the social engineering | | | | |
| Recognize any outstanding GSG team member(s) | Vatsal did a wonderful job! Thank you Jay, Vicki , and everyone else applicable | | | | |

| | (Place **"X"** Where Applicable) | | |
|---|---|---|---|
| | Yes | May Be | No |
| Will you recommend our services to others? | X | | |
| Can we provide your name as a Reference to potential clients? | X | | |

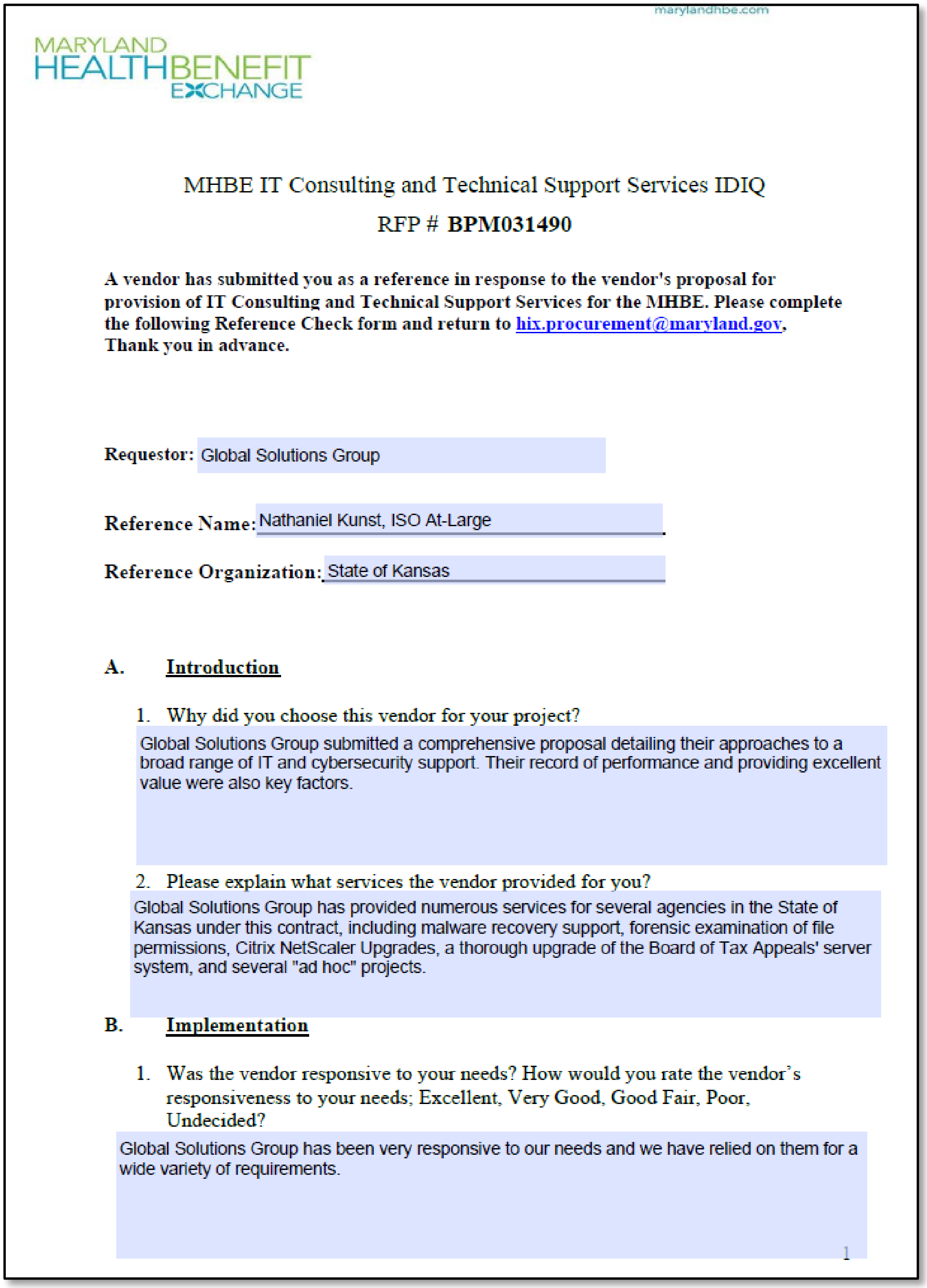
### 3. Any Suggestions/Remarks

**Signature:** Bobby Panaretos

**Name:** Bobby Panaretos **Date:** 5/6/2020

## 5.a.3 State of Kansas

**Synopsis: Vendor Performance Excellent**



marylandhbe.com

MARYLAND HEALTHBENEFIT EXCHANGE

MHBE IT Consulting and Technical Support Services IDIQ

RFP # **BPM031490**

**A vendor has submitted you as a reference in response to the vendor's proposal for provision of IT Consulting and Technical Support Services for the MHBE. Please complete the following Reference Check form and return to hix.procurement@maryland.gov. Thank you in advance.**

**Requestor:** Global Solutions Group

**Reference Name:** Nathaniel Kunst, ISO At-Large

**Reference Organization:** State of Kansas

**A. Introduction**

1. Why did you choose this vendor for your project?

Global Solutions Group submitted a comprehensive proposal detailing their approaches to a broad range of IT and cybersecurity support. Their record of performance and providing excellent value were also key factors.

2. Please explain what services the vendor provided for you?

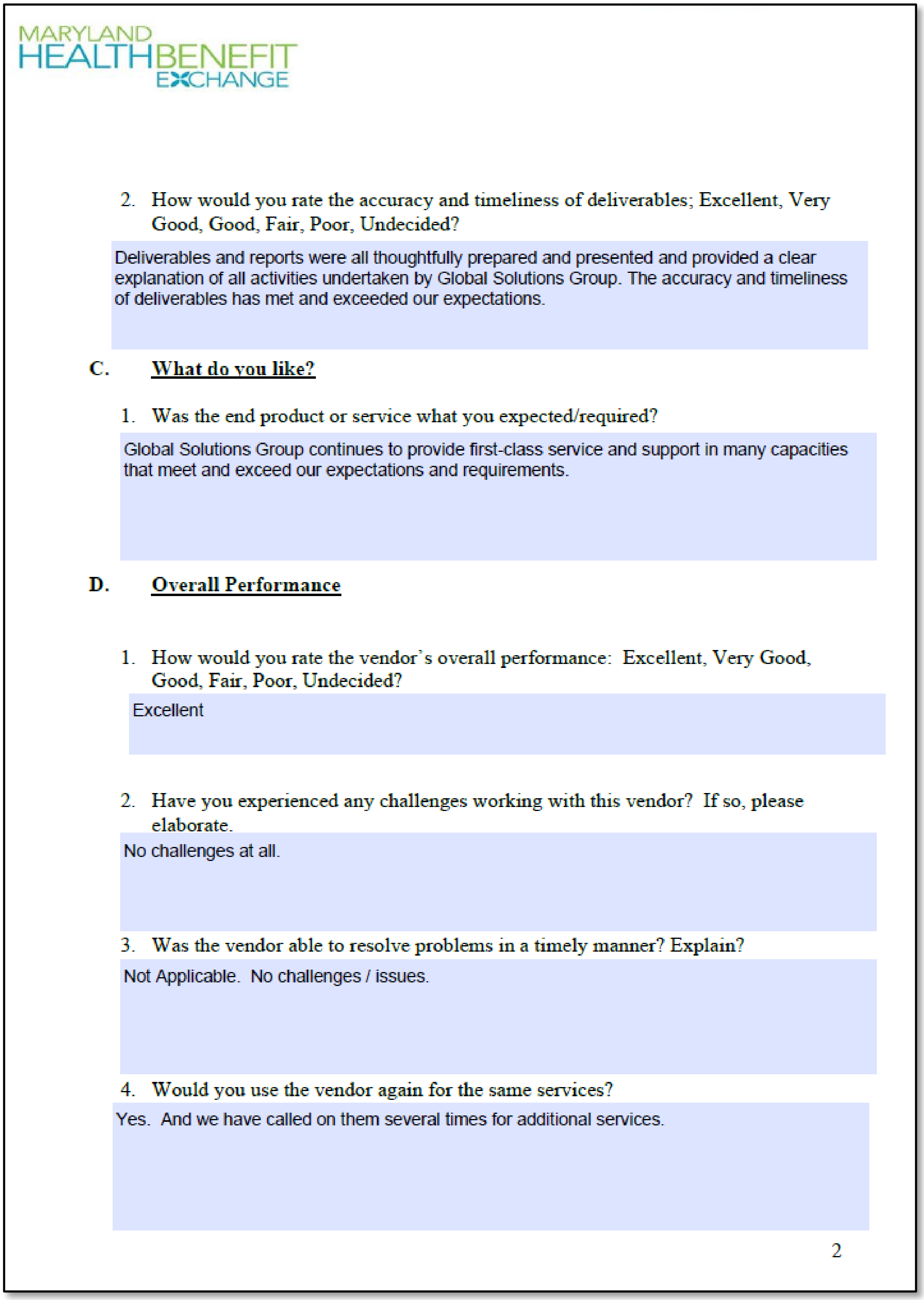
Global Solutions Group has provided numerous services for several agencies in the State of Kansas under this contract, including malware recovery support, forensic examination of file permissions, Citrix NetScaler Upgrades, a thorough upgrade of the Board of Tax Appeals' server system, and several "ad hoc" projects.

**B. Implementation**

1. Was the vendor responsive to your needs? How would you rate the vendor's responsiveness to your needs; Excellent, Very Good, Good Fair, Poor, Undecided?

Global Solutions Group has been very responsive to our needs and we have relied on them for a wide variety of requirements.

1



MARYLAND HEALTHBENEFIT EXCHANGE

2. How would you rate the accuracy and timeliness of deliverables; Excellent, Very Good, Good, Fair, Poor, Undecided?

Deliverables and reports were all thoughtfully prepared and presented and provided a clear explanation of all activities undertaken by Global Solutions Group. The accuracy and timeliness of deliverables has met and exceeded our expectations.

**C. What do you like?**

1. Was the end product or service what you expected/required?

Global Solutions Group continues to provide first-class service and support in many capacities that meet and exceed our expectations and requirements.

**D. Overall Performance**

1. How would you rate the vendor's overall performance: Excellent, Very Good, Good, Fair, Poor, Undecided?

Excellent

2. Have you experienced any challenges working with this vendor? If so, please elaborate.

No challenges at all.

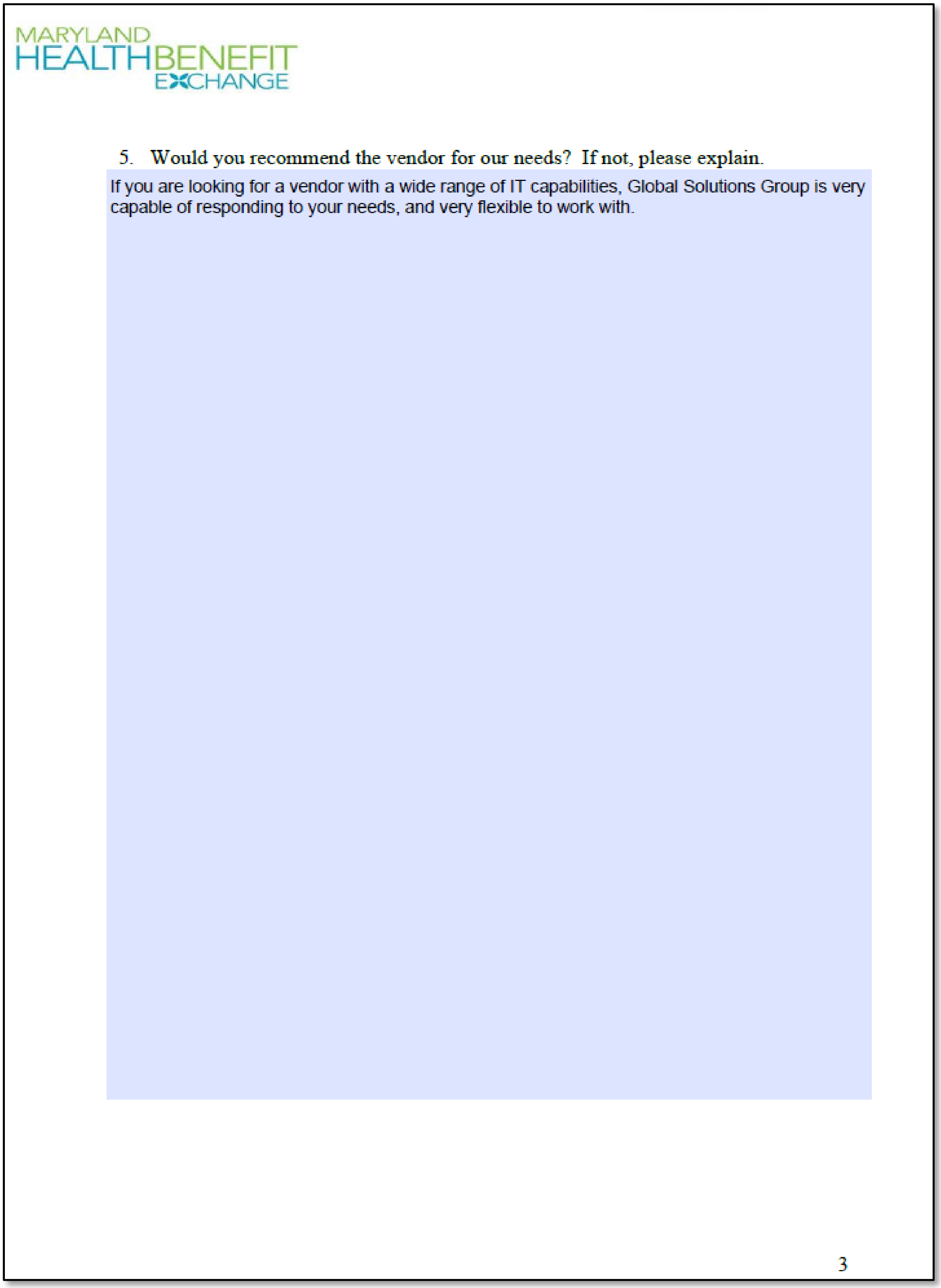
3. Was the vendor able to resolve problems in a timely manner? Explain?

Not Applicable. No challenges / issues.

4. Would you use the vendor again for the same services?

Yes. And we have called on them several times for additional services.

2



MARYLAND HEALTH BENEFIT EXCHANGE

5. Would you recommend the vendor for our needs? If not, please explain.

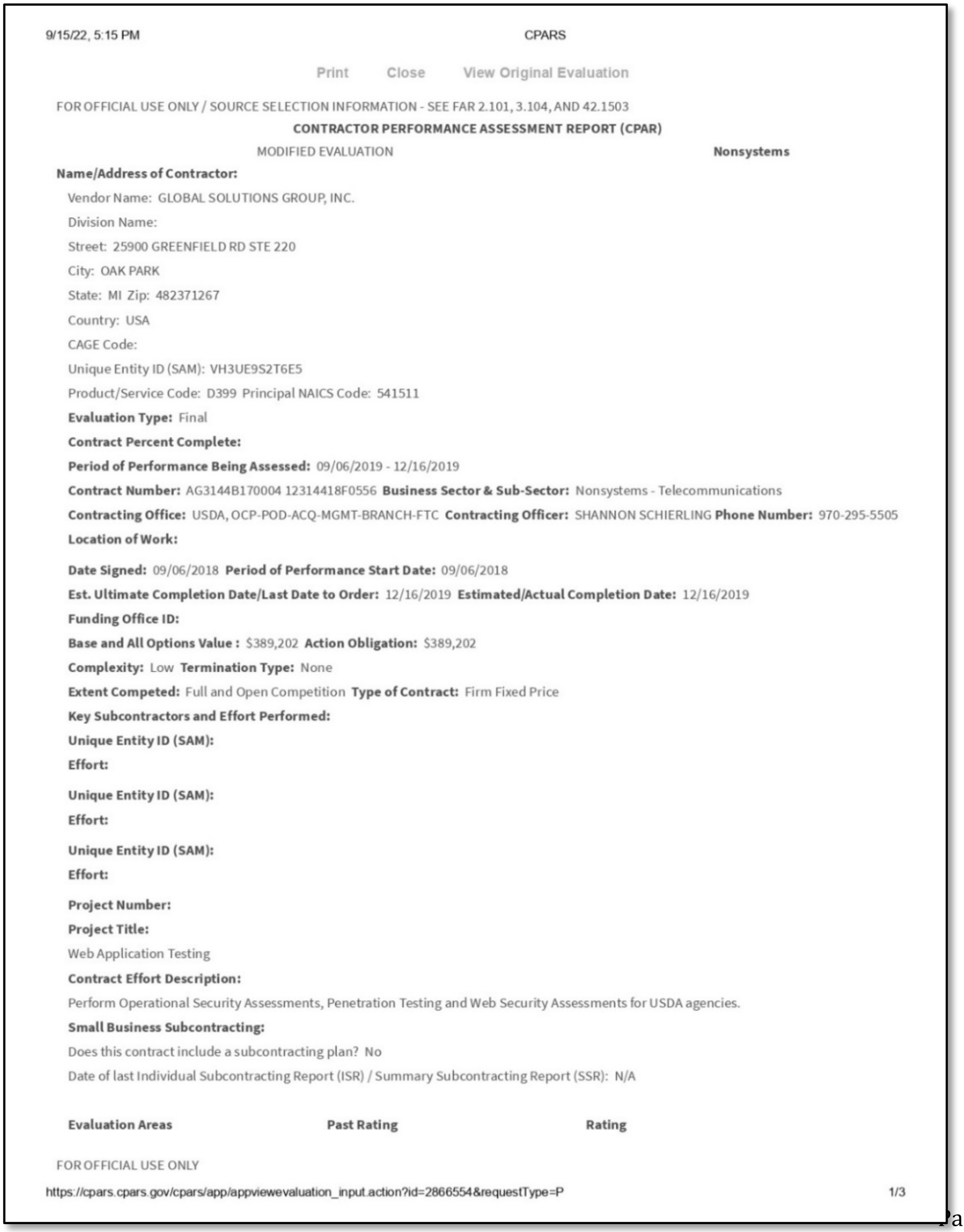
If you are looking for a vendor with a wide range of IT capabilities, Global Solutions Group is very capable of responding to your needs, and very flexible to work with.

### *b) Contract Performance Assessment Reporting System (CPARS)*

The following are Contract Performance Assessment Reporting System (CPARS) evaluations for several cybersecurity engagements. These are official assessments of performance made by federal government agencies regarding contractor performance on contracts.

### 5.b.1 2019 Operational Security Assessments, Penetration Testing, and Web Security Assessments x0556

**Synopsis: Quality and Cost Control are Exceptional**



9/15/22, 5:15 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)**

MODIFIED EVALUATION **Nonsystems**

**Name/Address of Contractor:**

Vendor Name: GLOBAL SOLUTIONS GROUP, INC.

Division Name:

Street: 25900 GREENFIELD RD STE 220

City: OAK PARK

State: MI Zip: 482371267

Country: USA

CAGE Code:

Unique Entity ID (SAM): VH3UE9S2T6E5

Product/Service Code: D399 Principal NAICS Code: 541511

**Evaluation Type:** Final

**Contract Percent Complete:**

**Period of Performance Being Assessed:** 09/06/2019 - 12/16/2019

**Contract Number:** AG3144B170004 12314418F0556 **Business Sector & Sub-Sector:** Nonsystems - Telecommunications

**Contracting Office:** USDA, OCP-POD-ACQ-MGMT-BRANCH-FTC **Contracting Officer:** SHANNON SCHIERLING **Phone Number:** 970-295-5505

**Location of Work:**

**Date Signed:** 09/06/2018 **Period of Performance Start Date:** 09/06/2018

**Est. Ultimate Completion Date/Last Date to Order:** 12/16/2019 **Estimated/Actual Completion Date:** 12/16/2019

**Funding Office ID:**

**Base and All Options Value :** $389,202 **Action Obligation:** $389,202

**Complexity:** Low **Termination Type:** None

**Extent Competed:** Full and Open Competition **Type of Contract:** Firm Fixed Price

**Key Subcontractors and Effort Performed:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Project Number:**

**Project Title:**

Web Application Testing

**Contract Effort Description:**

Perform Operational Security Assessments, Penetration Testing and Web Security Assessments for USDA agencies.

**Small Business Subcontracting:**

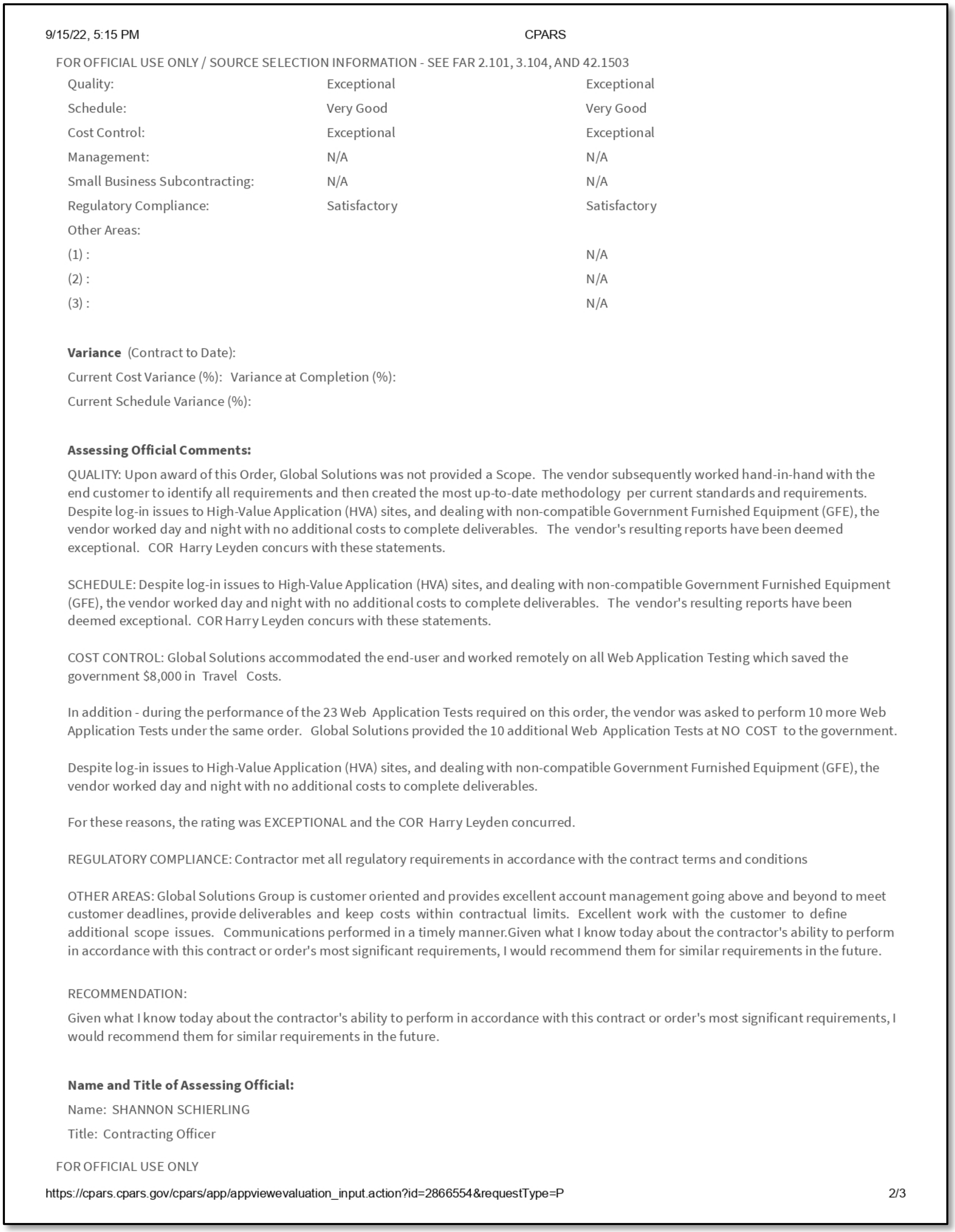
Does this contract include a subcontracting plan? No

Date of last Individual Subcontracting Report (ISR) / Summary Subcontracting Report (SSR): N/A

| Evaluation Areas | Past Rating | Rating |
|---|---|---|

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2866554&requestType=P 1/3



9/15/22, 5:15 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

| | | |
|---|---|---|
| Quality: | Exceptional | Exceptional |
| Schedule: | Very Good | Very Good |
| Cost Control: | Exceptional | Exceptional |
| Management: | N/A | N/A |
| Small Business Subcontracting: | N/A | N/A |
| Regulatory Compliance: | Satisfactory | Satisfactory |
| Other Areas: | | |
| (1) : | | N/A |
| (2) : | | N/A |
| (3) : | | N/A |

**Variance** (Contract to Date):

Current Cost Variance (%): Variance at Completion (%):

Current Schedule Variance (%):

**Assessing Official Comments:**

QUALITY: Upon award of this Order, Global Solutions was not provided a Scope. The vendor subsequently worked hand-in-hand with the end customer to identify all requirements and then created the most up-to-date methodology per current standards and requirements. Despite log-in issues to High-Value Application (HVA) sites, and dealing with non-compatible Government Furnished Equipment (GFE), the vendor worked day and night with no additional costs to complete deliverables. The vendor's resulting reports have been deemed exceptional. COR Harry Leyden concurs with these statements.

SCHEDULE: Despite log-in issues to High-Value Application (HVA) sites, and dealing with non-compatible Government Furnished Equipment (GFE), the vendor worked day and night with no additional costs to complete deliverables. The vendor's resulting reports have been deemed exceptional. COR Harry Leyden concurs with these statements.

COST CONTROL: Global Solutions accommodated the end-user and worked remotely on all Web Application Testing which saved the government $8,000 in Travel Costs.

In addition - during the performance of the 23 Web Application Tests required on this order, the vendor was asked to perform 10 more Web Application Tests under the same order. Global Solutions provided the 10 additional Web Application Tests at NO COST to the government.

Despite log-in issues to High-Value Application (HVA) sites, and dealing with non-compatible Government Furnished Equipment (GFE), the vendor worked day and night with no additional costs to complete deliverables.

For these reasons, the rating was EXCEPTIONAL and the COR Harry Leyden concurred.

REGULATORY COMPLIANCE: Contractor met all regulatory requirements in accordance with the contract terms and conditions

OTHER AREAS: Global Solutions Group is customer oriented and provides excellent account management going above and beyond to meet customer deadlines, provide deliverables and keep costs within contractual limits. Excellent work with the customer to define additional scope issues. Communications performed in a timely manner.Given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.

RECOMMENDATION:

Given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.

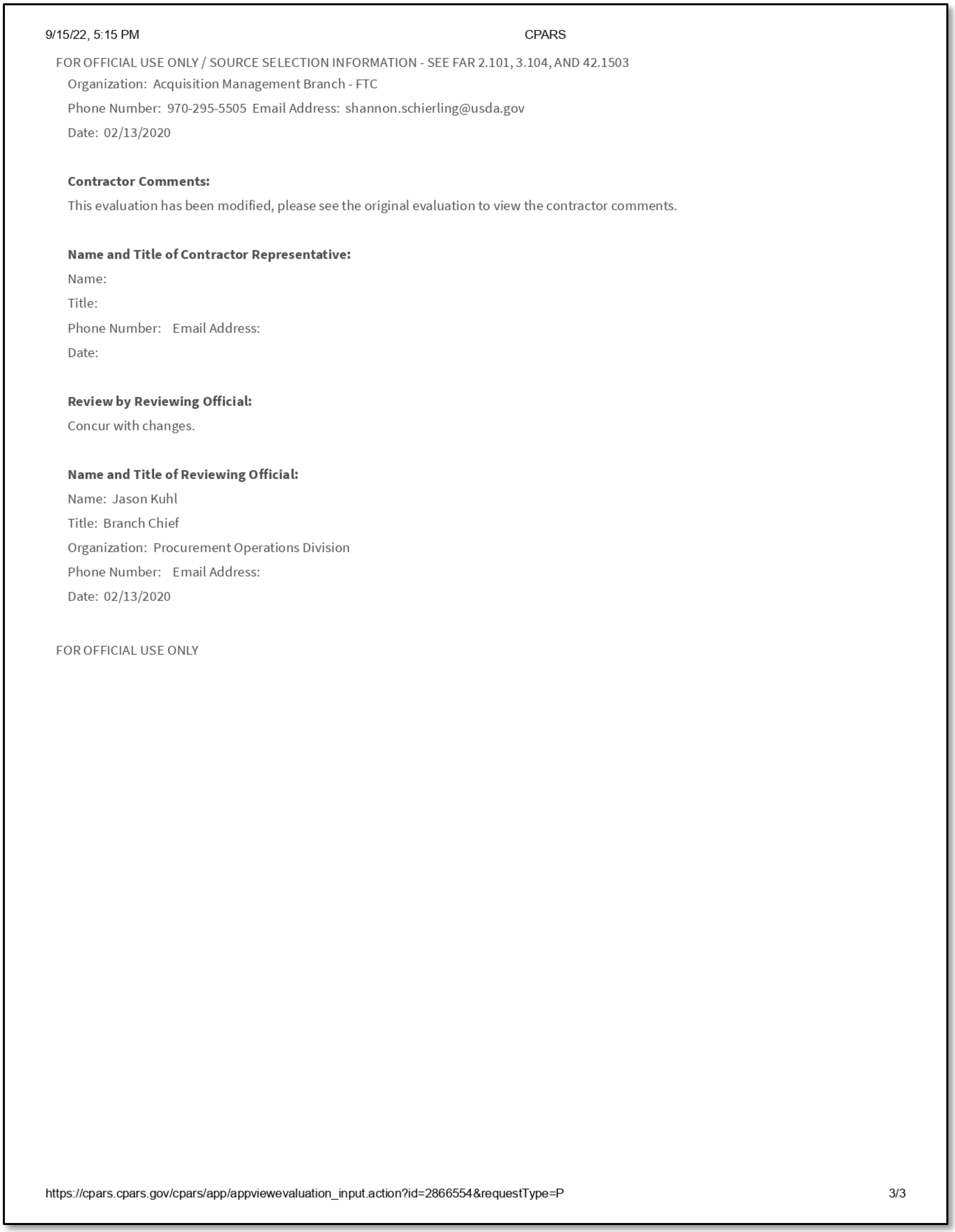
**Name and Title of Assessing Official:**

Name: SHANNON SCHIERLING

Title: Contracting Officer

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2866554&requestType=P 2/3



9/15/22, 5:15 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

Organization: Acquisition Management Branch - FTC

Phone Number: 970-295-5505 Email Address: shannon.schierling@usda.gov

Date: 02/13/2020

**Contractor Comments:**

This evaluation has been modified, please see the original evaluation to view the contractor comments.

**Name and Title of Contractor Representative:**

Name:

Title:

Phone Number: Email Address:

Date:

**Review by Reviewing Official:**

Concur with changes.

**Name and Title of Reviewing Official:**

Name: Jason Kuhl

Title: Branch Chief

Organization: Procurement Operations Division

Phone Number: Email Address:

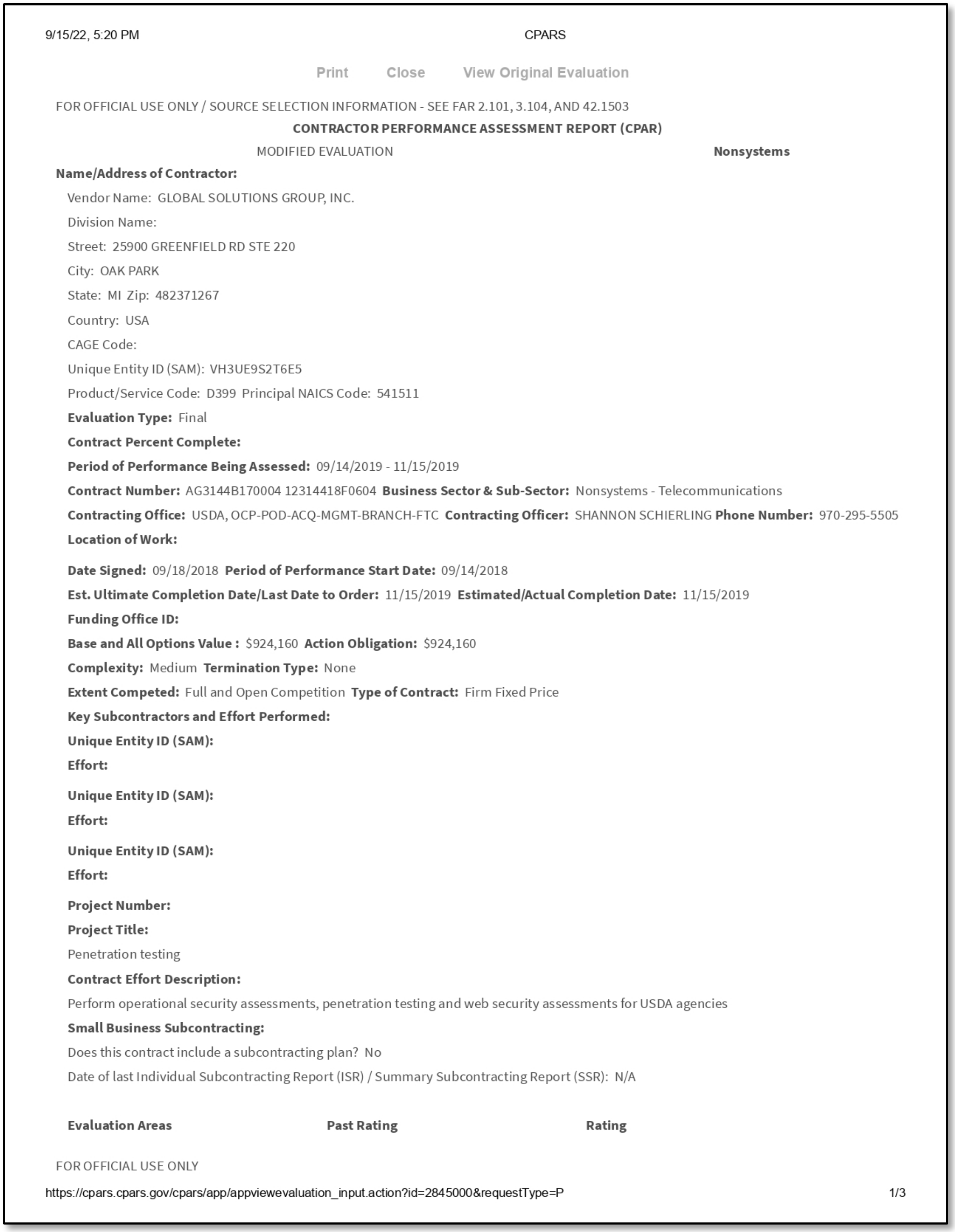
Date: 02/13/2020

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2866554&requestType=P 3/3

## 5.b.2 2019 Operational Security Assessment, Penetration Testing, and Web Security Assessment x0604

**Synopsis: Quality and Cost Control are Exceptional**



9/15/22, 5:20 PM CPARS

Print Close View Original Evaluation

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)**

MODIFIED EVALUATION **Nonsystems**

**Name/Address of Contractor:**

Vendor Name: GLOBAL SOLUTIONS GROUP, INC.

Division Name:

Street: 25900 GREENFIELD RD STE 220

City: OAK PARK

State: MI Zip: 482371267

Country: USA

CAGE Code:

Unique Entity ID (SAM): VH3UE9S2T6E5

Product/Service Code: D399 Principal NAICS Code: 541511

**Evaluation Type:** Final

**Contract Percent Complete:**

**Period of Performance Being Assessed:** 09/14/2019 - 11/15/2019

**Contract Number:** AG3144B170004 12314418F0604 **Business Sector & Sub-Sector:** Nonsystems - Telecommunications

**Contracting Office:** USDA, OCP-POD-ACQ-MGMT-BRANCH-FTC **Contracting Officer:** SHANNON SCHIERLING **Phone Number:** 970-295-5505

**Location of Work:**

**Date Signed:** 09/18/2018 **Period of Performance Start Date:** 09/14/2018

**Est. Ultimate Completion Date/Last Date to Order:** 11/15/2019 **Estimated/Actual Completion Date:** 11/15/2019

**Funding Office ID:**

**Base and All Options Value :** $924,160 **Action Obligation:** $924,160

**Complexity:** Medium **Termination Type:** None

**Extent Competed:** Full and Open Competition **Type of Contract:** Firm Fixed Price

**Key Subcontractors and Effort Performed:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Project Number:**

**Project Title:**

Penetration testing

**Contract Effort Description:**

Perform operational security assessments, penetration testing and web security assessments for USDA agencies

**Small Business Subcontracting:**

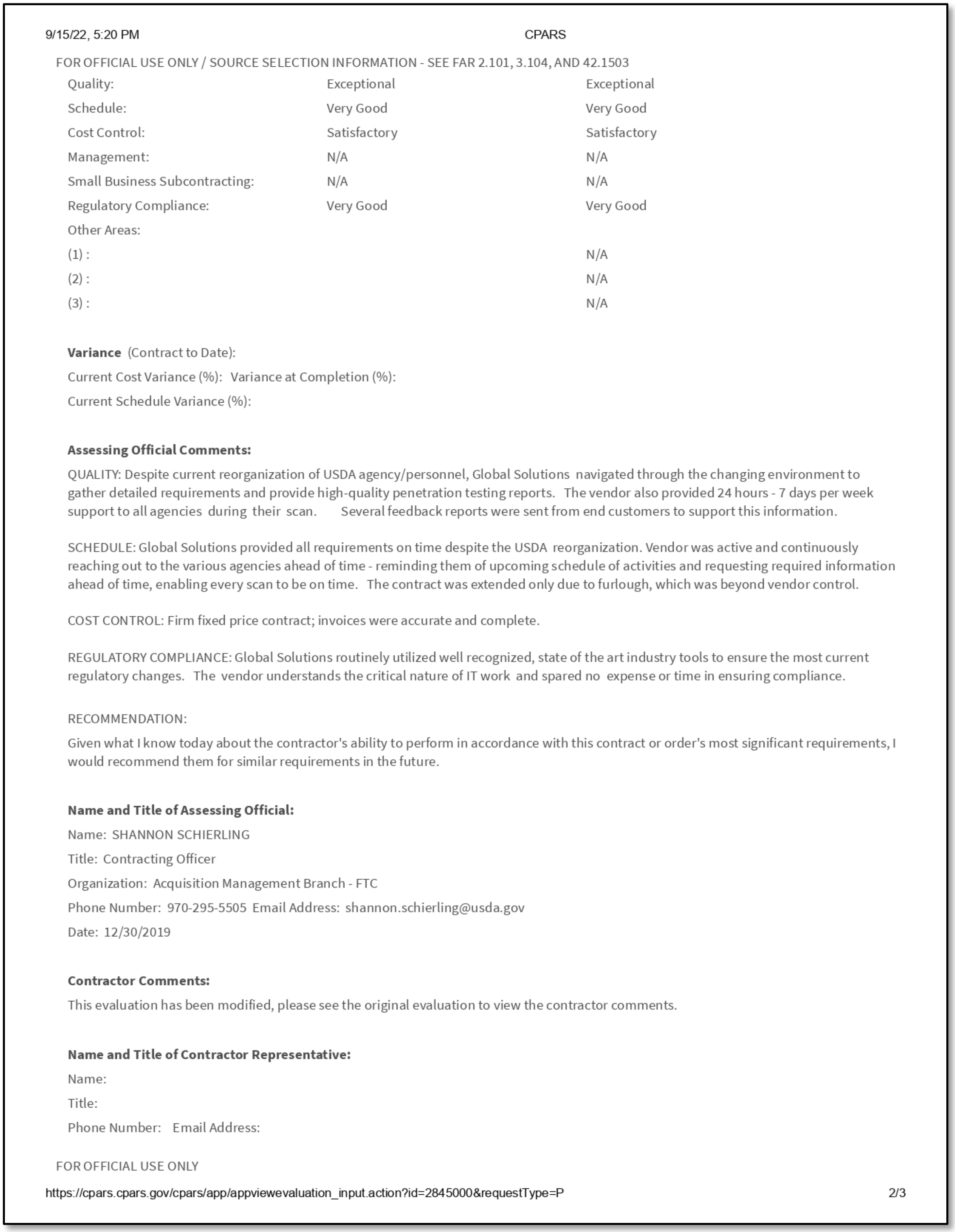
Does this contract include a subcontracting plan? No

Date of last Individual Subcontracting Report (ISR) / Summary Subcontracting Report (SSR): N/A

| Evaluation Areas | Past Rating | Rating |
|---|---|---|

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2845000&requestType=P 1/3



9/15/22, 5:20 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

| | | |
|---|---|---|
| Quality: | Exceptional | Exceptional |
| Schedule: | Very Good | Very Good |
| Cost Control: | Satisfactory | Satisfactory |
| Management: | N/A | N/A |
| Small Business Subcontracting: | N/A | N/A |
| Regulatory Compliance: | Very Good | Very Good |
| Other Areas: | | |
| (1) : | | N/A |
| (2) : | | N/A |
| (3) : | | N/A |

**Variance** (Contract to Date):

Current Cost Variance (%): Variance at Completion (%):

Current Schedule Variance (%):

**Assessing Official Comments:**

QUALITY: Despite current reorganization of USDA agency/personnel, Global Solutions navigated through the changing environment to gather detailed requirements and provide high-quality penetration testing reports. The vendor also provided 24 hours - 7 days per week support to all agencies during their scan. Several feedback reports were sent from end customers to support this information.

SCHEDULE: Global Solutions provided all requirements on time despite the USDA reorganization. Vendor was active and continuously reaching out to the various agencies ahead of time - reminding them of upcoming schedule of activities and requesting required information ahead of time, enabling every scan to be on time. The contract was extended only due to furlough, which was beyond vendor control.

COST CONTROL: Firm fixed price contract; invoices were accurate and complete.

REGULATORY COMPLIANCE: Global Solutions routinely utilized well recognized, state of the art industry tools to ensure the most current regulatory changes. The vendor understands the critical nature of IT work and spared no expense or time in ensuring compliance.

RECOMMENDATION:

Given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.

**Name and Title of Assessing Official:**

Name: SHANNON SCHIERLING

Title: Contracting Officer

Organization: Acquisition Management Branch - FTC

Phone Number: 970-295-5505 Email Address: shannon.schierling@usda.gov

Date: 12/30/2019

**Contractor Comments:**

This evaluation has been modified, please see the original evaluation to view the contractor comments.

**Name and Title of Contractor Representative:**

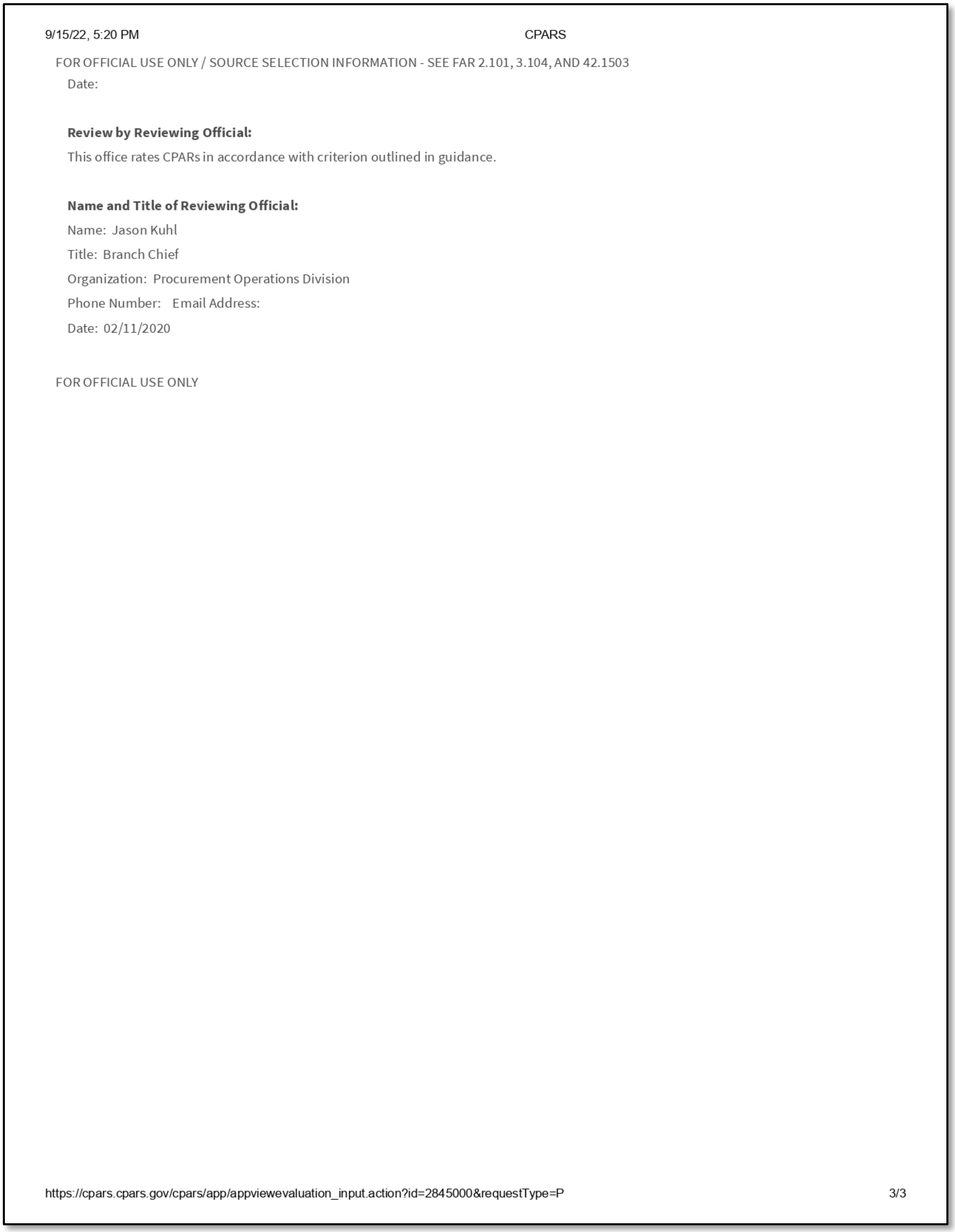
Name:

Title:

Phone Number: Email Address:

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2845000&requestType=P 2/3



9/15/22, 5:20 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

Date:

**Review by Reviewing Official:**

This office rates CPARs in accordance with criterion outlined in guidance.

**Name and Title of Reviewing Official:**

Name: Jason Kuhl

Title: Branch Chief

Organization: Procurement Operations Division

Phone Number: Email Address:

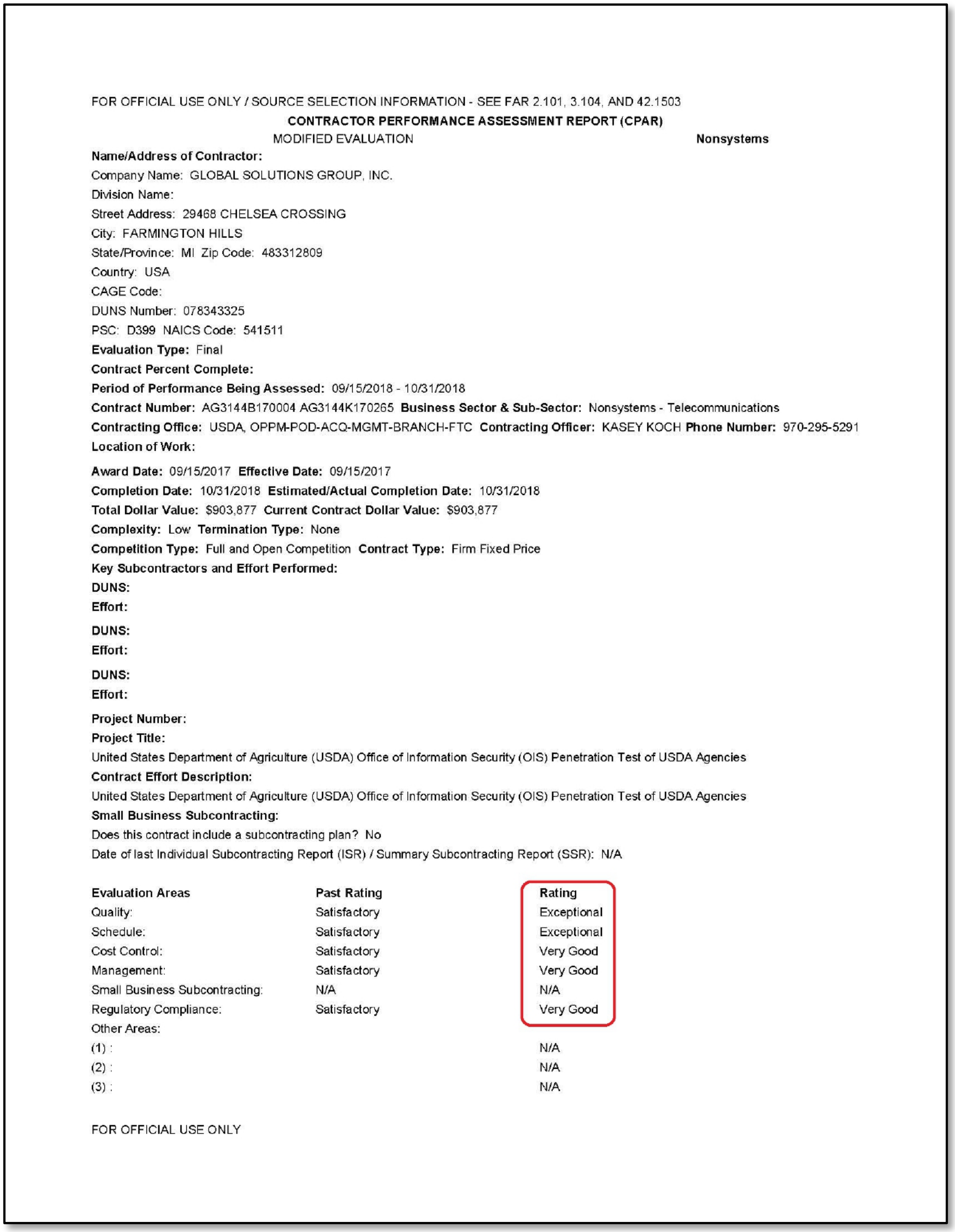
Date: 02/11/2020

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2845000&requestType=P 3/3

## 5.b.3 2018 Penetration Testing for USDA Agencies x0265

**Synopsis: Quality and Schedule are Exceptional**



FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)**

MODIFIED EVALUATION **Nonsystems**

**Name/Address of Contractor:**

Company Name: GLOBAL SOLUTIONS GROUP, INC.
Division Name:
Street Address: 29468 CHELSEA CROSSING
City: FARMINGTON HILLS
State/Province: MI Zip Code: 483312809
Country: USA
CAGE Code:
DUNS Number: 078343325
PSC: D399 NAICS Code: 541511

**Evaluation Type:** Final
**Contract Percent Complete:**
**Period of Performance Being Assessed:** 09/15/2018 - 10/31/2018
**Contract Number:** AG3144B170004 AG3144K170265 **Business Sector & Sub-Sector:** Nonsystems - Telecommunications
**Contracting Office:** USDA, OPPM-POD-ACQ-MGMT-BRANCH-FTC **Contracting Officer:** KASEY KOCH **Phone Number:** 970-295-5291
**Location of Work:**

**Award Date:** 09/15/2017 **Effective Date:** 09/15/2017
**Completion Date:** 10/31/2018 **Estimated/Actual Completion Date:** 10/31/2018
**Total Dollar Value:** $903,877 **Current Contract Dollar Value:** $903,877
**Complexity:** Low **Termination Type:** None
**Competition Type:** Full and Open Competition **Contract Type:** Firm Fixed Price
**Key Subcontractors and Effort Performed:**
**DUNS:**
**Effort:**

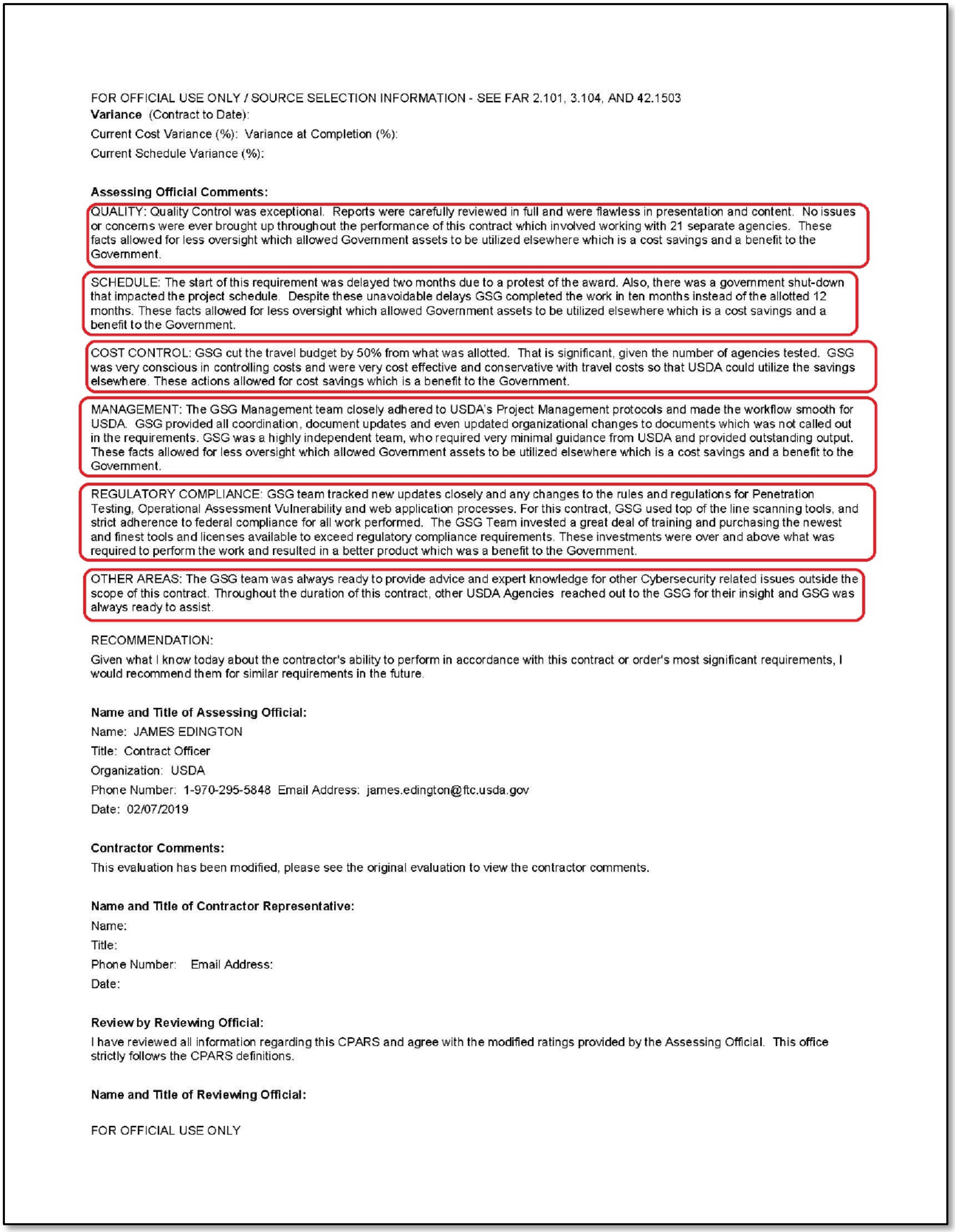
**DUNS:**
**Effort:**

**DUNS:**
**Effort:**

**Project Number:**
**Project Title:**
United States Department of Agriculture (USDA) Office of Information Security (OIS) Penetration Test of USDA Agencies
**Contract Effort Description:**
United States Department of Agriculture (USDA) Office of Information Security (OIS) Penetration Test of USDA Agencies
**Small Business Subcontracting:**
Does this contract include a subcontracting plan? No
Date of last Individual Subcontracting Report (ISR) / Summary Subcontracting Report (SSR): N/A

| Evaluation Areas | Past Rating | Rating |
|---|---|---|
| Quality: | Satisfactory | Exceptional |
| Schedule: | Satisfactory | Exceptional |
| Cost Control: | Satisfactory | Very Good |
| Management: | Satisfactory | Very Good |
| Small Business Subcontracting: | N/A | N/A |
| Regulatory Compliance: | Satisfactory | Very Good |
| Other Areas: | | |
| (1) : | | N/A |
| (2) : | | N/A |
| (3) : | | N/A |

FOR OFFICIAL USE ONLY



FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**Variance** (Contract to Date):

Current Cost Variance (%): Variance at Completion (%):

Current Schedule Variance (%):

**Assessing Official Comments:**

QUALITY: Quality Control was exceptional. Reports were carefully reviewed in full and were flawless in presentation and content. No issues or concerns were ever brought up throughout the performance of this contract which involved working with 21 separate agencies. These facts allowed for less oversight which allowed Government assets to be utilized elsewhere which is a cost savings and a benefit to the Government.

SCHEDULE: The start of this requirement was delayed two months due to a protest of the award. Also, there was a government shut-down that impacted the project schedule. Despite these unavoidable delays GSG completed the work in ten months instead of the allotted 12 months. These facts allowed for less oversight which allowed Government assets to be utilized elsewhere which is a cost savings and a benefit to the Government.

COST CONTROL: GSG cut the travel budget by 50% from what was allotted. That is significant, given the number of agencies tested. GSG was very conscious in controlling costs and were very cost effective and conservative with travel costs so that USDA could utilize the savings elsewhere. These actions allowed for cost savings which is a benefit to the Government.

MANAGEMENT: The GSG Management team closely adhered to USDA's Project Management protocols and made the workflow smooth for USDA. GSG provided all coordination, document updates and even updated organizational changes to documents which was not called out in the requirements. GSG was a highly independent team, who required very minimal guidance from USDA and provided outstanding output. These facts allowed for less oversight which allowed Government assets to be utilized elsewhere which is a cost savings and a benefit to the Government.

REGULATORY COMPLIANCE: GSG team tracked new updates closely and any changes to the rules and regulations for Penetration Testing, Operational Assessment Vulnerability and web application processes. For this contract, GSG used top of the line scanning tools, and strict adherence to federal compliance for all work performed. The GSG Team invested a great deal of training and purchasing the newest and finest tools and licenses available to exceed regulatory compliance requirements. These investments were over and above what was required to perform the work and resulted in a better product which was a benefit to the Government.

OTHER AREAS: The GSG team was always ready to provide advice and expert knowledge for other Cybersecurity related issues outside the scope of this contract. Throughout the duration of this contract, other USDA Agencies reached out to the GSG for their insight and GSG was always ready to assist.

RECOMMENDATION:

Given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.

**Name and Title of Assessing Official:**

Name: JAMES EDINGTON

Title: Contract Officer

Organization: USDA

Phone Number: 1-970-295-5848 Email Address: james.edington@ftc.usda.gov

Date: 02/07/2019

**Contractor Comments:**

This evaluation has been modified, please see the original evaluation to view the contractor comments.

**Name and Title of Contractor Representative:**

Name:

Title:

Phone Number: Email Address:

Date:

**Review by Reviewing Official:**

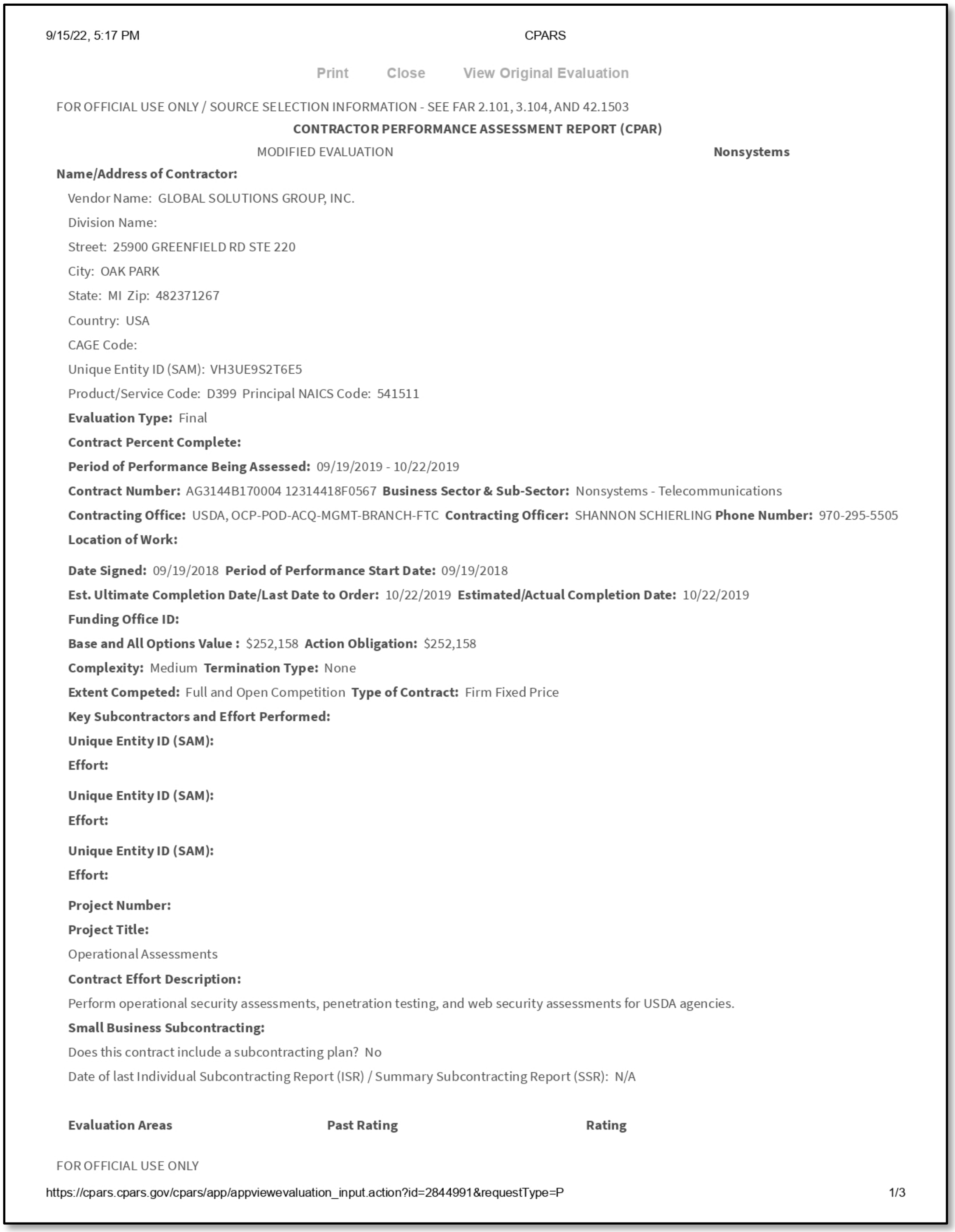
I have reviewed all information regarding this CPARS and agree with the modified ratings provided by the Assessing Official. This office strictly follows the CPARS definitions.

**Name and Title of Reviewing Official:**

FOR OFFICIAL USE ONLY

### 5.b.4 2019 Operational Security Assessment, Penetration Testing, and Web Security Assessment x0567

**Synopsis: Quality and Cost Control are Exceptional**



9/15/22, 5:17 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)**

MODIFIED EVALUATION **Nonsystems**

**Name/Address of Contractor:**

Vendor Name: GLOBAL SOLUTIONS GROUP, INC.

Division Name:

Street: 25900 GREENFIELD RD STE 220

City: OAK PARK

State: MI Zip: 482371267

Country: USA

CAGE Code:

Unique Entity ID (SAM): VH3UE9S2T6E5

Product/Service Code: D399 Principal NAICS Code: 541511

**Evaluation Type:** Final

**Contract Percent Complete:**

**Period of Performance Being Assessed:** 09/19/2019 - 10/22/2019

**Contract Number:** AG3144B170004 12314418F0567 **Business Sector & Sub-Sector:** Nonsystems - Telecommunications

**Contracting Office:** USDA, OCP-POD-ACQ-MGMT-BRANCH-FTC **Contracting Officer:** SHANNON SCHIERLING **Phone Number:** 970-295-5505

**Location of Work:**

**Date Signed:** 09/19/2018 **Period of Performance Start Date:** 09/19/2018

**Est. Ultimate Completion Date/Last Date to Order:** 10/22/2019 **Estimated/Actual Completion Date:** 10/22/2019

**Funding Office ID:**

**Base and All Options Value :** $252,158 **Action Obligation:** $252,158

**Complexity:** Medium **Termination Type:** None

**Extent Competed:** Full and Open Competition **Type of Contract:** Firm Fixed Price

**Key Subcontractors and Effort Performed:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Project Number:**

**Project Title:**

Operational Assessments

**Contract Effort Description:**

Perform operational security assessments, penetration testing, and web security assessments for USDA agencies.

**Small Business Subcontracting:**

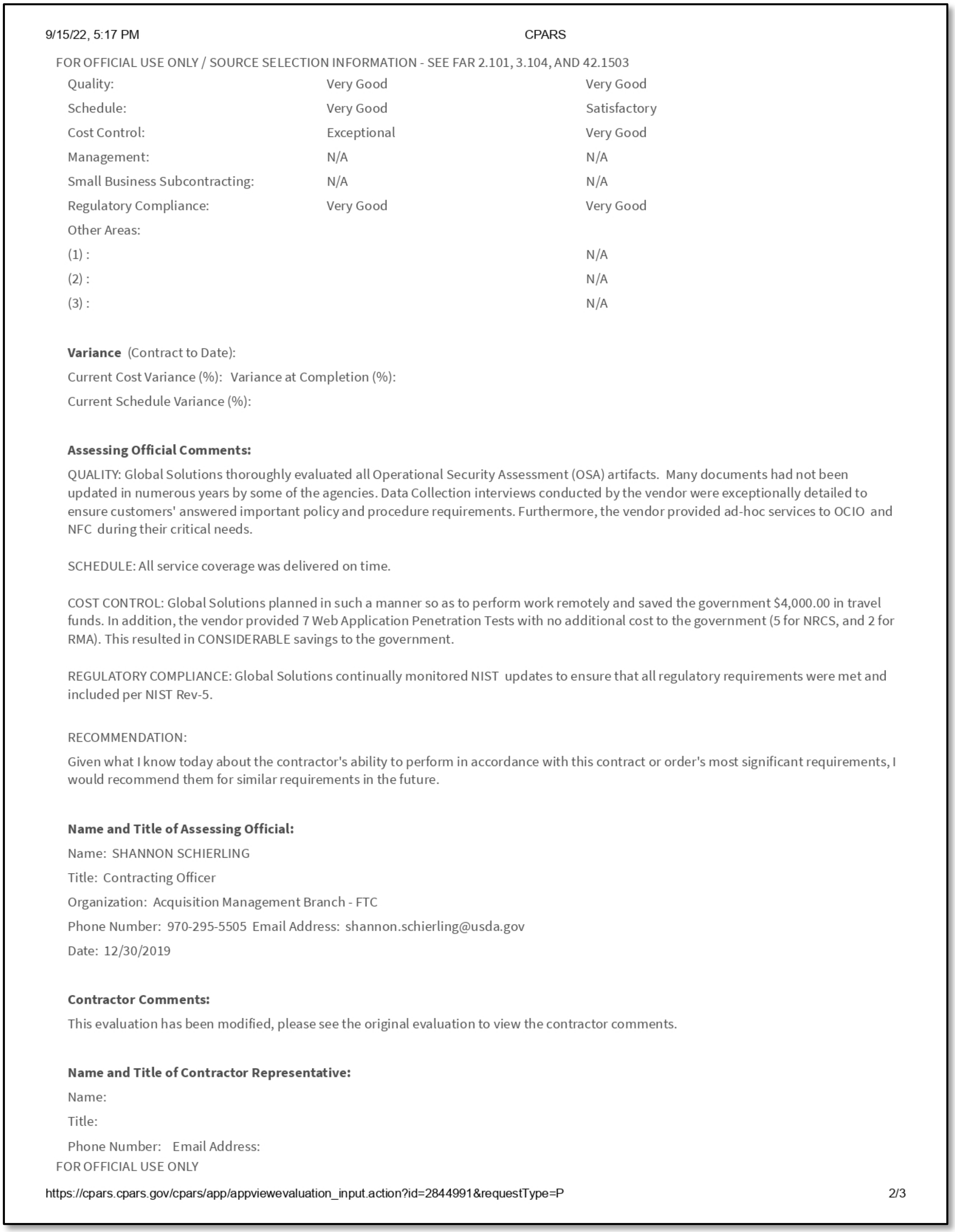
Does this contract include a subcontracting plan? No

Date of last Individual Subcontracting Report (ISR) / Summary Subcontracting Report (SSR): N/A

| **Evaluation Areas** | **Past Rating** | **Rating** |
|---|---|---|

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2844991&requestType=P 1/3



9/15/22, 5:17 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

| | | |
|---|---|---|
| Quality: | Very Good | Very Good |
| Schedule: | Very Good | Satisfactory |
| Cost Control: | Exceptional | Very Good |
| Management: | N/A | N/A |
| Small Business Subcontracting: | N/A | N/A |
| Regulatory Compliance: | Very Good | Very Good |
| Other Areas: | | |
| (1) : | | N/A |
| (2) : | | N/A |
| (3) : | | N/A |

**Variance** (Contract to Date):

Current Cost Variance (%): Variance at Completion (%):

Current Schedule Variance (%):

**Assessing Official Comments:**

QUALITY: Global Solutions thoroughly evaluated all Operational Security Assessment (OSA) artifacts. Many documents had not been updated in numerous years by some of the agencies. Data Collection interviews conducted by the vendor were exceptionally detailed to ensure customers' answered important policy and procedure requirements. Furthermore, the vendor provided ad-hoc services to OCIO and NFC during their critical needs.

SCHEDULE: All service coverage was delivered on time.

COST CONTROL: Global Solutions planned in such a manner so as to perform work remotely and saved the government $4,000.00 in travel funds. In addition, the vendor provided 7 Web Application Penetration Tests with no additional cost to the government (5 for NRCS, and 2 for RMA). This resulted in CONSIDERABLE savings to the government.

REGULATORY COMPLIANCE: Global Solutions continually monitored NIST updates to ensure that all regulatory requirements were met and included per NIST Rev-5.

RECOMMENDATION:

Given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.

**Name and Title of Assessing Official:**

Name: SHANNON SCHIERLING

Title: Contracting Officer

Organization: Acquisition Management Branch - FTC

Phone Number: 970-295-5505 Email Address: shannon.schierling@usda.gov

Date: 12/30/2019

**Contractor Comments:**

This evaluation has been modified, please see the original evaluation to view the contractor comments.

**Name and Title of Contractor Representative:**

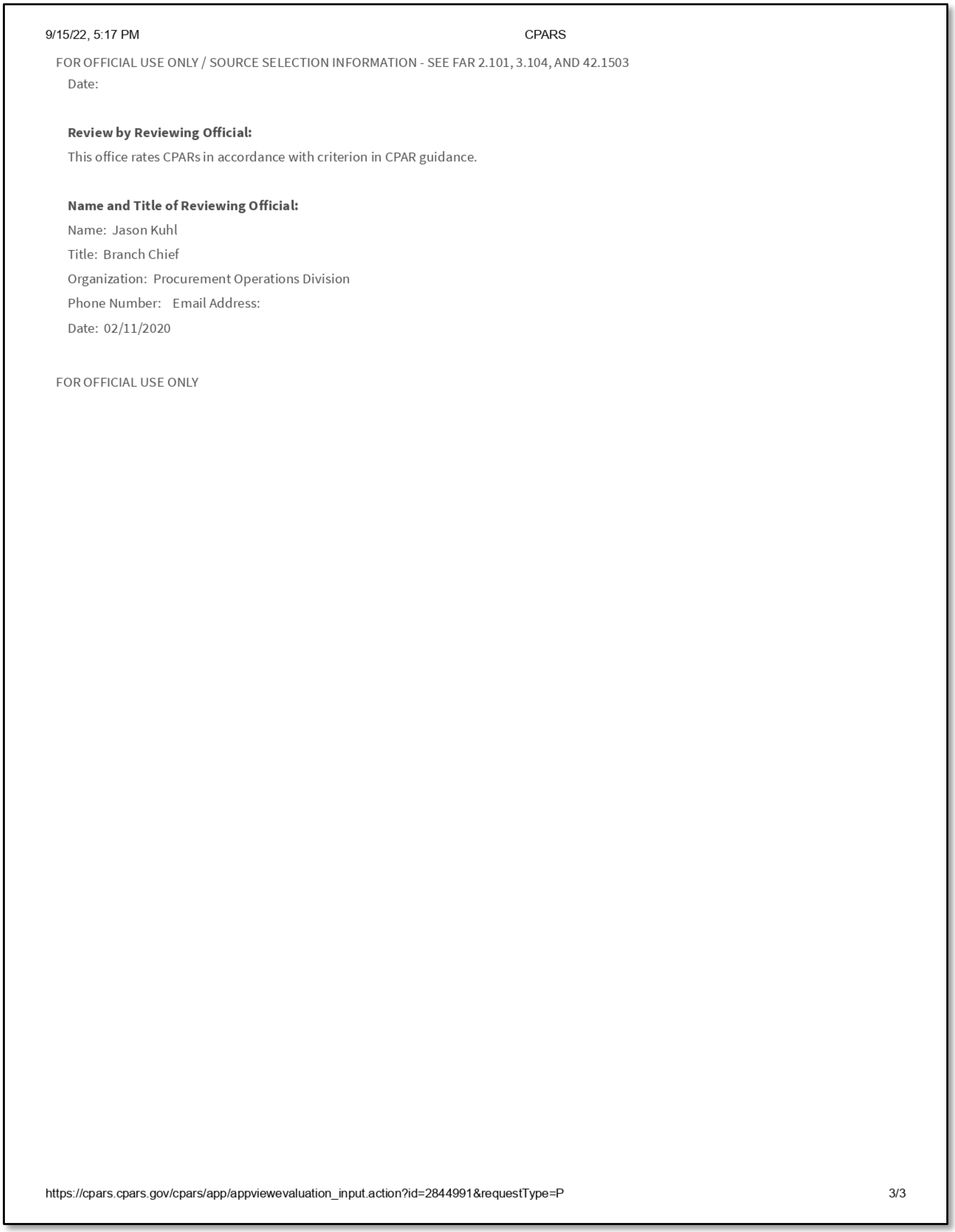
Name:

Title:

Phone Number: Email Address:

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2844991&requestType=P 2/3



9/15/22, 5:17 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

Date:

**Review by Reviewing Official:**

This office rates CPARs in accordance with criterion in CPAR guidance.

**Name and Title of Reviewing Official:**

Name: Jason Kuhl

Title: Branch Chief

Organization: Procurement Operations Division

Phone Number: Email Address:

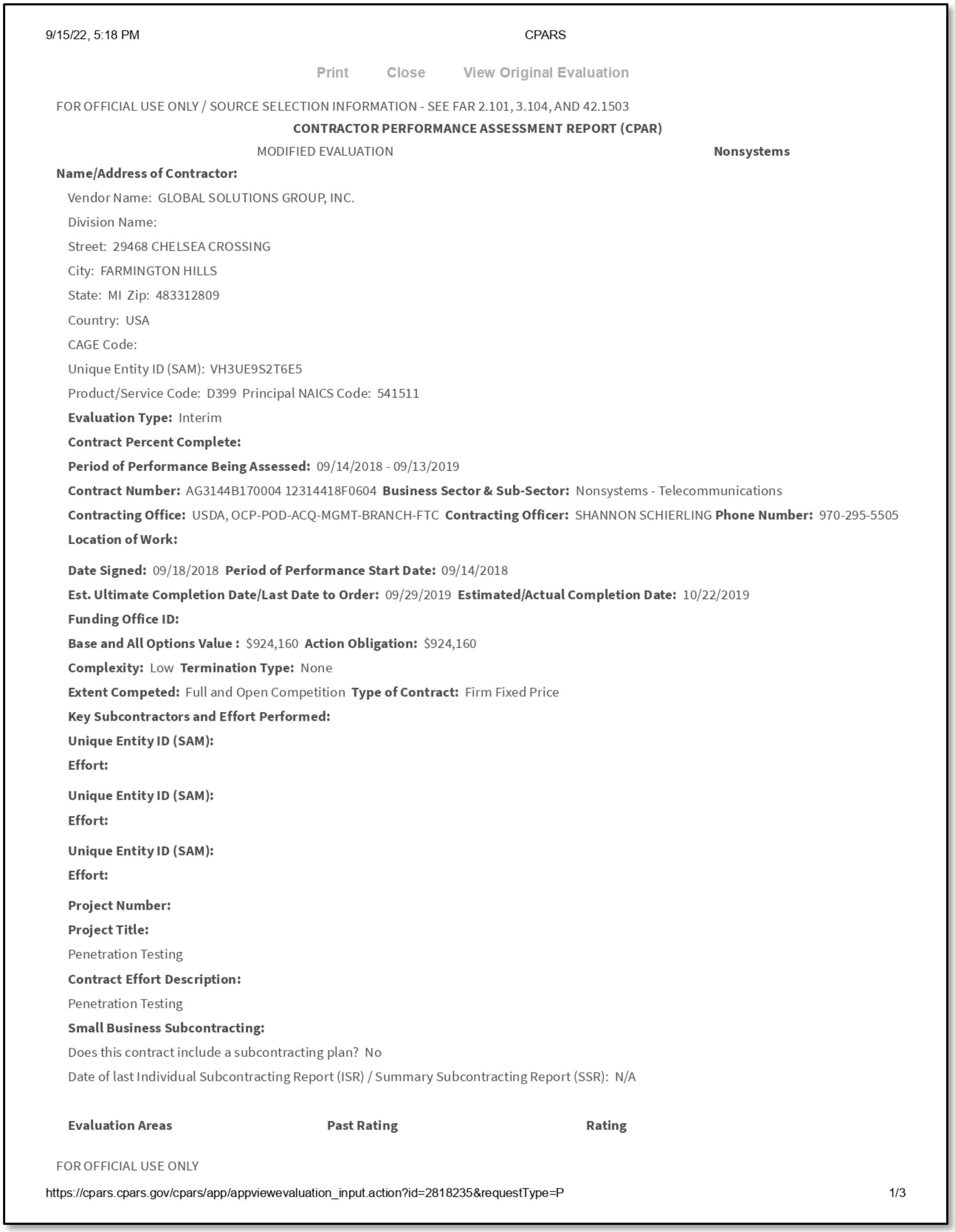
Date: 02/11/2020

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2844991&requestType=P 3/3

## 5.b.5 2019 Penetration Testing x0604

**Synopsis: Quality Exceptional**



9/15/22, 5:18 PM CPARS

Print Close View Original Evaluation

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)**

MODIFIED EVALUATION **Nonsystems**

**Name/Address of Contractor:**

Vendor Name: GLOBAL SOLUTIONS GROUP, INC.

Division Name:

Street: 29468 CHELSEA CROSSING

City: FARMINGTON HILLS

State: MI Zip: 483312809

Country: USA

CAGE Code:

Unique Entity ID (SAM): VH3UE9S2T6E5

Product/Service Code: D399 Principal NAICS Code: 541511

**Evaluation Type:** Interim

**Contract Percent Complete:**

**Period of Performance Being Assessed:** 09/14/2018 - 09/13/2019

**Contract Number:** AG3144B170004 12314418F0604 **Business Sector & Sub-Sector:** Nonsystems - Telecommunications

**Contracting Office:** USDA, OCP-POD-ACQ-MGMT-BRANCH-FTC **Contracting Officer:** SHANNON SCHIERLING **Phone Number:** 970-295-5505

**Location of Work:**

**Date Signed:** 09/18/2018 **Period of Performance Start Date:** 09/14/2018

**Est. Ultimate Completion Date/Last Date to Order:** 09/29/2019 **Estimated/Actual Completion Date:** 10/22/2019

**Funding Office ID:**

**Base and All Options Value :** $924,160 **Action Obligation:** $924,160

**Complexity:** Low **Termination Type:** None

**Extent Competed:** Full and Open Competition **Type of Contract:** Firm Fixed Price

**Key Subcontractors and Effort Performed:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Unique Entity ID (SAM):**

**Effort:**

**Project Number:**

**Project Title:**

Penetration Testing

**Contract Effort Description:**

Penetration Testing

**Small Business Subcontracting:**

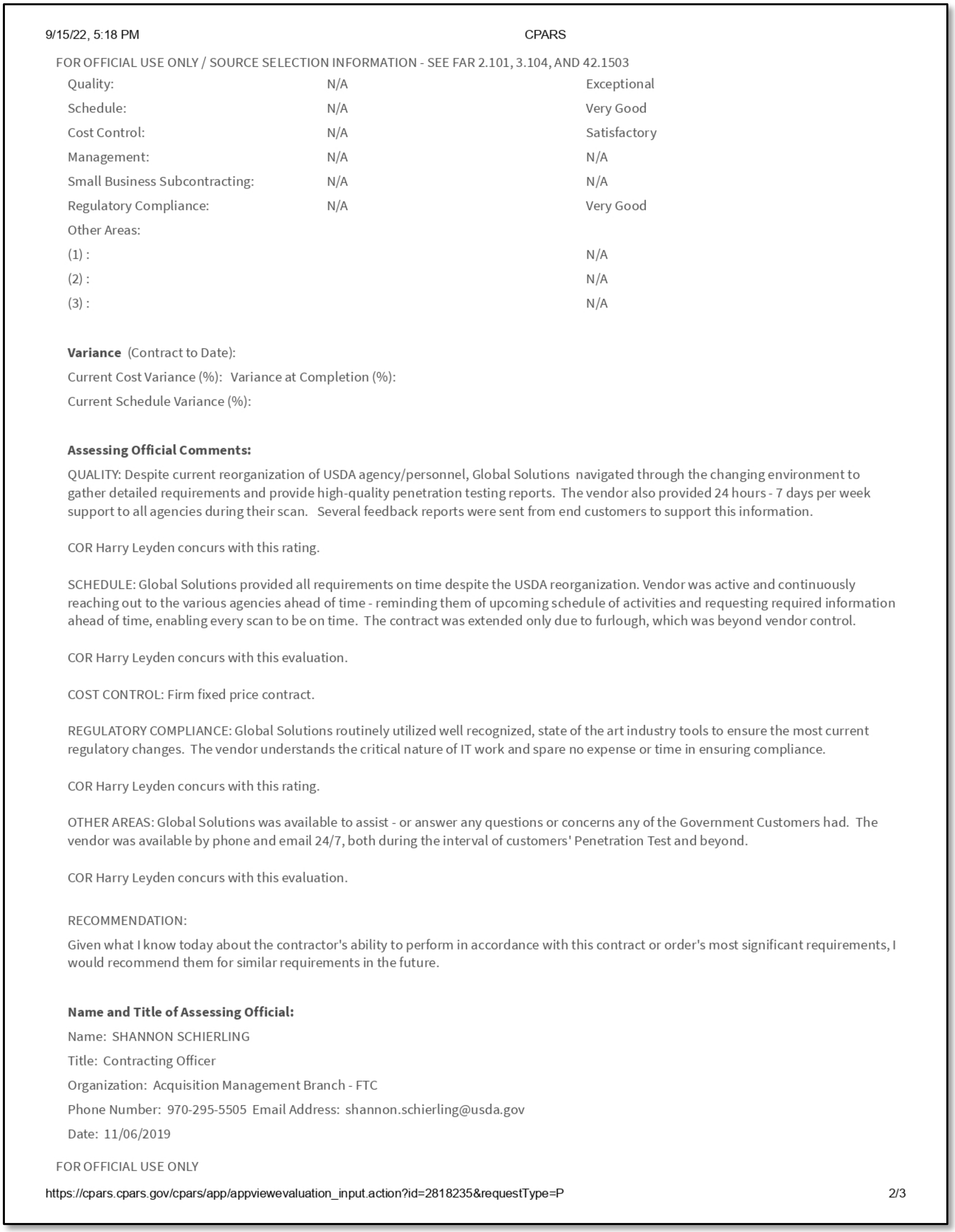
Does this contract include a subcontracting plan? No

Date of last Individual Subcontracting Report (ISR) / Summary Subcontracting Report (SSR): N/A

| Evaluation Areas | Past Rating | Rating |
|---|---|---|

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2818235&requestType=P 1/3



9/15/22, 5:18 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

| | | |
|---|---|---|
| Quality: | N/A | Exceptional |
| Schedule: | N/A | Very Good |
| Cost Control: | N/A | Satisfactory |
| Management: | N/A | N/A |
| Small Business Subcontracting: | N/A | N/A |
| Regulatory Compliance: | N/A | Very Good |
| Other Areas: | | |
| (1) : | | N/A |
| (2) : | | N/A |
| (3) : | | N/A |

**Variance** (Contract to Date):

Current Cost Variance (%): Variance at Completion (%):

Current Schedule Variance (%):

**Assessing Official Comments:**

QUALITY: Despite current reorganization of USDA agency/personnel, Global Solutions navigated through the changing environment to gather detailed requirements and provide high-quality penetration testing reports. The vendor also provided 24 hours - 7 days per week support to all agencies during their scan. Several feedback reports were sent from end customers to support this information.

COR Harry Leyden concurs with this rating.

SCHEDULE: Global Solutions provided all requirements on time despite the USDA reorganization. Vendor was active and continuously reaching out to the various agencies ahead of time - reminding them of upcoming schedule of activities and requesting required information ahead of time, enabling every scan to be on time. The contract was extended only due to furlough, which was beyond vendor control.

COR Harry Leyden concurs with this evaluation.

COST CONTROL: Firm fixed price contract.

REGULATORY COMPLIANCE: Global Solutions routinely utilized well recognized, state of the art industry tools to ensure the most current regulatory changes. The vendor understands the critical nature of IT work and spare no expense or time in ensuring compliance.

COR Harry Leyden concurs with this rating.

OTHER AREAS: Global Solutions was available to assist - or answer any questions or concerns any of the Government Customers had. The vendor was available by phone and email 24/7, both during the interval of customers' Penetration Test and beyond.

COR Harry Leyden concurs with this evaluation.

RECOMMENDATION:

Given what I know today about the contractor's ability to perform in accordance with this contract or order's most significant requirements, I would recommend them for similar requirements in the future.

**Name and Title of Assessing Official:**

Name: SHANNON SCHIERLING

Title: Contracting Officer

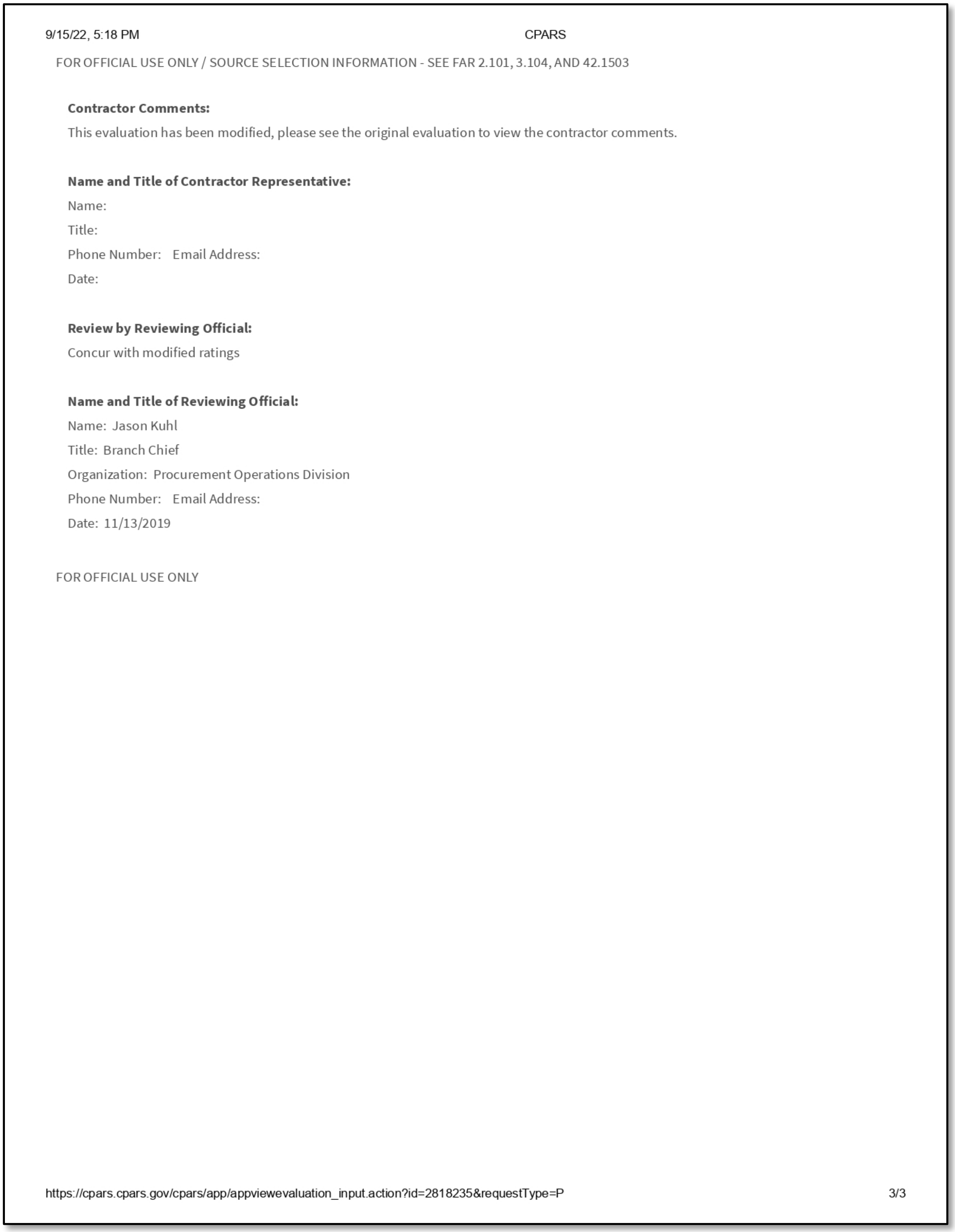
Organization: Acquisition Management Branch - FTC

Phone Number: 970-295-5505 Email Address: shannon.schierling@usda.gov

Date: 11/06/2019

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2818235&requestType=P 2/3



9/15/22, 5:18 PM CPARS

FOR OFFICIAL USE ONLY / SOURCE SELECTION INFORMATION - SEE FAR 2.101, 3.104, AND 42.1503

**Contractor Comments:**

This evaluation has been modified, please see the original evaluation to view the contractor comments.

**Name and Title of Contractor Representative:**

Name:

Title:

Phone Number: Email Address:

Date:

**Review by Reviewing Official:**

Concur with modified ratings

**Name and Title of Reviewing Official:**

Name: Jason Kuhl

Title: Branch Chief

Organization: Procurement Operations Division

Phone Number: Email Address:

Date: 11/13/2019

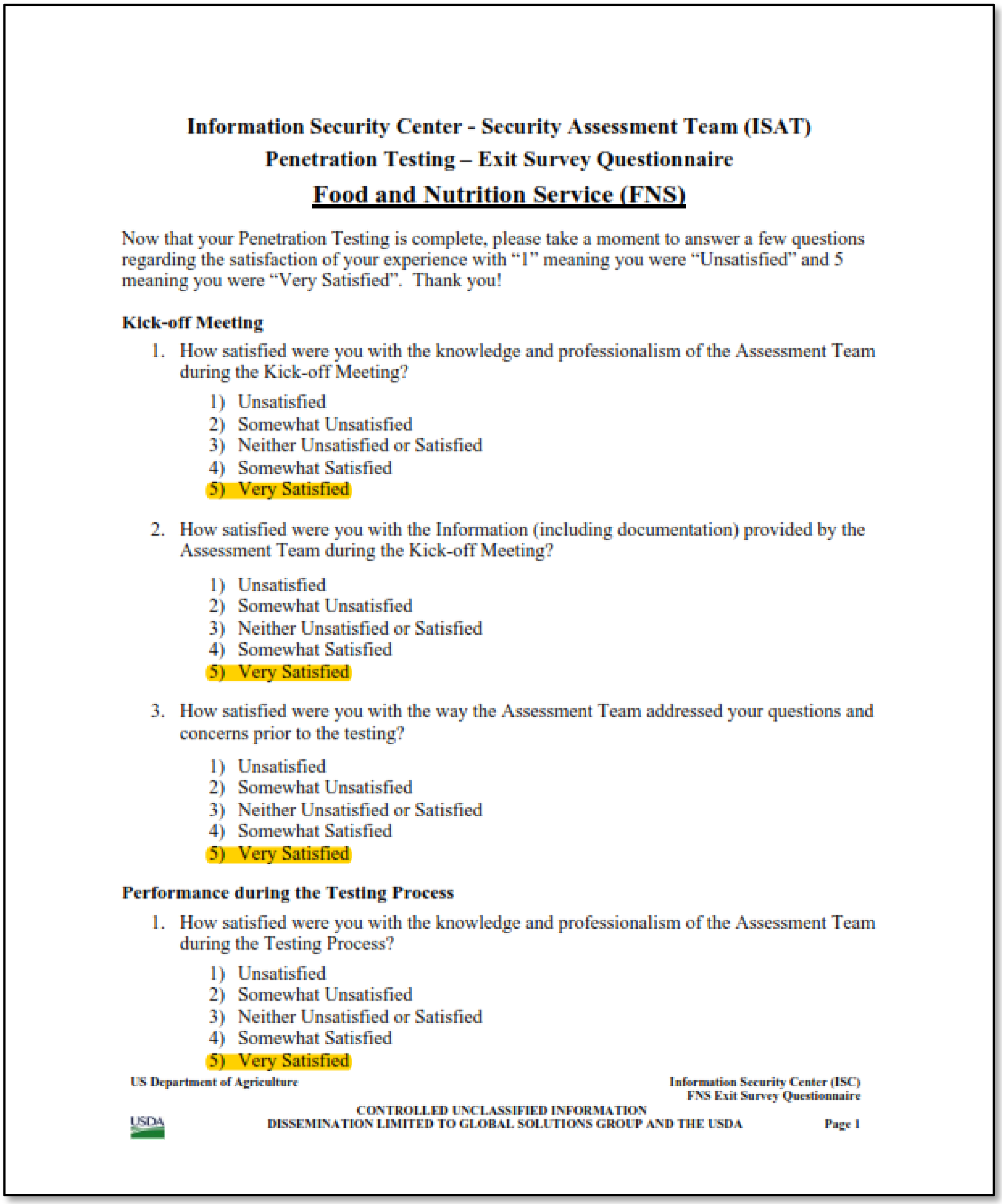
FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=2818235&requestType=P 3/3

## *c) Exit Surveys*

### 5.c.1 Food and Nutrition Service, Information Security Center, Security Assessment Team, Penetration Testing

**Synopsis: Very Satisfied (Maximum rating) in all categories**



**Information Security Center - Security Assessment Team (ISAT)**

**Penetration Testing – Exit Survey Questionnaire**

**Food and Nutrition Service (FNS)**

Now that your Penetration Testing is complete, please take a moment to answer a few questions regarding the satisfaction of your experience with "1" meaning you were "Unsatisfied" and 5 meaning you were "Very Satisfied". Thank you!

**Kick-off Meeting**

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Kick-off Meeting?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied

2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Kick-off Meeting?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied

3. How satisfied were you with the way the Assessment Team addressed your questions and concerns prior to the testing?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied

**Performance during the Testing Process**

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Testing Process?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied

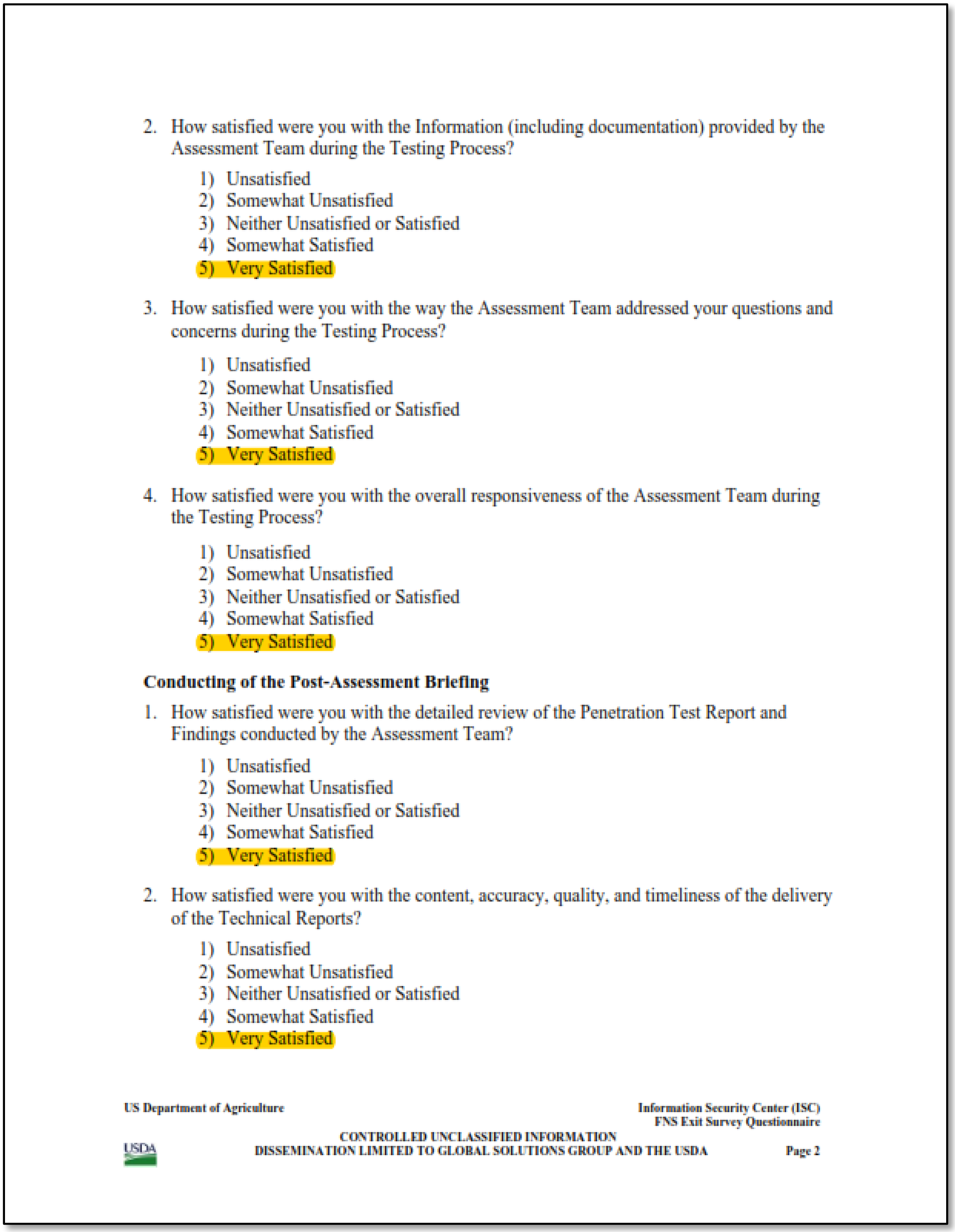
US Department of Agriculture

Information Security Center (ISC)
FNS Exit Survey Questionnaire

USDA

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

Page 1



2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Testing Process?

   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) [✓ Very Satisfied]

3. How satisfied were you with the way the Assessment Team addressed your questions and concerns during the Testing Process?

   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) [✓ Very Satisfied]

4. How satisfied were you with the overall responsiveness of the Assessment Team during the Testing Process?

   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) [✓ Very Satisfied]

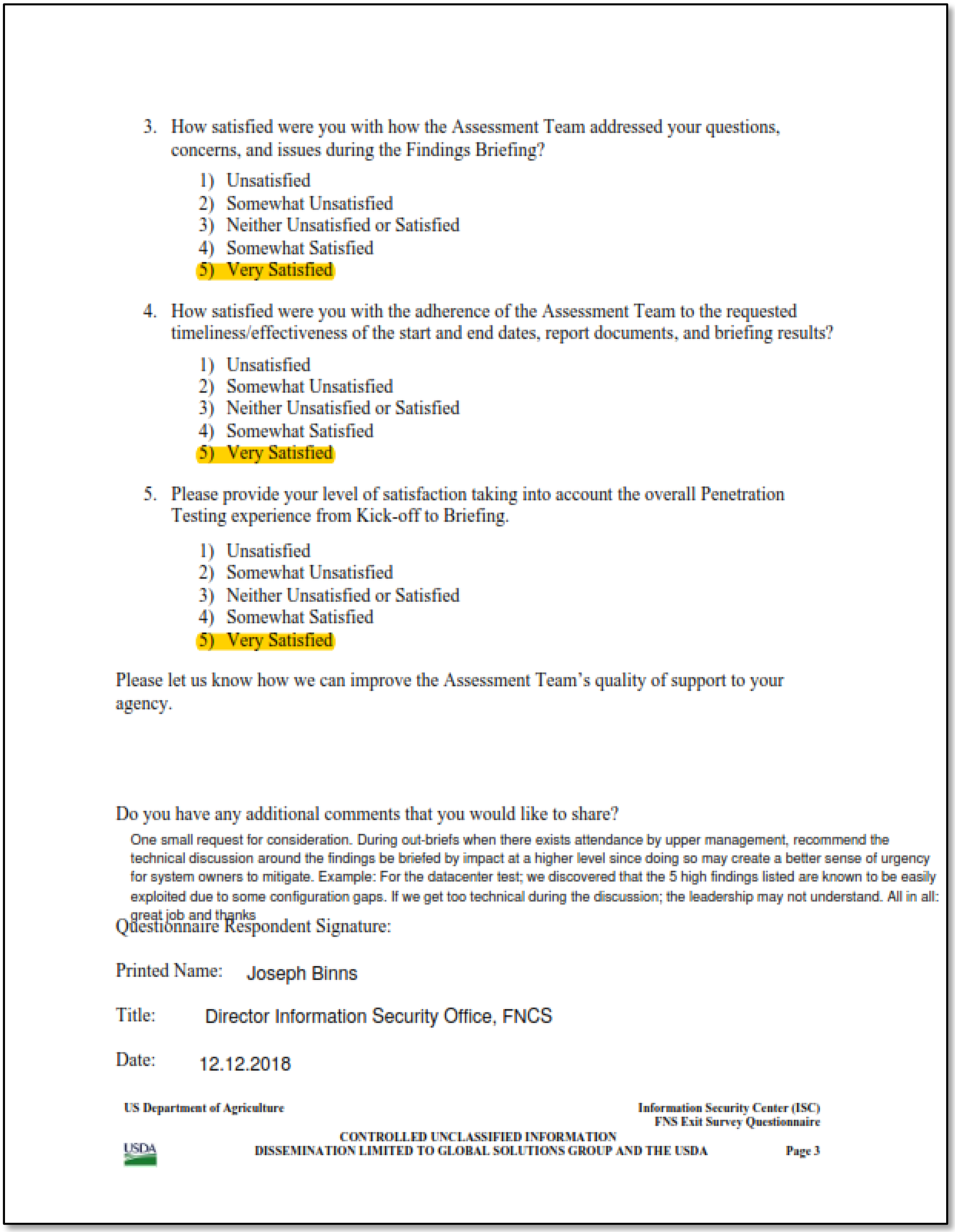
**Conducting of the Post-Assessment Briefing**

1. How satisfied were you with the detailed review of the Penetration Test Report and Findings conducted by the Assessment Team?

   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) [✓ Very Satisfied]

2. How satisfied were you with the content, accuracy, quality, and timeliness of the delivery of the Technical Reports?

   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) [✓ Very Satisfied]



3. How satisfied were you with how the Assessment Team addressed your questions, concerns, and issues during the Findings Briefing?
    1) Unsatisfied
    2) Somewhat Unsatisfied
    3) Neither Unsatisfied or Satisfied
    4) Somewhat Satisfied
    [✓ 5) Very Satisfied]

4. How satisfied were you with the adherence of the Assessment Team to the requested timeliness/effectiveness of the start and end dates, report documents, and briefing results?
    1) Unsatisfied
    2) Somewhat Unsatisfied
    3) Neither Unsatisfied or Satisfied
    4) Somewhat Satisfied
    [✓ 5) Very Satisfied]

5. Please provide your level of satisfaction taking into account the overall Penetration Testing experience from Kick-off to Briefing.
    1) Unsatisfied
    2) Somewhat Unsatisfied
    3) Neither Unsatisfied or Satisfied
    4) Somewhat Satisfied
    [✓ 5) Very Satisfied]

Please let us know how we can improve the Assessment Team's quality of support to your agency.

Do you have any additional comments that you would like to share?

One small request for consideration. During out-briefs when there exists attendance by upper management, recommend the technical discussion around the findings be briefed by impact at a higher level since doing so may create a better sense of urgency for system owners to mitigate. Example: For the datacenter test; we discovered that the 5 high findings listed are known to be easily exploited due to some configuration gaps. If we get too technical during the discussion; the leadership may not understand. All in all: great job and thanks

Questionnaire Respondent Signature:

Printed Name: Joseph Binns

Title: Director Information Security Office, FNCS

Date: 12.12.2018

US Department of Agriculture

Information Security Center (ISC)
FNS Exit Survey Questionnaire

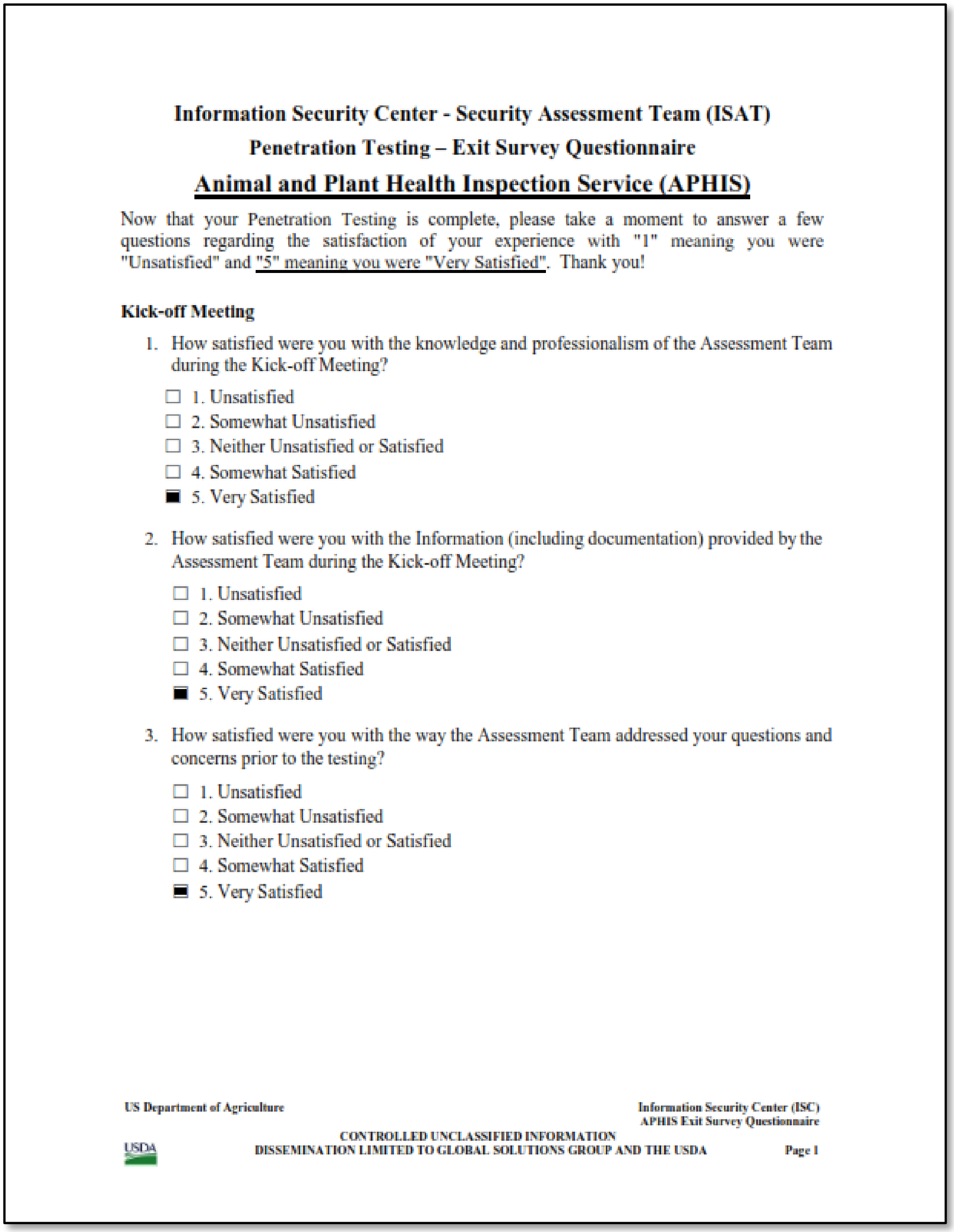
USDA

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

Page 3

## 5.c.2 APHIS - Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for Animal and Plant Health Inspection Service

**Synopsis: Very Satisfied (Maximum rating) in all categories**



**Information Security Center - Security Assessment Team (ISAT)**

**Penetration Testing – Exit Survey Questionnaire**

**Animal and Plant Health Inspection Service (APHIS)**

Now that your Penetration Testing is complete, please take a moment to answer a few questions regarding the satisfaction of your experience with "1" meaning you were "Unsatisfied" and "5" meaning you were "Very Satisfied". Thank you!

**Kick-off Meeting**

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Kick-off Meeting?

☐ 1. Unsatisfied
☐ 2. Somewhat Unsatisfied
☐ 3. Neither Unsatisfied or Satisfied
☐ 4. Somewhat Satisfied
■ 5. Very Satisfied

2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Kick-off Meeting?

☐ 1. Unsatisfied
☐ 2. Somewhat Unsatisfied
☐ 3. Neither Unsatisfied or Satisfied
☐ 4. Somewhat Satisfied
■ 5. Very Satisfied

3. How satisfied were you with the way the Assessment Team addressed your questions and concerns prior to the testing?

☐ 1. Unsatisfied
☐ 2. Somewhat Unsatisfied
☐ 3. Neither Unsatisfied or Satisfied
☐ 4. Somewhat Satisfied
■ 5. Very Satisfied

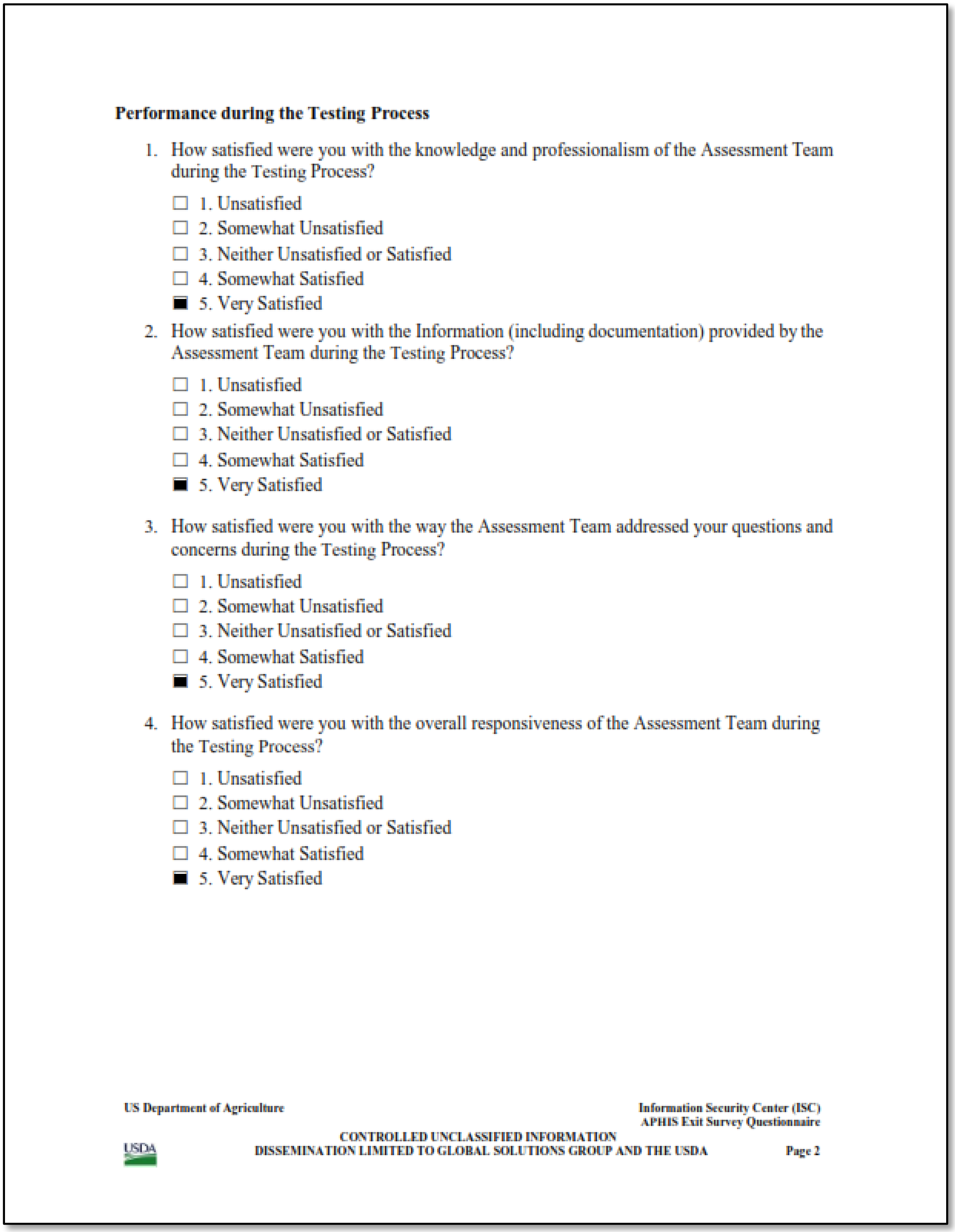
US Department of Agriculture

Information Security Center (ISC)
APHIS Exit Survey Questionnaire

USDA

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

Page 1



**Performance during the Testing Process**

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Testing Process?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Testing Process?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

3. How satisfied were you with the way the Assessment Team addressed your questions and concerns during the Testing Process?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

4. How satisfied were you with the overall responsiveness of the Assessment Team during the Testing Process?

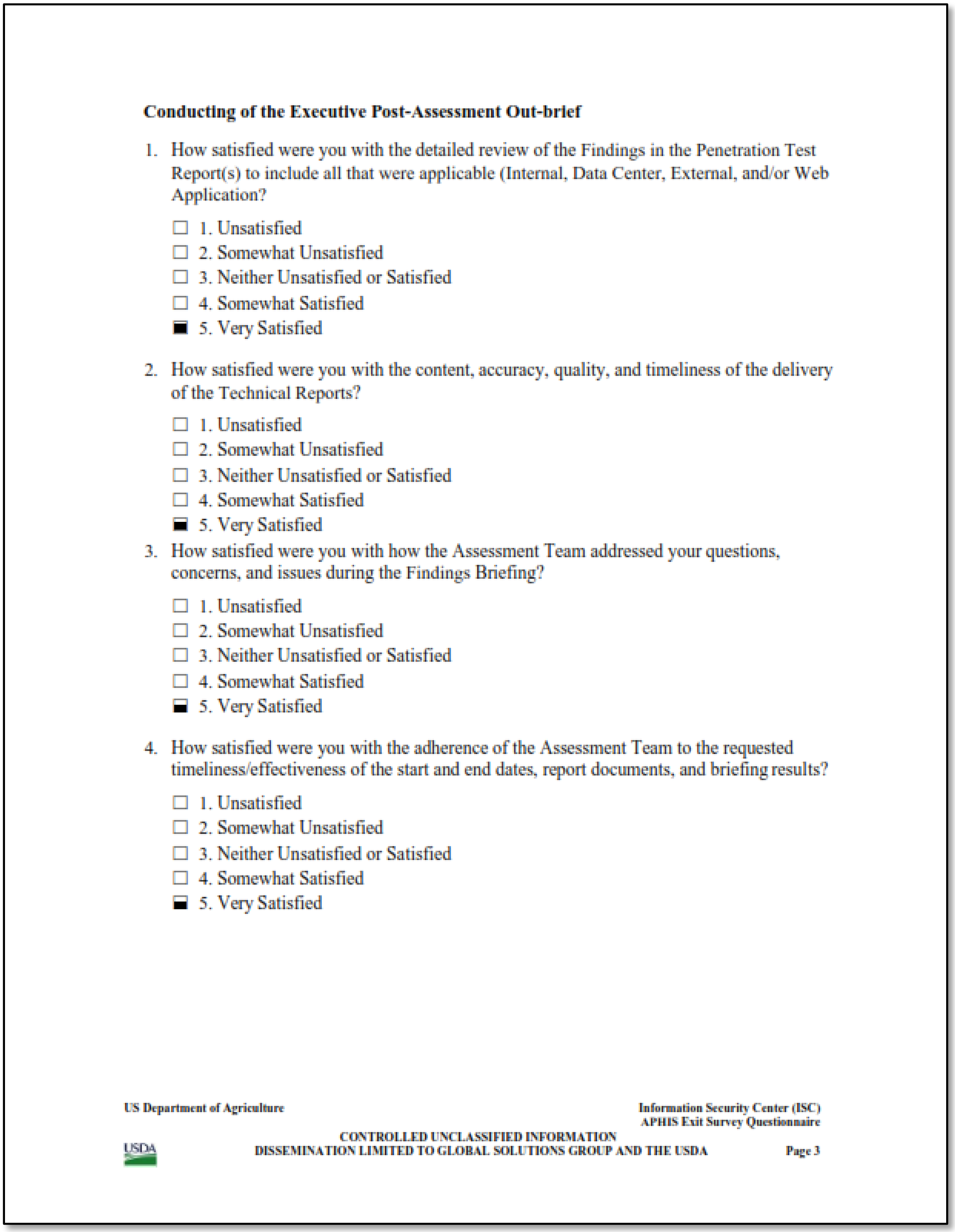
   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

US Department of Agriculture

Information Security Center (ISC)
APHIS Exit Survey Questionnaire

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

Page 2



**Conducting of the Executive Post-Assessment Out-brief**

1. How satisfied were you with the detailed review of the Findings in the Penetration Test Report(s) to include all that were applicable (Internal, Data Center, External, and/or Web Application?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

2. How satisfied were you with the content, accuracy, quality, and timeliness of the delivery of the Technical Reports?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

3. How satisfied were you with how the Assessment Team addressed your questions, concerns, and issues during the Findings Briefing?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

4. How satisfied were you with the adherence of the Assessment Team to the requested timeliness/effectiveness of the start and end dates, report documents, and briefing results?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

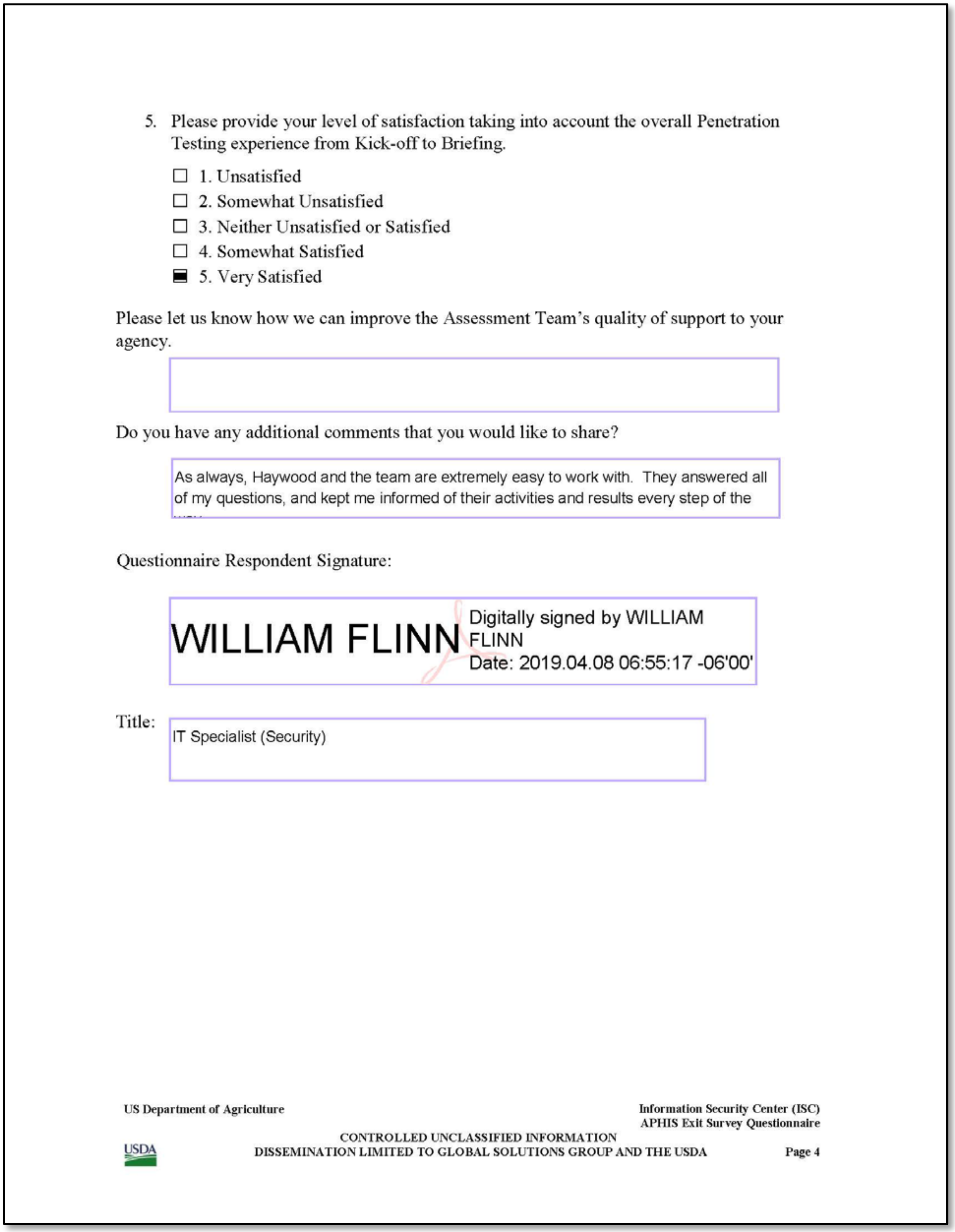
US Department of Agriculture

Information Security Center (ISC)
APHIS Exit Survey Questionnaire

USDA

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

Page 3



5. Please provide your level of satisfaction taking into account the overall Penetration Testing experience from Kick-off to Briefing.

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

Please let us know how we can improve the Assessment Team's quality of support to your agency.

Do you have any additional comments that you would like to share?

As always, Haywood and the team are extremely easy to work with. They answered all of my questions, and kept me informed of their activities and results every step of the

Questionnaire Respondent Signature:

WILLIAM FLINN Digitally signed by WILLIAM FLINN
Date: 2019.04.08 06:55:17 -06'00'

Title: IT Specialist (Security)

US Department of Agriculture

Information Security Center (ISC)
APHIS Exit Survey Questionnaire

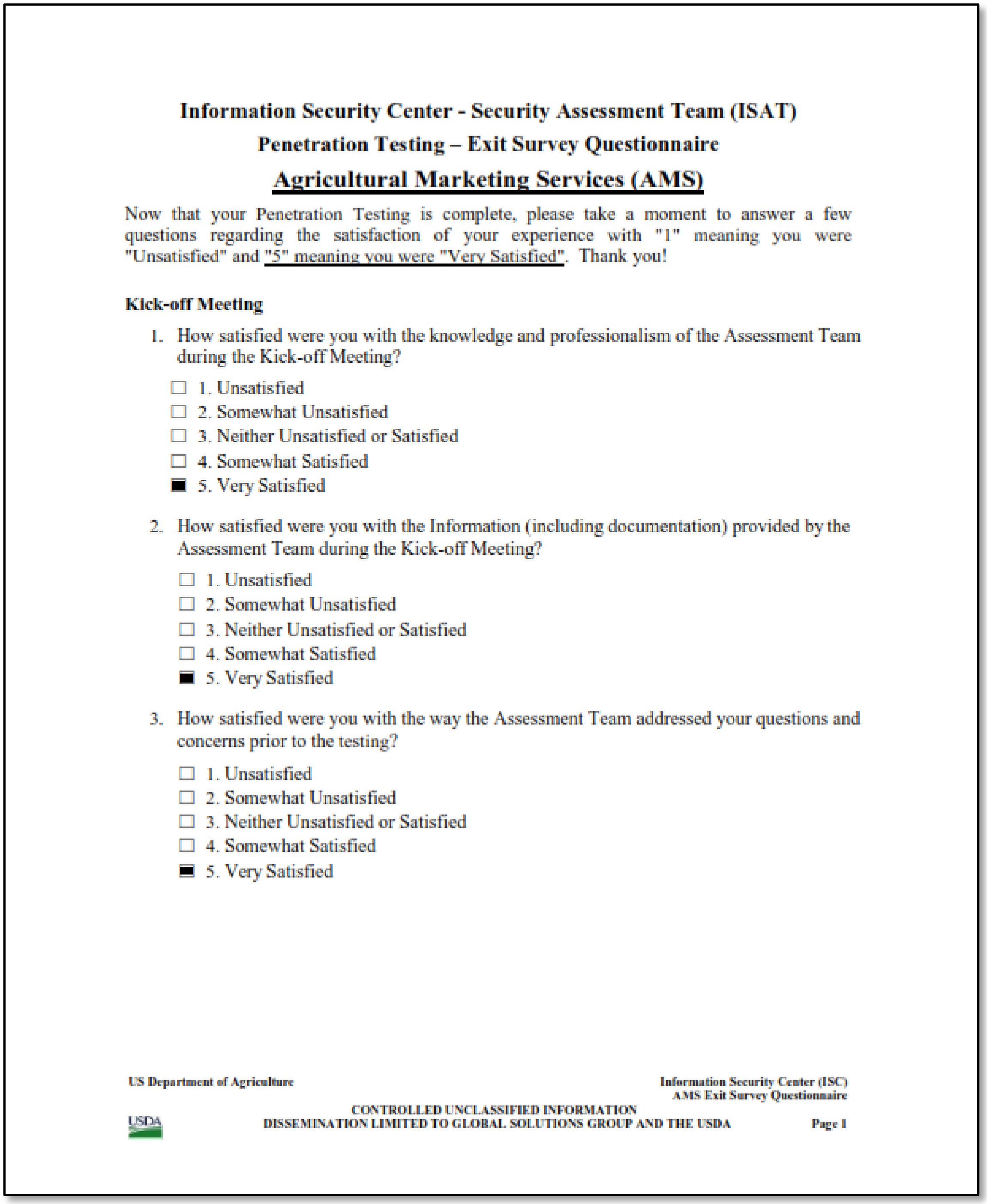
CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

USDA

Page 4

## 5.c.3 AMS - Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for Agriculture Marketing Services

**Synopsis: Very Satisfied (Maximum rating) in all categories**



### Information Security Center - Security Assessment Team (ISAT)
### Penetration Testing – Exit Survey Questionnaire
### Agricultural Marketing Services (AMS)

Now that your Penetration Testing is complete, please take a moment to answer a few questions regarding the satisfaction of your experience with "1" meaning you were "Unsatisfied" and "5" meaning you were "Very Satisfied". Thank you!

**Kick-off Meeting**

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Kick-off Meeting?

☐ 1. Unsatisfied
☐ 2. Somewhat Unsatisfied
☐ 3. Neither Unsatisfied or Satisfied
☐ 4. Somewhat Satisfied
■ 5. Very Satisfied

2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Kick-off Meeting?

☐ 1. Unsatisfied
☐ 2. Somewhat Unsatisfied
☐ 3. Neither Unsatisfied or Satisfied
☐ 4. Somewhat Satisfied
■ 5. Very Satisfied

3. How satisfied were you with the way the Assessment Team addressed your questions and concerns prior to the testing?

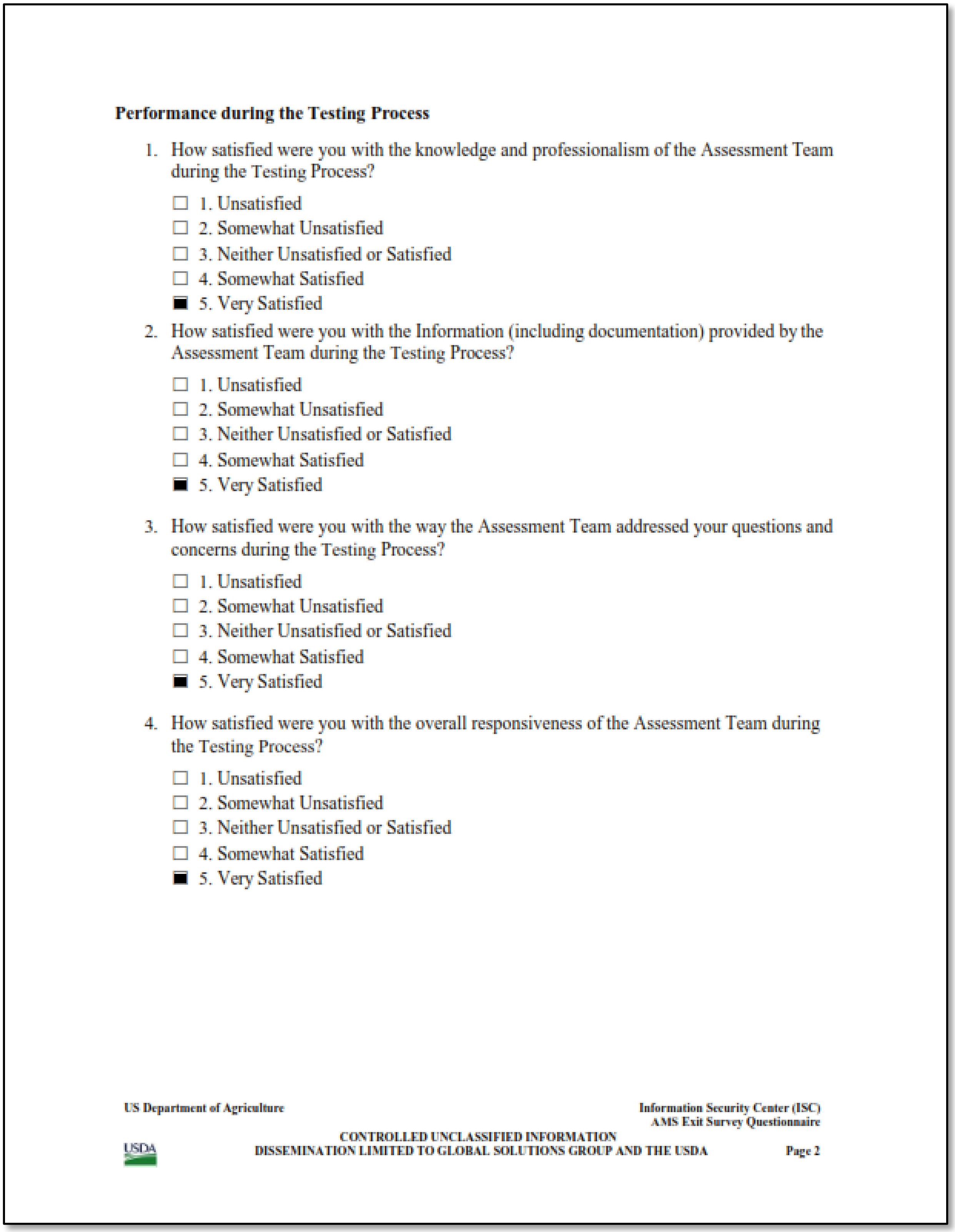
☐ 1. Unsatisfied
☐ 2. Somewhat Unsatisfied
☐ 3. Neither Unsatisfied or Satisfied
☐ 4. Somewhat Satisfied
■ 5. Very Satisfied

US Department of Agriculture

Information Security Center (ISC)
AMS Exit Survey Questionnaire

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

Page 1



**Performance during the Testing Process**

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Testing Process?

   ☐ 1. Unsatisfied
   ☐ 2. Somewhat Unsatisfied
   ☐ 3. Neither Unsatisfied or Satisfied
   ☐ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Testing Process?

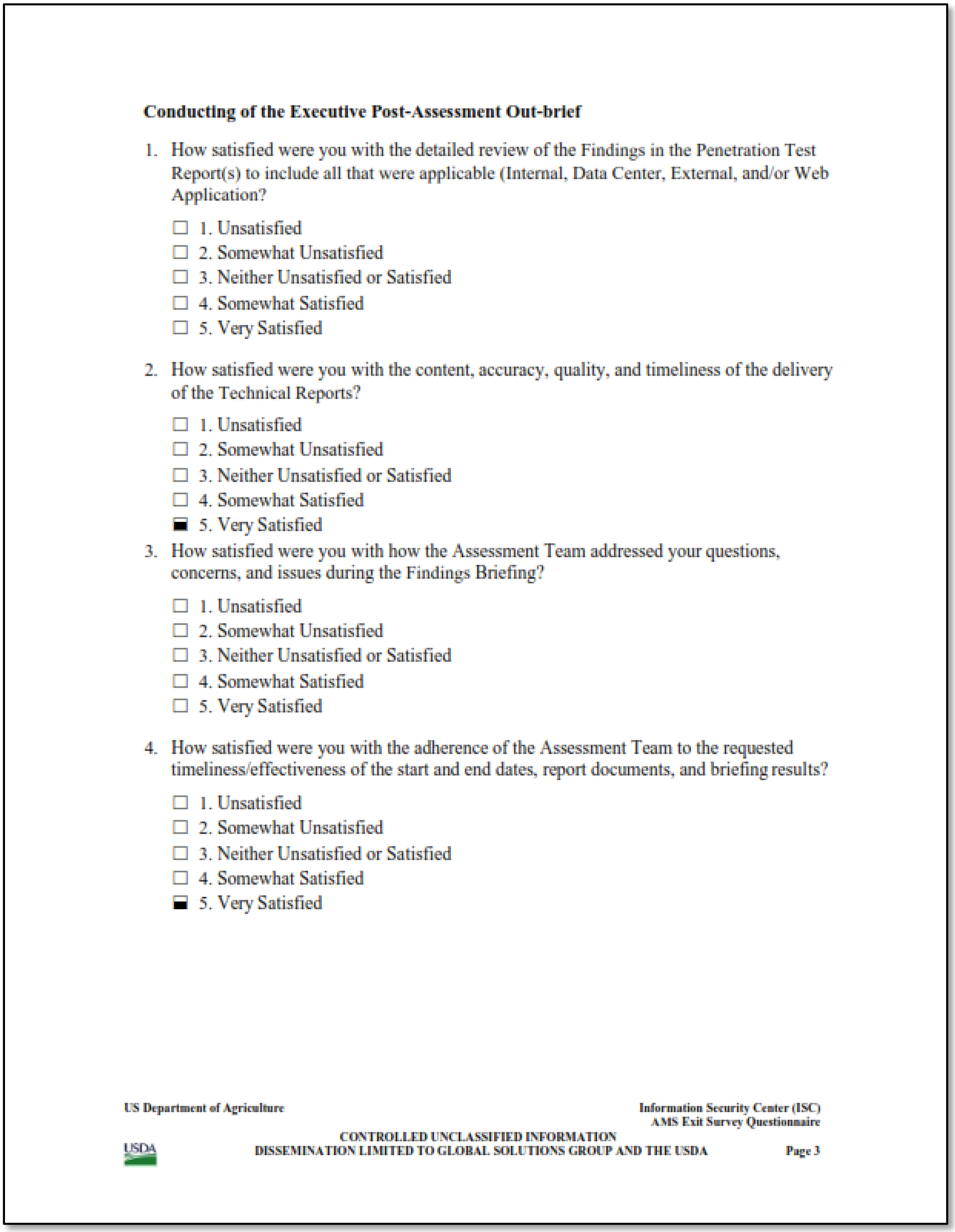
   ☐ 1. Unsatisfied
   ☐ 2. Somewhat Unsatisfied
   ☐ 3. Neither Unsatisfied or Satisfied
   ☐ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

3. How satisfied were you with the way the Assessment Team addressed your questions and concerns during the Testing Process?

   ☐ 1. Unsatisfied
   ☐ 2. Somewhat Unsatisfied
   ☐ 3. Neither Unsatisfied or Satisfied
   ☐ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

4. How satisfied were you with the overall responsiveness of the Assessment Team during the Testing Process?

   ☐ 1. Unsatisfied
   ☐ 2. Somewhat Unsatisfied
   ☐ 3. Neither Unsatisfied or Satisfied
   ☐ 4. Somewhat Satisfied
   ■ 5. Very Satisfied



**Conducting of the Executive Post-Assessment Out-brief**

1. How satisfied were you with the detailed review of the Findings in the Penetration Test Report(s) to include all that were applicable (Internal, Data Center, External, and/or Web Application?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   □ 5. Very Satisfied

2. How satisfied were you with the content, accuracy, quality, and timeliness of the delivery of the Technical Reports?

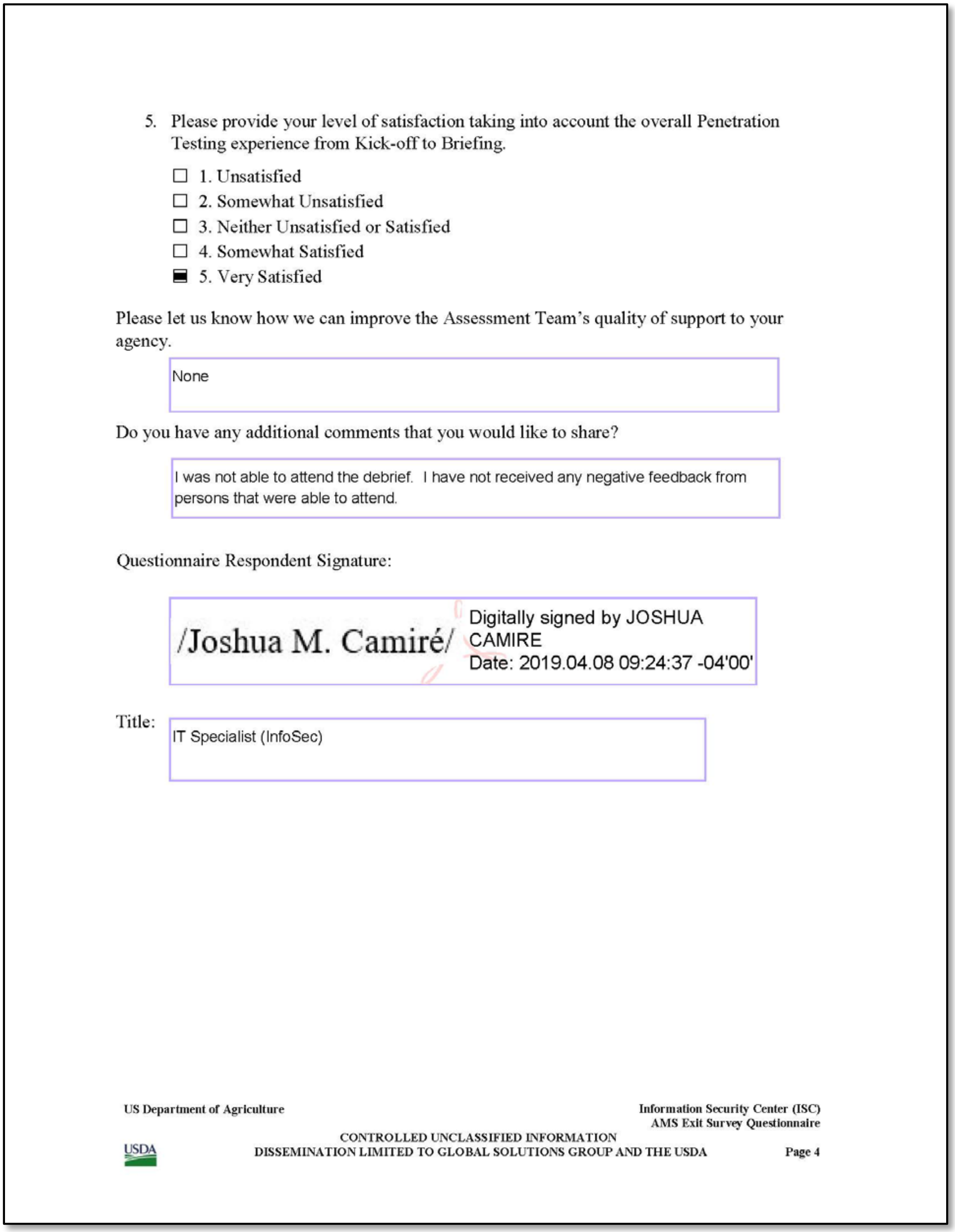
   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

3. How satisfied were you with how the Assessment Team addressed your questions, concerns, and issues during the Findings Briefing?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   □ 5. Very Satisfied

4. How satisfied were you with the adherence of the Assessment Team to the requested timeliness/effectiveness of the start and end dates, report documents, and briefing results?

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied



5. Please provide your level of satisfaction taking into account the overall Penetration Testing experience from Kick-off to Briefing.

   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

Please let us know how we can improve the Assessment Team's quality of support to your agency.

None

Do you have any additional comments that you would like to share?

I was not able to attend the debrief. I have not received any negative feedback from persons that were able to attend.

Questionnaire Respondent Signature:

/Joshua M. Camiré/ Digitally signed by JOSHUA CAMIRE
Date: 2019.04.08 09:24:37 -04'00'

Title: IT Specialist (InfoSec)

# GLOBAL

SOLUTIONS GROUP, INC.

FORTINET
AUTHORIZED PARTNER

ORACLE
PARTNERNETWORK

MANDIANT

IBM
PartnerWorld

CISCO
Partner

Microsoft
Gold Partner

MICRO FOCUS
BUSINESS PARTNER

Trellix

tenable

Laserfiche

amazon webservices
Partner Network

## Evaluation of  Information Technology Management Services and Cybersecurity Assessment Services

| MileStone Description | Number of Devices | Monthly Hours | Annual Hours | Hourly Rate | Year 1 | Year 2 | Option Year 1 | Option Year 2 | Total Cost - 4 Years |
|---|---|---|---|---|---|---|---|---|---|
| **Information Technology Management Services** | | | | | | | | | |
| **Option A - Small Size Municipal Agency / Department**** | | **50** | **600** | **$ 75** | **$ 45,000.00** | **$ 45,900.00** | **$ 46,818.00** | **$ 47,754.36** | **$ 185,472.36** |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | **Up to 25 endpoints /  2 firewalls  / 10 network devices** | 8 | 96 | | | | | | |
| (B) Proactive monitoring and alerts; | | 10 | 120 | | | | | | |
| (C) On-site and remote support services; | | 15 | 180 | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | 10 | 120 | | | | | | |
| (E) and on-call infrastructure professionals | | 7 | 84 | | | | | | |
| **Option B - Medium Size Municipal  Municipal Agency / Department**** | | **100** | **1200** | **$ 75** | **$ 90,000.00** | **$ 91,800.00** | **$ 93,636.00** | **$ 95,508.72** | **$ 370,944.72** |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | **Up to 100 endpoints / 3 firewalls /  25 network devices** | 16 | 192 | | | | | | |
| (B) Proactive monitoring and alerts; | | 20 | 240 | | | | | | |
| (C) On-site and remote support services; | | 32 | 384 | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | 20 | 240 | | | | | | |
| (E) and on-call infrastructure professionals | | 12 | 144 | | | | | | |
| **Option C - Large Size Municipal Agency / Department**** | | **160** | **1920** | **$ 75** | **$ 144,000.00** | **$ 146,880.00** | **$ 149,817.60** | **$ 152,813.95** | **$ 593,511.55** |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | **Up to  250 endpoints / 5  firewalls / 40 network devices** | 25 | 300 | | | | | | |
| (B) Proactive monitoring and alerts; | | 24 | 288 | | | | | | |
| (C) On-site and remote support services; | | 45 | 540 | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | 30 | 360 | | | | | | |
| (E) and on-call infrastructure professionals | | 16 | 192 | | | | | | |
| **Option D - Extra Large Size Municipal Agency / Department**** | | **160 Hours + additional hours as needed** | **1920 Hours + additional hours as needed** | **$ 75** | **As Needed** | **As Needed** | **As Needed** | **As Needed** | **As Needed** |
| (A) Management of firewalls, anti-virus, anti-malware, and threat identification; | **Above 250 endpoints / 5  firewalls / 40 network devices** | | | | | | | | |
| (B) Proactive monitoring and alerts; | | | | | | | | | |
| (C) On-site and remote support services; | | | | | | | | | |
| (D) Private, hybrid, and public cloud options; and | | | | | | | | | |
| (E) and on-call infrastructure professionals | | | | | | | | | |
| | | | | | | | | | |
| **On-Demand Services***** | | | | | | | | | |
| 1. Consultation (Remote, for onsite - travel charges will be additional) | IT/Network Consulting (Intermediate Level Resource) | - | - | $ 50 | TBD | TBD | TBD | TBD | TBD |
| | IT/Network Consulting (Senior/SME Level Resource) | - | - | $ 95 | TBD | TBD | TBD | TBD | TBD |
| 2. Small-scale testing services, as needed, to augment ongoing audits or testing | QA Testing (Intermediate Level Resource) | - | - | $ 60 | As per scope | As per scope | As per scope | As per scope | As per scope |
| | QA Testing (Senior/SME Level Resource) | - | - | $ 90 | As per scope | As per scope | As per scope | As per scope | As per scope |
| 3. Ability to use firm during normal business hours | | | | | Yes | Yes | Yes | Yes | Yes |
| | | | | | | | | | |
| **Cybersecurity Assessment Services** | | | | | | | | | |
| **Option A - Small Size Municipal Agency / Department**** | | **N/A** | **160** | **$ 124** | **$ 19,840.00** | **$ 20,236.80** | **$ 20,641.54** | **$ 21,054.37** | **$ 81,772.70** |
| (A) Independent view of current information technology security measures; | **Up to 200 devices (network and endpoints)** | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **Option B - Medium Size Municipal Agency / Department**** | | **N/A** | **240** | **$ 124** | **$ 29,760.00** | **$ 30,355.20** | **$ 30,962.30** | **$ 31,581.55** | **$ 122,659.05** |
| (A) Independent view of current information technology security measures; | **Up to 500 devices (network and endpoints)** | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **Option C - Large Size Municipal Agency / Department**** | | **N/A** | **480** | **$ 124** | **$ 59,520.00** | **$ 60,710.40** | **$ 61,924.61** | **$ 63,163.10** | **$ 245,318.11** |
| (A) Independent view of current information technology security measures; | **Up to 1000 devices (network and endpoints)** | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **Option D - Extra Large Size Municipal Agency / Department**** | | **N/A** | **480 Hours + additional hours as needed** | **$ 124** | **As Needed** | **As Needed** | **As Needed** | **As Needed** | **As Needed** |
| (A) Independent view of current information technology security measures; | **Above 1000 devices (network and endpoints)** | | | | | | | | |
| (B) Recommendations for modified information security measures based upon stated priorities and identified vulnerabilities; | | | | | | | | | |
| (C) Recommendations for improving short-term and long-term planning to increase information technology security; | | | | | | | | | |
| (D) Recommendations for information security best practices; and | | | | | | | | | |
| (E) Assistance with implementation of sections 2(a)(2)(B)to 2(a)(2)(D). | | | | | | | | | |
| **On-Demand Services***** | | | | | | | | | |
| 1. Consultation (Remote, for onsite - travel charges will be additional) | Cybersecurity Consulting (Intermediate Level Resource) | - | - | $ 85 | TBD | TBD | TBD | TBD | TBD |
| | Cybersecurity Consulting (Senior/SME Level Resource) | - | - | $ 125 | TBD | TBD | TBD | TBD | TBD |
| 2. Small-scale testing services, as needed, to augment ongoing audits or testing | Cybersecurity Audit (Intermediate Level Resource) | - | - | $ 90 | As per scope | As per scope | As per scope | As per scope | As per scope |
| | Cybersecurity Audit (Senior/SME Level Resource) | - | - | $ 124 | As per scope | As per scope | As per scope | As per scope | As per scope |
| 3. Ability to use firm during normal business hours | | | | | Yes | Yes | Yes | Yes | Yes |
| **Optional Cost - Estimated Travel Cost (1 Trip - 3 to 4 days) - If required** | | | | | **TBD** | **TBD** | **TBD** | | **TBD** |
| **Total Cost (Varies based upon selected options)** | | | | | **TBD** | **TBD** | **TBD** | | **TBD** |

**Payment Schedule:**
**IT Management Services**  -GSG will invoice the appropriate amount on a monthly basis.
**Cybersecurity Assessment Services -** GSG will accept a 100% services fee invoice upon acceptance of all final deliverables.

**Assumptions:**

** Due to lack of exact assets/network devices information about each Municipal Agency / Department, GSG would like to propose total  **FOUR Options** for both "Information Technology Management Services" and "Cybersecurity Assessment Services" based upon the size/scope of each Municipal Agency / Department.  Each Option for Municipal Agency / Department size included with ceiling limits from numbers of network devices/endpoints.  However, if these options are not the best fit then we are open to consider other options as well.  Above hours are based upon scope and clarification response provided in RFP and Q&A document. If any of the scope and/or quantities of devices increases then our effort will be increased appropriately.

**IT Management Services - Hours Break-down**
**Option A** -We have estimated **50 hours** on a monthly basis for a Small agency with specified devices  Up to **25 endpoints, 2 firewalls, and 10 network devices.**
**Option B** -We have estimated **100 hours** on a monthly basis for a  Medium agency with specified devices Up to  **100 endpoints, 3 firewalls, and 25 network devices.**
**Option C** -We have estimated **160 hours** on a monthly basis for a Large Agency with specified devices Up to  **250 endpoints, 5  firewalls, and 40 network devices.**
**Option D** -We have estimated **160 Hours + additional hours as needed** on a monthly basis for an Extra Large Agency with specified devices  Above **250 endpoints, 5  firewalls, and 40 network devices.**

**Cybersecurity Assessment Services - Hours Break-down**
**Option A** -  We have estimated a one-time effort of **160 hours** for a Small Agency with specified devices Up to a total of **200 devices (network and endpoints)**.
**Option B** -  We have estimated a one-time effort of  **240 hours** for a Medium Agency with specified devices Up to a total of **500 devices (network and endpoints).**
**Option C** -  We have estimated a one-time effort of  **480 hours** for a  Large  Agency with specified devices Up to a total of **1000 devices (network and endpoints).**
**Option D** -  We have estimated a one-time effort of  **480 Hours + additional hours as a needed base** for an Extra Large Agency with specified devices Above **1000 devices (network and endpoints).**

**Note:**
Based upon understanding from RFP and Q&A, GSG proposes an estimated number of hours for different tasks and support categories. Our price will increase prorated if there is an increase in the total number of supported endpoints, servers, network devices, and/or users. If total number of monthly hours exceeds than estimated hours then it will be charged as an additional cost as per the billable hourly rate.

*** For "On-Demand Services", we are providing hourly rate for "Consultation" OR "Small-scale testing services" on an as-needed basis to augment ongoing audits or testing for Years 1, 2, 3, and 4.  We also agree to provide our resources during normal business hours. All services will be remote. However, if onsite services is required then travel cost will be an additional cost.

As part of our proposed cost for on-site support resources, GSG propose a local Michigan area resources with as-needed onsite hours on a monthly basis. These additional travels to the customer site, however, will incur a  comprehensive onsite cost of $150/trip/day/person for any customer within the Detroit Metropolitan Area, and $300/trip/day/person for any customer outside of the Detroit Metropolitan Area but within the State of Michigan. Any onsite trip outside of normal business hours will be charged at 1.5 times the regular bill rate of the appropriate resource.

Our proposed billing rate includes pay and benefit towards holiday, vacation, and various health insurance in order to attract and retain skilled and experienced talent. However, this above proposed cost doesn't include any onsite travel-related cost, software license, hardware, equipment, network device or any other item that is specifically required for this project and it will be an additional cost as an actual cost.

GSG team has large pool of resources based in Michigan for all offered services including IT, Network, and Cybersecurity technical team and we are planning to propose 2-4 resources team for each Municipal Agency / Department depending upon various criteria including scope of work, number of covered assets/endpoints/devices, budget, project schedule, stakeholder availability, etc.   Some tasks may be accomplished in parallel depending upon information, systems and stakeholders' availability.

For effective project scheduling, the Authority management needs to provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project and all the Authority stakeholders should be available as needed to ensure the timeliness and success of this project.

| |
|---|
| The Authority will provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project. |
| During this engagement, any vulnerabilities, sensitive data, or configuration data found will not be disclosed except to specified the Authority staff. |
| During this effort, GSG will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between the Authority and third parties. |
| The Authority management will ensure that appropriate personnel are available to meet with the GSG team, as necessary to ensure the success of this project. |
| GSG will not be accountable when delays result from the Authority's inability to meet stated prerequisites prior to an engagement, nor when delays result from the Authority personnel not being available to provide the required support for the success of this project. |
| The proposal will be valid for 90 days. |

Guidehouse
Outwit Complexity

Michigan Municipal Services Authority
Solicitation #RFP 2023-1

# Information Technology Managed Services and Cybersecurity Assessment Services

August 21, 2023

| Provided to: | Provided by: |
|---|---|
| Michigan Municipal Services Authority<br>Samantha Harkins<br>Chief Executive Officer<br>ceo@michiganmsa.gov | Guidehouse Inc.<br>Jeffrey Bankowski<br>Partner<br>1676 International Drive, Suite 800<br>McLean, VA 22102<br>Telephone (734) 644-0595<br>jbankowski@guidehouse.com<br>www.guidehouse.com<br><br>Taxpayer Identification Number (TIN): 36-4094854<br>SAM Unique Entity ID: N9NJK877QJK9<br>Commercial and Government Entity (CAGE) Code: 1HLR9 |

guidehouse.com

2023-530

Guidehouse
Outwit *Complexity*

This proposal includes data that is proprietary and confidential to Guidehouse and shall not be disclosed outside the recipient's organization and shall not be duplicated, used, or disclosed, in whole or in part, for any purpose other than to evaluate this proposal. However, if a contract is awarded to this offeror as a result of, or in connection with, the submission of these data, the recipient shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the recipient's right to use information contained in these data if they are obtained from another source without restriction. The data subject to this restriction are contained in specified pages/sheets herein.

This proposal does not constitute a contract to perform services and cannot be used to award a unilateral agreement. Final acceptance of this engagement by Guidehouse is contingent upon successful completion of Guidehouse’s acceptance procedures. Any engagement arising out of this proposal will be subject to negotiation of a mutually satisfactory engagement contract including modifications to certain RFP terms and conditions and including our standard terms and conditions and fees and billing rates established therein.

Guidehouse
Outwit *Complexity*

August 21, 2023

Michigan Municipal Services Authority

Samantha Harkins

Chief Executive Officer

ceo@michiganmsa.gov

Subject: Solicitation #RFP 2023-1 | Information Technology Managed Services and Cybersecurity Assessment Services

Dear Ms. Harkins:

Guidehouse Inc. (Guidehouse) is pleased to submit to the Michigan Municipal Services Authority (the Authority) our proposal to provide technology management and cybersecurity assessment services. We are confident that you will find that our proposal offers the best value solution to the Authority.

Guidehouse is a leading global provider of consulting services to the public sector and commercial markets, with broad capabilities in management, technology, and risk consulting. By combining our public and private sector expertise, we help clients address their most complex challenges and navigate significant regulatory pressures focusing on transformational change, business resiliency, and technology-driven innovation. Across a range of advisory, consulting, outsourcing, and digital services, we create scalable, innovative solutions that help our clients outwit complexity and position them for future growth and success. The company has more than 16,500 professionals in over 50 locations globally. Guidehouse is a Veritas Capital portfolio company, led by seasoned professionals with proven and diverse expertise in traditional and emerging technologies, markets, and agenda-setting issues driving national and global economies. For more information, please visit www.guidehouse.com.

Guidehouse appreciates the opportunity to be considered for this important project and if selected, will provide the Authority with a team of professionals committed to your success. If you have any questions about our response, please contact Contracts, Virginia Boyd, at (512) 402-3954 (slgcontracts@guidehouse.com) or me at (734) 644-0595 (jbankowski@guidehouse.com).

Sincerely,

Jeffrey Bankowski

Partner

# Table of Contents

## List of Figures

## List of Tables

## 1.0 Overview

At Guidehouse, we combine unequaled expertise, specialized resources, and deep domain experience to solve problems that cross sectors, industries, and geographies for clients of the public sector and the regulated commercial markets they serve. Guidehouse is the only scaled consultancy in the world to fully integrate commercial and public or government businesses within each of our industry segments because complex problems require both perspectives to address and outwit. Our public sector work extends across a broad spectrum of clients where we have performed successfully and gained the expertise necessary to make the engagement a success. **Our firm's guiding principle – building trust in society by solving complex problems –** defines who we are and is particularly relevant as we prepare to work with the Authority. We take our guiding principle to heart, every day, working side by side with our clients to solve their most challenging problems.

Guidehouse is highly qualified to assist Michigan Municipal Services Authority with **both managed services and cybersecurity assessment services** and already has significant experience conducting cyber security services including program level assessments, implementing technical solutions, and conducting cyber security trainings. Our cybersecurity professionals have multiple industry certifications including CISSP (Certified Information Systems Security Professionals). Guidehouse partners with its clients to assess, design, implement and train on robust security practices. Guidehouse has worked with several large and vertically integrated government entities such as Los Angeles Department of Water and Power, California Department of Water Resources, and New York Power Authority to make program level assessments, implement enhancements, and establish sustainable knowledge management and training programs. Further, across these areas, the Guidehouse team has worked with international entities such Dubai Electric and Water Authority, Abu Dhabi Distribution Company and Puerto Rico to make enterprise level cybersecurity improvements.

**The Guidehouse team has recognized industry and reliability compliance experts.** Our team has cybersecurity experts, not just in utilities and energy industry but also in healthcare and finance industries given a unique broad range of cyber security experience that is unmatched. Given our diverse cyber security experience, we are confident we can fully support the Authority in attaining its overall cyber security program development goals. We bring a customer-focused approach aligned to your strategic objectives. We are not beholden to any specific system, tool, or product vendors. Our objective is to understand your business, and drive optimal enabling solutions, rather than forcing your business to adjust to vendor technology. Guidehouse offers best in class risk and cybersecurity consulting, combined with industry leading expertise in emergency management, disaster recovery, and system hardening. Our team includes experts with over thirty years' experience as cybersecurity and IT experts.

# 2.0 General Description of Responder's Qualifications and Experience

## *2.1 Proposed Personnel And Organizational Chart*

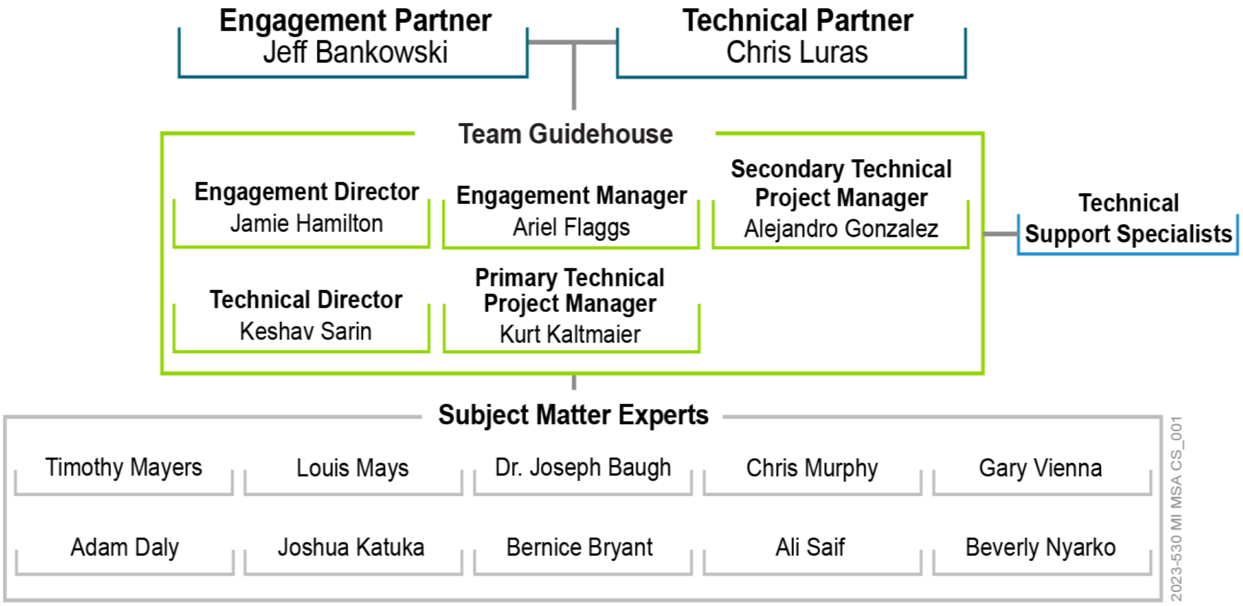


**Figure 1. Organizational Chart**

### 2.1.1 Jeff Bankowski, Engagement Partner

**Certifications**

- Certified Public Accountant
- Certified Internal Auditor
- Certified in Financial Forensics
- Certified in Risk Management Assurance
- Certified in (re) Vision™ Change Management

**Degree/Education**

- MBA, DePaul University
- BA, University of Michigan

**Total Years of Experience:**

25+ Years

**Relevant/Key Qualifications**

Jeff is Guidehouse's State and Local Government Transformation and Financial Effectiveness Leader and has more than 25 years of experience leading enterprise performance improvement and financial transformation in the public, private, and nonprofit sectors.

Previously, Jeff was the Chief Internal Auditor for the State of Michigan reporting to its Governor. In 2018, Jeff was selected by the Association of Government Accountants (AGA) as the national award winner given in recognition of a state government professional who exemplifies and promotes excellence in government management for his work in financial management. Jeff is a national thought leader on government finance and innovation and has spoken at the National Governors Association (NGA) Learning Lab, the American Society for Public Administration (ASPA) National Conference, and has taught in the Master's Program at the Gerald R. Ford School of Public Policy at the University of Michigan. Jeff is a Board Member on the Executive Committee of the National Association of Chief Administrators (NASCA) which is composed of Cabinet-level and senior public and private officials that provide operational support and transformational change to State departments. In September 2019, Jeff was appointed by the Government Finance Officers Association (GFOA) as an advisor to the Committee on Governmental Budgeting and Fiscal Policy.

**Relevant Experience**

**City of Detroit, Oakland County, and Wayne County**

Jeff is the engagement partner leading the firm's work supporting the City and Counties to identify authorized use of CARES, FEMA, and CRF relief funds including verifying eligibility and creating financial projections of expenditures and dashboard/transparency reporting.

**State of Oklahoma**

Jeff led an organization assessment of the Executive branch to identify potential ways to achieve collaboration, simplification, efficiency, and mission accomplishment for state operations. Mr. Bankowski also supports the State's COVID-19 grant management portal built on the Salesforce platform to accept applications for relief funds.

**State of South Dakota**

Jeff led the management visioning and strategy effort designed to create an operating model for the Bureau of Financial Management and the Office of the CFO for the next 4 years. Following this effort, Jeff and his team led a program management office (PMO) that oversaw the implementation of new business processes and controls to improve fiscal effectiveness, risk management and accountability.

**City of Detroit**

Jeff oversaw a high-profile, comprehensive strategic transformation of the revenue and tax collection process to support Detroit's emergence and rebirth after its historic bankruptcy filing. Jeff and his team oversee multiple workstreams to insource the tax collection process from the State of Michigan including conducting a variety of quantitative and qualitative analyses to create a call center, e-filing capabilities, and developing a robust return on investment model that was presented to the Mayor and City Council.

**State of Michigan**

In the role of Chief Internal Auditor, Jeff led the risk assessment and process review for the State operations including financial, operational, and performance-based audits. Jeff supported DTMB in its roadmap to prioritize information technology control deficiencies at the request of the DTMB Director and the Legislature.

At the request of its Governor, Jeff was asked to implement the state's first enterprise risk management framework. Leveraging leading practices from the public and private sectors, Jeff led a top down and bottom-up assessment of Michigan's departments, agencies, and related programs. Over a one-year period, Jeff and his team identified, and documented areas of the greatest risk based upon impact and likelihood for a $56 billion enterprise serving 9.9 million people. Jeff's work was presented to both the Governor's office and the Legislature and resulted in the creation of the Enterprise Risk and Control Committee that included, the Governor's office, the State Budget Director, the DTMB Director, members of the Cabinet, and independent members from the public selected by the Governor.

Jeff held the role of Chief Performance Officer and Transformation Director, in which he was responsible for streamlining administration and improving the delivery of government services for a $56 billion enterprise serving 9.9 million people. Jeff oversaw operating reviews, lean transformation, risk management and enterprise performance improvement. In 2018, Jeff and his team accepted on behalf of the State of Michigan the 2018 North American Government Employee Engagement Agency of the Year award presented in Chicago, Illinois.

Jeff was appointed to the Information Technology Investment Fund (ITIF) Board. Jeff and his team supported the prioritization and allocation of the State's technology investments that were then approved by the State Legislature.

Jeff led the financial review and oversight team for Wayne County (19th largest county in the United States), which had been declared by the Governor to be in a state of financial emergency. Jeff led the financial analysis and recommendations for the county's financial operations and pension system. Jeff presented to various oversight boards including the State Treasurer, the State Budget Director, and members of the Local Emergency Financial Assistance Loan Board. Jeff was responsible for the financial and economic analysis of Wayne County's current debt structure and underfunded pension system including detailed analysis of budgetary gaps, accumulated deficits, declining revenue sources, and deteriorating cash position. Through Treasury, Jeff oversaw the implementation of the Wayne County recovery plan and the exit of a government consent agreement in 2016.

**State of Ohio**

Jeff led annual benchmarking and best practice sharing regarding internal controls, risk assessment, and anti-fraud, waste, and abuse programs.

**City of Flint**

Jeff led the financial integrity and oversight monitoring for the Federal government and State's recovery operations in response to the contaminated drinking water crisis. After the declaration of a state of emergency for the City of Flint (7th largest in Michigan) and Genesee County, Jeff provided financial auditing and compliance expertise to the City for all grant compliance and the related implementation of anti-fraud, waste and abuse programs.

### 2.1.2 Chris Luras, Technical Partner

**Degree/Education**

- MBA, Finance and Strategy Emphasis, Honors, University of Utah
- BS, Economics, University of Utah
- BS, Communications, University of Utah

**Total Years of Experience:**

25+ Years

**Relevant/Key Qualifications**

Chris joined Guidehouse in 2015 and has over 20 years of experience in the energy industry. Chris serves as a Partner and the solution leader for Guidehouse's Risk, Compliance and Security services, working with utilities on all aspects of NERC Reliability and Security compliance. Specifically, Chris leads the development, management, and execution of tools and services aimed at cybersecurity, security compliance, risk management, resiliency, internal controls, and process and program improvement within the energy sector. Chris was formerly the Western Electricity Coordinating Council

(WECC) Director of Compliance Risk Analysis and Enforcement, where he led a team of regulatory professionals, cybersecurity professionals, and electrical engineers. During his seven years at WECC, Chris created and developed the Compliance Risk Analysis and Enforcement teams and led the development of all the tools, processes, policies, and procedures, which paved the way for how WECC monitors and enforces all Reliability standards in the Western Interconnection. Chris also created and led most of the WECC Reliability Compliance Processes.

**Relevant Experience**

**Compliance Assessments**

Chris led, reviewed, and oversaw the review and assessment of over 3,000 reliability compliance mitigation plans and its associated RSAWs and evidence packages. Created the WECC Mitigation Plan review process. Led, reviewed, and oversaw the review and assessment of the WECC Self-Certification process. Oversaw the review of more than 1,000 Self-Certifications. Helped create the WECC Self-Certification process. Conducted reviews of more than 100 WECC audit reports and participated in WECC audits. Helped develop the scope for more than 75 audits. Successfully facilitated over 300 enforcement settlement negotiations.

Created the enforcement settlement process at WECC. Worked with three Entities on the Self-Logging Process and was part of the NERC and regional process teams that created this process. Chris created the Self-Logging Process at WECC. Led and participated in three audit preparations that resulted in no findings. Developed compliance processes and procedures for several companies.

**Internal Controls Evaluation**

Chris was on the NERC and Regional Project Team that created the ICE process. He also created all the ICE processes at WECC. Co-authored the first Internal Controls Evaluation Guide with NERC. Designed, developed and supervised WECC's process to conduct ICE for WECC utilities. Conducted training for utilities and WECC auditors on the ICE process. As WECC staff conducted 10 Internal Controls Evaluations. Conducted six ICE including USBR, BPA, PEAK RC, Los Angeles Department of Water and Power's (LADWP), CDWR and PRPA. During these projects, evaluated internal controls associated with NERC Critical Infrastructure Protection (CIP) and Operations and Planning (O&P) Standards. The evaluation included the identification and evaluation of internal controls (including type, maturity level, key controls, and gaps), internal controls process maps and final reports, which included control summaries, analyses of controls and recommendations on how to improve controls.

**Risk Assessments**

Chris helped develop WECC's audit approach for most of WECC's actively monitored standards. Conducted and led more than 25 IRAs. Was on the NERC and Regional Project Team that created the IRA process. He also created the IRA processes at WECC.

Part of the NERC and regional team that developed the risk-based framework under Reliability Assurance Initiative (RAI). Developed and led WECC's process to conduct IRA for WECC utilities. Conducted training for utilities and WECC auditors on the IRA process.

As WECC staff, his team collectively conducted 30 IRAs. Chris conducted 7 IRAs including USBR, BPA, PEAK RC, LADWP, IID, CDWR and PRPA. During these projects, he assessed the inherent risk for each utility per the WECC IRA process, identified a list of requirements based on risk and provided recommendations to reduce future inherent risk.

**Internal Compliance Program Assessments**

Chris led, reviewed, and oversaw the assessment of over 125 ICPA. Created the WECC ICPA process, which is a tool to assess the effectiveness of compliance programs.

Chris also led the team that assessed the following reliability compliance programs: BPA, Arizona Public Service Company, Pacific Gas and Electric, PacifiCorp, NV Energy, and SMUD.

### 2.1.3 Jamie Hamilton, Engagement Director

**Degree/Education**

- MS, Computer Science, Clark Atlanta University
- BS, Computer Science, Grambling State University

**Total Years of Experience:**

20 Years

**Relevant/Key Qualifications**

Formerly a Director of Engineering with Oracle, Jamie Hamilton is Guidehouse's Technology Director based in Michigan with proven experience in planning, developing, and building cutting edge solutions to address client opportunities and business needs. Jamie has extensive experience developing talent, leading teams, and implementing strategic technology initiatives in a fast-paced environment. Jamie has proven success designing and developing comprehensive Internet and application architectures for high traffic eCommerce websites and critical business applications. Jamie also has several years of experience managing outsourced development teams as well as Software Engineering and QA teams. Jamie has a depth of technical knowledge, including extensive knowledge of web development and LAMP, implementation of cloud-based solutions, and DevOps Experience.

## Relevant Experience

### Oracle

As the Director of Engineering, Jamie managed and led the Software Engineering department for Oracle's Ann Arbor office, which focused on the delivery of custom eCommerce solutions for clients. Jamie acted as a senior representative of Oracle with prospective and existing clients. Jamie duties include assisting Program Managers in allocating resources, oversight of numerous Web projects, making tactical staffing decisions, providing leadership for the department, participating in the development and execution of the department and company-wide strategy, developing engineering process efficiencies, project scoping, project staffing, resource projections, interviewing, hiring, terminations, performance reviews, mentoring and issue resolution. Jamie team had approximately 50 Software Engineers and Interface Developers. Jamie also led and managed approximately 25 off-shore Software Engineers and a QA team, which consisted of 12 QA team members.

### Quicken Loans

As Vice President of Information Technology, Jamie's team was aligned with internal business partners (Accounting, HR, Focus Team, etc.) to ensure the successful execution of their business goals, supporting their technology needs and building strong partnerships. This role required him to develop people, align process and technology in the pursuit of strategic business outcomes. The team consisted of approximately 50 team members, which included IT Directors, Team Leaders, Software Engineers, Business Analysts, and Application Administrators. The team used a diverse set of technologies including Microsoft .Net, PHP and mobile platforms (iOS and Android). Jamie provided technical and strategic guidance to IT Directors and Team Leaders to ensure achievement of goals and objectives and ensured value across internal Business Partners. Jamie also interacted with all levels of Leadership, setting short and long-term strategic objectives, operating procedures, resource allocation and budget, while providing the leadership necessary to achieve the goals of the team.

As Vice President of the Software Engineering Team, Jamie reported to the CIO, directly led 9 IT Directors and was responsible for approximately 220 team members, which included the IT Directors, Team Leaders, and Software Engineers. He was responsible for enterprise-wide application development including loan origination system of record, document workflow, Call Center Technology, business logic services, web application, native mobile development and maintaining hundreds of supporting applications built on various technologies including but not limited to.Net, Java, LAMP and Progress OpenEdge. Jamie estimated engineering efforts, planned development and deployment, and rollout system changes that met requirements for functionality, performance, scalability, reliability, and adherence to development goals and principles. As part of this role, Jamie had to anticipate bottlenecks, assess, and mitigate risks, provide escalation management, anticipate, and make tradeoffs, and balance the business needs versus technical constraints.

**North American Bancar**

As Vice President of Engineering, Jamie led the Software Development Team, the Project Management Office (PMO) and the Quality Assurance Team. Jamie's team was responsible for all internal application development at NAB, as well as, managing the company's project portfolio. Jamie created and maintained architectural best practices and standards that address applications, data, and technology in the context of business processes across the NAB IT landscape. He provided leadership for the overall strategic application architecture plans, system design, and implementation. In this role, Jamie worked with project teams across the organization to develop and apply architectural best practices and standards, including performing a more involved advisory role on complex initiatives. He also developed and maintain global technology roadmaps and application evolution plans for the IT portfolio.

**United Shore**

As Vice President of Engineering, Jamie led six key IT teams: Software Development Team, the QA Team, the Application Deployment Team, a Tier 2 Support Team (Business Analysts and Software Engineers), IT Service Desk Team (Tier 1 Support) and the Client Engineering Team (Desktop and End User Support). Additionally, he was responsible for Incident Management and playing the role of Incident Manager on severe system degradation and application outages. The six teams totaled over 100 people, consisting of Software Engineers, QAs, Business Analysts, Operations Analysts, Field Technicians and Team Leaders. Jamie not only provided leadership to all IT team members, including mentoring and career development, he was also involved in operations. He developed and maintained technology roadmaps for all teams, and on application outages, he identified business impact, root causes, technology fixes and prevention approaches.

**Revegy, Inc**.

As Senior Vice President of Technology, Jamie was responsible for overseeing all technology aspects of the company, including application, quality assurance, IT operations, product implementation & configuration, Tier 1 & 2 product support and Project Management. He carried out strategic planning by establishing and driving the technology vision for Revgy and ensured the Technology Team aligned perfectly with Revegy's overall strategy and goals and the development of the Technology team members. Jamie worked with Product Management to ensure optimal value is delivered to Revegy clients by this solution transition, and ensured issues raised by customers were addressed in accordance with SLAs. In this role, Jamie managed strategic vendor and partner relationships. He also prepared budgets for the technology team and ensured adherence to those budgets.

**Guidehouse**

As Director, Jamie leads the Technology Strategy for Guidehouse's State and Local Government practice as well as overseeing technology strategy for States and Cities in the Midwest.

**Wayne County**

Jamie leads Wayne County's ERP PMO. This engagement required a migrate to Oracle HCM and Financials Cloud from legacy HCM (PeopleSoft 9.0) and Financials (JD Edwards World 9.1A) "on-prem" hosted systems. There are several Oracle modules being implemented…Core Financial, Core Human Resources, Payroll for Active and Retiree populations, Workforce learning and professional development, Compensation, Benefits and several other key modules. Jamie and his team are also providing the following services to Wayne County: Testing, Training, Change Management, Staff Augmentation and Enterprise Architecture Services.

**Oakland County**

Jamie has been leading the PMO where he managed the county's transition to Workday Financials. In this role, he has led the team to complete a current state assessment of the implementation. Following the assessment, Jamie oversaw the team's development of a new project timeline and go-live date, governance structure, change control and communications strategy, cross-functional impact analysis, business requirement document repository, test strategy & plan, and provided both functional and technical expertise related to Workday features, functionality, and best practices. During the County's implementation of Workday Financials, Jamie led the review and documentation of the county's current state Workday configurations and business processes. In this role, he was able to ensure the team mapped back to initial business requirements, streamlined processes, simplified security configuration, and solidified cross-functional impacts within Workday.

### 2.1.4 Ariel Flaggs, Engagement Manager

**Certifications**

- Certified SAFe® 6 Product Owner/Product Manager
- Six Sigma Yellow Belt

**Degree/Education**

- MPA, Columbia University
- BA, Spelman College

**Total Years of Experience**

10+ Years

**Relevant / Key Qualifications**

Ariel is a Managing Consultant in Guidehouse's State and Local Practice. Ariel has experience in orchestrating successful cross-functional initiatives, strategic planning, and leadership. Adept at driving end-to-end product management, leading high-performing teams, and fostering innovation. She has strong analytical skills and a user-centric approach to product development.

**Relevant Experience**

**Multination software consulting firm**

Ariel led the coordination of strategic initiatives spanning three distinct team functions, orchestrating seamless monitoring, tracking, and comprehensive daily progress reporting. Ariel demonstrated exceptional engagement skills by collaborating with stakeholders to deeply understand their needs and translate high-level ideas into user stories, effectively capturing constraints and envisioning solutions through mockups and prototypes. She designed and executed robust functional and cross-functional test strategies, assuring software quality and reinforcing your commitment to delivering a superior end product. Ariel significantly expedited project delivery time by a remarkable two weeks through diligent daily progress monitoring, tracking, and reporting, showcasing dedication to efficient and timely execution.

**City of Detroit**

Ariel provided expert-level technical guidance and strategic support across diverse work streams, ensuring the seamless transition of income tax administration from the State of Michigan to the City of Detroit. Ariel led a pivotal role in overseeing the procurement process for a multimillion-dollar income tax administration software, guaranteeing precise and error-free processing of returns, thereby enhancing operational accuracy. She also skillfully managed the restructuring of department staffing and orchestrated implementation improvements, resulting in substantial efficiency enhancements across the organization.

**Wayne County**

Ariel exemplified adept leadership across geographically dispersed teams, steering a complex spectrum of priorities and commitments with a resolute focus on excellence, while adeptly leveraging Agile frameworks to drive project quality. Ariel navigated and guided design discussions, formulated launch strategies, and methodically created process maps, all while maintaining a vigilant oversight of project health. She crafted impactful communications and executive presentations catering to diverse audiences, translating complex technical concepts into digestible insights.

### 2.1.5 Alejandro Gonzalez, Secondary Technical Project Manager

**Certifications**

- OSHA 30 Certified

**Degree/Education**

- BS, Electrical Engineering, University of Texas Pan-American(RGV)

**Total Years of Experience:**

12 Years

**Relevant/Key Qualifications**

Alejandro has professional experience in multiple roles related to technology including asset management, systems performance analytics, cyber security implementation, project management, systems development, and development of policies and procedures. Alejandro's experience includes managing renewables systems projects for RES, administering SCADA/EMS and cyber security practices for Austin Energy, and leading the evaluation of cyber and physical security systems of electric companies for Texas RE. Most recently Alejandro has worked with numerous companies in various technology projects as a Consultant with Guidehouse. In these roles Alejandro evaluated systems, investigated issues, provided solutions, built tools, managed assets, wrote policies and procedures and implemented them.

**Relevant Experience**

**Guidehouse – AES(S-Power) – Cyber Security and NERC Compliance**

S-Power is a is a developer, owner, and operator of utility-scale wind and solar assets. The company develops utility-scale projects and sells the power to large off takers such as commercial businesses or utilities. The work with S-Power consisted in evaluating their entire

Cyber Security and NERC posture and provide program improvements including network equipment, servers, appliances, desktops and their virtual environment. Additional work is being performed to assist S-Power in transitioning from a low impact to medium impact registration and the necessary work required to become compliant by the required deadline.

Identified the ports and services being used and provided guidance on removal of risky services, justifications for necessary ports and services and compliance gaps to meet the system security requirements.

Evaluated password manager and identified use cases for features that can be used to facilitate compliance requirements and security improvements.

Completed a compliance evaluation for multiple cyber security requirements from a documentation perspective, identified gaps and provided guidance on tool upgrades that would assist with automation and compliance improvements.

Assisted with procurement for baseline, AV/AM, back-up/recovery, SEIM and software integrity verification tools required to meet multiple cyber security requirements.

**California Department of Water Resources (CDWR)**

The California Department of Water Resources is part of the California Natural Resources Agency and is responsible for the management and regulation of the State of California's water usage. The project includes assisting CDWR in developing a procurement program that meets their supply chain requirements and Executive Order 13920.

Assisted with development of vendor questionnaire tool used to evaluate the security risk of vendors for products and services prior to procuring them.

Assisted in developing mitigations for supply chain requirements where the vendors may not contractually be able to or refuse to assist CDWR meet the requirements.

Assisted in developing a supply chain risk mitigation (SCRM) plan that will be used by CDWR to ensure meeting the cyber security requirements.

**Los Angeles Department of Water and Power (LADWP) – Cyber Security and NERC Compliance**

For LADWP, one of the largest municipal utilities in the country, Alejandro helped evaluate internal cyber security controls. The project consisted in looking at evidence of methods being used, evaluating their tools and providing guidance on how to improve cyber security controls. The evaluation included their Incident Response Plans and Recovery Procedures.

Provided guidance on cyber security compliance requirements for multiple systems. This involved interviewing multiple groups, evaluating their compliance documentation and providing a gap analysis. Additionally, Alejandro has evaluated of audit evidence prior to sending to compliance enforcing entity to ensure there were no gaps.

Created guidance documentation for performing internal evaluation of cyber security compliance requirements. This project consisted in developing step by step instructions on how to evaluate compliance documentation, methodologies, risks and controls on all cyber security related systems.

Provided guidance on multiple scenarios for equipment upgrades to ensure compliance of NERC requirements.

**American Electric Power (AEP) – Cyber Security, NERC Compliance, Asset Management**

AEP is one of the largest utilities in the country with offices in several states. Assisted in implementing controls on cyber security systems from the result of control evaluations. This includes working with multiple groups, providing methods to complete implementation of controls and reviewing the implementation to ensure it meets the recommendation from the control evaluations.

Developed a method to automatically produce a large set of data into a spreadsheet that was once being complied manually. This project consisted in having a centralized data warehouse where the large set of data can be produced from. This required working with multiple groups that owned data sources, ensuring the data was being delivered into the data warehouse and evaluating the output of the data to ensure it was complete and accurate. We assisted with providing strategies on how to ensure each section was complete, methods for evaluating the data accuracy, controls to maintain the data and provided a project plan to ensure completion of the project.

Provided AEP guidance on securely handling network activities for inbound and outbound communications, including encryption, multifactor authentication and remote access methods.

Consolidated Edison – Cyber Security

Consolidated Edison provides electricity to 10 million people in the New York City area. Assisted with review of critical communication networks for cyber security risks and reporting of results.

**Texas Reliability Entity (Texas RE) – Cyber Security, NERC Compliance, Asset Management**

Entrusted with leading Critical Infrastructure Protection (CIP) and Operations & Planning (O&P) audits of multiple electric companies. This involved coordinating with the companies' audit lead, creating presentations for the teams involved, coordinating schedules and travel of auditors, ensuring a full evaluation is complete and writing a final report of results.

Performed CIP and O&P audits, including documenting deficiencies, evaluating controls and presenting findings to many electric companies. This involved evaluating cyber security procedures provided from the company, asking question for clarification online and in person, documenting in detail what was determined, providing recommendations, and writing a report of the evaluation. Evaluations included Incident Response Plans and Recovery Procedures. Table-top exercises, actual incidents and how recovery was performed was also evaluated. Alejandro was collaborated on CIP-013 Supply Chain Risk Management standards on audit approach for upcoming implementation requirements.

**Austin Energy – Cyber Security, NERC Compliance, Asset Management**

Administered tools used for ongoing cyber security compliance requirements. Some of these tools included Industrial Defender which produced baseline reports ensuring that all changes to systems were being recorded. Nexpose Rapid 7 which was used for performing network discovery scans and system vulnerability assessments. Windows System Update Services for updating windows systems with security patches. Periodic evaluation of third-party hash signatures were performed to ensure software integrity was maintained when software was obtained from online source.

Assisted administration of SCADA system operation and security, ensured cyber security compliance, and developed tools to enhance productivity. This included installing new equipment, ensuring we had a recovery method for each one, monitored logs for any performance issues and responded to technical problems affecting operations. Additionally, database updates to the SCADA/EMS system was performed, for equipment upgrades in the field along with validating functionally prior to delivering upgrade to operators for field operations.

Entrusted with completion of required cyber security compliance plans and procedures. This included evaluating current systems, determining how cyber security compliance was going to be applied, documenting the steps for on-going implementation, testing procedures for performance and implementing them. Plans and procedures created, tested and implemented included Incident Response Plans and Recovery Procedures.

**Renewable Energy Systems (RES)-Americas – Asset Management**

Ensured the finalization of procurement and installation of photo voltaic solar panels. This included communicating with procurement managers that informed each step from manufacturing to delivery. Alejandro inspected each shipment container and approved them for delivery to construction site for staging and installation. Installation was monitored daily and ensured it was according to design.

Developed mapping system that enables a user to view manufacture performance data and physical location of solar panels. This involved pulling data from a database for each solar modal, individually scanning them to identify in the field and developing a mapping to locate them. The data also provided performance statistics based on voltages of each panel and how they were configured in the field. Full review was completed with this data and Alejandro provided guidance for adjustments of solar panel installations to improve energy efficiency and monitored for completion.

### 2.1.6 Keshav Sarin, Technical Director

**Certifications**

- CISA

**Degree/Education**

- MBA, Operations and Management Emphasis, University of Utah
- BS, Engineering, Electronics and Communications, Karnataka University

**Total Years of Experience:**

25+ Years

**Relevant/Key Qualifications**

Keshav is a Director in Guidehouse’s Energy, Sustainability, and Infrastructure practice. Keshav brings more than 25 years of professional experience in a variety of roles related to risk management, information systems, development, cybersecurity, and project management in the energy, finance, and healthcare industries. He specializes in critical infrastructure protection, reliability and resilience areas.

**Relevant Experience**

**Los Angeles Department of Water and Power (LADWP)**

Assessed, designed, and implemented LADWP’s critical infrastructure protection, resilience and cyber governance program pertaining to its power systems infrastructure. Recommended a roadmap to strengthen LADWP's critical infrastructure protection and resilience program. Designed, and implemented a critical infrastructure risk and controls framework to identify and manage regulatory, compliance and operational risks. Designed and implemented a critical infrastructure protection and cyber security training framework to provide training to all compliance, security and critical infrastructure protection personnel. Conducted a risk assessment and internal controls evaluation to manage identified critical infrastructure protection, compliance and security risks pertaining to critical infrastructure. Conducted an cyber vulnerability assessment (CVA) for LADWP's critical infrastructure cyber systems. Provided recommendations to remediate vulnerabilities and ensure resiliency of LADWP's SCADA and EMS. Trained LADWP's personnel on CVA process and tools.

**California Department of Water Resource (CDWR)**

Developed and updated operational, IT and security engineering processes and procedures associated with cybersecurity and NERC Critical Infrastructure Protection requirements for critical infrastructure facilities such as Dams and associated Control Rooms. Provided mentorship, training, and transfer knowledge related to security processes, procedures and tools developed. Conducted risk assessment and identified controls pertaining to critical infrastructure facilities and cyber systems to improve the resilience of critical infrastructure.

**New York Power Authority (NYPA)**

Assessed, implemented, and improved NYPA's current critical infrastructure cyber / physical security resiliency, and emergency management posture, including developing security-focuses project plans and strategies, considering the availability and overlapping dependence of multiple client personnel, and competing deadlines. Designed and implemented a cyber and physical ICS security incident response plan to improve NYPA's grid resilience. Led and conducted an exercise of the incident response plan. Customized, supported and facilitated active participation in the national cyber and physical security exercise, GridEx, to simulate a cyber/physical attack on electric and other critical infrastructure across North America to test cyber and physical incident response and resiliency plans. Implemented external routable connectivity for NYPA's facilities; configured Interactive remote access; established intermediate systems for such access; configured strong authentication processes.

**Western Electricity Coordinating Council (WECC)**

Designed, developed, and supervised WECC's processes to conduct risk assessment for security, operations and resilience of critical infrastructure owned and operated by more than 300 entities under WECC's jurisdiction. Conducted more the 50 trainings and outreach for critical infrastructure owners and operators of the western power grid on all aspects of WECC's risk and compliance processes. Conducted 30 inherent risk assessments and controls evaluation to identify gaps and areas of improvement for critical infrastructure associated with the Western electric grid. Part of the NERC and Regional team that developed a nationwide risk-based framework for critical infrastructure associated with North American power grid.

### 2.1.7 Kurt Kaltmaier, Primary Technical Project Manager

**Certifications**

- Certified Project Management Professional (PMP) Credential ID: 445636
- Certified Information Systems Security Professional (CISSP) Credential ID: 541032

- Information Technology Infrastructure Library Certification (ITIL)
- Member of International Information System Security Certification Consortium (ISC)2
- Member of Project Management Institute

## Degree/Education

- BS, Business Management, Redlands University
- AS, Computer Information Science, MSJC

## Total Years of Experience:

20 Years

## Relevant/Key Qualifications

Kurt is an associate director with focus on cyber security/information security. With more than 20 years' experience in IT/OT systems, cyber security, and program/project management. His background includes contributor and leadership cyber security positions in the utility and technology manufacturing sectors and includes managing teams to measure and mitigate security risks, assure compliance, and architect secure systems. Kurt is an expert in Infrastructure Technology (IT) / Operational Technology (OT) and cyber security, and NERC CIP compliance. Kurt supports clients through information protection (vulnerability assessments / penetration testing and mitigation, policy creation, automation), reviewing security/compliance posture, system design and automation, and providing actionable recommendations. His expertise includes both compute and network environments including cutting edge cyber security concepts aimed at securing client systems.

Additionally, Kurt has worked with various clients to improve their systems and policy environments. Frameworks and compliance knowledge include NERC CIP, NIST 800, and ISO 27000. Prior to joining Guidehouse, Kurt work with SEL Inc in Pullman WA supporting OT clients world-wide with unique and sound OT cyber security solutions. During this time, Kurt worked with various utilities including DEWA in the UAE, Copel in Brazil, Qatar Power Co in Doha, and others. Prior to SEL, Kurt lead the CIP infrastructure team from the Information Security department at San Diego Gas and Electric where he also held various other management positions such as Data Center manager for both SDG&E and the Southern California Gas Company. While at SDG&E Kurt implemented various technical innovations such as on-demand virtual server resources, server-based computing, data center physical asset management, and innovated program management through enterprise projects as WAN rebuilds and VoIP conversions.

## Relevant Experience

### IT/OT Systems and Design

Assess, design, and build security solutions Review client requirements to design and build secure network and computer systems and provide residual risk reports for domestic and international electrical utilities as well as mining and other energy related industries.

Develop security-based training material Engage clients on various Learning Management Systems (LMS) and develop custom security training programs including building CIP Training for Schweitzer Engineering Laboratories (SEL). Lead CIP and network security training and workshops for various clients while at SEL.

### Compliance and Regulatory Control

NERC CIP compliance / security expert Over 10 years' experience with NERC CIP standards advising clients on interpretation of requirements, designing IT/OT compliant systems, and assessing risk as an employee of San Diego Gas and Electric along with other electric utilities across the US.

NERC CIP Controls Evaluations at Guidehouse, lead multiple Internal Controls Evaluations which included evaluation preparation, conducting client interviews, research on existing controls, formatting data findings that included executive reports, controls, recommendations and implantation schedules of findings.

NERC CIP Compliance Gap Analysis at Guidehouse, reviewed various programs/processes to determine business unit involvement, adherence to procedures, review and mitigation of incidents along with RSAW review and rewrite .

### 2.1.8 Timothy Mayers, Subject Matter Expert

**Certifications**

- Certified Information Systems Security Professional (CISSP) (2007), Active, License# 106248
- Certified Ethical Hacker (CEH) (2007) Active, License# ECC923011
- Certificate of Cloud Security Knowledge (CCSK) (2014) Active, License# 660888664798

**Degree/Education**

- MBA, The University of Texas at El Paso
- BA, Computer Information Systems, The University of Texas at El Paso

**Total Years of Experience:**

25 Years

**Relevant/Key Qualifications**

Timothy is a dedicated cybersecurity professional and has more than twenty-five years of professional experience within the government and commercial sectors, with over fifteen years of performing and leading cyber security tool optimization, threat analysis, information security architecture reviews, information security policy development, cybersecurity performance reviews, software engineering, and organizational programmatic analysis.

Timothy has in-depth experience leading and performing security assessments to identify IT assets and provide Chief Information Security Officers with valuable actionable information on the current state of managerial, operational, and technical security controls. Timothy is experienced in helping diverse Federal departments, agencies, and commercial businesses design, document, and test security controls ranging from policies and procedures to technical configuration settings.

Timothy has in-depth experience assessing compliance with leading cybersecurity frameworks and best guidance which includes National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems" and NIST SP 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," with a focus in business mission risk analysis, internal Information Technology (IT) BUSINESS INTERNAL \ GENERAL controls reviews, analyzing

Use or disclosure of data contained on this page is subject to the restriction on the cover page of this document.

compliance with Federal laws and regulations which include; Federal Information Security Modernization Act of 2014 (FISMA), and Department of Defense (DoD) RMF.

Timothy has led the development of Independent Validation and Verification (IV&V) Programs, enterprise level IT security policies, System Security and Authorization, IT architecture system security analysis, IT asset management, and database/software development.

In addition, Timothy has extensive experience performing as a technical writer and assisting with the development of the FY2012 – FY2015 Annual FISMA Metrics, congressional reports, senior executive reports, and leading briefings with Federal Chief Information Officers on the status of Federal-wide cybersecurity initiatives through the CyberStat program in support of the Office of Management and Budget and Department of Homeland Security.

Timothy has four years of honorable military service in the United States Army and has also earned a BBA in Computer Information Systems with honors and an MBA in General Business Management from the University of Texas at El Paso (UTEP). In addition, Timothy has maintained Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH) certification since 2007. Timothy earned the Certificate of Cloud Security Knowledge (CCSK) in 2014.

## Relevant Experience

### Guidehouse

Timothy is a member of the Cybersecurity Solutions Team, a component of Guidehouse Advance Solutions, and assists commercial and Federal organizations with strategic and tactical information security projects across a broad range of technology disciplines.

Timothy is currently serving as a Technical Operations Manager, leading the daily engineering operations for the deployment and maintenance of a Global Identity Management System (IDMS) for the Department of State - Diplomatic Security Identity Management (IDM) division to provide a global HSPD-12 compliant PIV card solution.

Timothy has served as a Cyber Risk Management Subject Matter Expert for the Department of State, providing risk assessments of IT security exposures based on NIST 800-53 and 800-30, and 800-37 Risk Management Guidance to assist the Global IT Risk Office to lead the Department of State efforts to identify and resolve areas of improvement to address system-level programmatic challenges, produce observations and reports of cyber risk to consistently determine risk throughout the Department's implementation of the Risk Management Framework (RMF) process.

Timothy served as the Program Manager for the Enterprise Vulnerability Assessment Program for the Federal Bureau of Investigation (FBI) which includes leading the development and operation of Tenable Security Center and Trustwave vulnerability scanning infrastructure, execution of the conducting vulnerability scans across all Agency security classifications and enclave types, leading executive vulnerability data calls, and advising senior executives and Information System Security Managers and Officers on required steps for remediation and compliance.

Timothy led the performance an end-to-end assessment of NIST 800-53 security controls for a Fortune 500 commercial client's government component to support cybersecurity program transformation initiatives.

Timothy served as a key advisor to the Office of the Air Force Chief Information Security Officer (CISO) and assisted the newly formed organization with implementing the Tanium Endpoint Management tool, aligning to the NIST Cybersecurity Framework, NIST 800-53, and improving IT asset management procedures for over 700,000 endpoints in near real-time.

Timothy led the support of the Air Force CISO Special Projects Division implementation of innovative cybersecurity initiatives through internal and external stakeholder collaboration and the prioritization of tasks or projects that increase resiliency and get the most business value of multiple technology investments to improve the identification and management of risk throughout the lifecycle of all Air Force IT systems.

Timothy as a member of the Air Force CISO Information Protection Team, supported the Special Projects Division's strategic and programmatic management efforts to strengthen the resiliency of Air Force systems/platforms through the leveraging and optimization of advanced defensive tools on Air Force Networks (AFN) to increase automation, awareness of threats, risks, vulnerabilities, and mitigation requirements.

Timothy performed NIST 800-53 security controls assessments for a multi-national corporation which included a comprehensive gap analysis for major systems required to implement core business functions.

Timothy served as team lead for the Department of Justice (DOJ), Federal Bureau of Investigation (FBI) vulnerability management program and led the documentation of vulnerabilities within the RiskVision GRC tool and the development of holistic enterprise-level strategies and program plans based on the Center for Internet Security (CIS) Top 20 "Critical Security Controls for Effective Cyber Defense" and NIST SP 800-160 "Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems" to reduce system vulnerabilities and improve visibility of the security posture.

Timothy performed independent testing of security controls for compliance with NIST 800-53 and FBI standards, developing enterprise remediation business plans for senior executives to increase the visibility of vulnerability management throughout the FBI information technology enterprise.

Timothy provided cybersecurity advisory and execution services to the DOJ Chief Information Security Officer (CISO) and developed strategies for managing its enterprise cybersecurity program. Timothy developed social engineering penetration test plans, provided recommendations on improving communications, business processes, organizational structures, and reporting methods to increase the overall impact and effectiveness of cybersecurity services and operations.

Timothy supported the development of orders, policies, and instructions for the DOJ Office of the Chief Information Officer (OCIO) Cybersecurity Services Staff (CSS) cybersecurity mission through identifying best practices, federal laws, regulations, and guidelines mandating the protection of information systems, and developing a tailored approach for program management, oversight, and execution of communications among components.

Timothy served as a team lead and key analyst for the Department of Homeland Security (DHS) and Office of Management and Budget (OMB) CyberStat program conducting analysis and reporting on cyber security data from across the Federal government, including assisting with the development of a common set of FISMA Metrics reporting criteria, which provided annual enterprise-wide reporting guidance to agencies Chief Financial Officers (CFOs), Chief

Information Officers (CIOs), and Chief Information Security Officers (CISOs). Timothy developed key

briefing materials that highlighted agencies risks, issues and progress on fiscal year FISMA Metrics goal requirements.

Timothy served as a member of the Delhaize Group, Food Lion Information Security assessment team; evaluating ISO/IEC 27002:2005 technical controls for the multi-national corporation’s ISO/IEC 27001:2005 based Information Security Management System (ISMS). Timothy provided penetration testing project management plan development support for a for Hewlett Packard’s (HP) Department of Homeland Security (DHS) Data Centers Risk and Vulnerability Analysis (RVA) Program Management Office (PMO).

Timothy served as a member of an executive dashboard software development team for the Department of Treasury, American Recovery and Reinvestment Act (ARRA) providing; database development, requirements documentation development, marketing and business development support, database architecture and database performance improvement.

Timothy served as a lead analyst for the PearsonVue educational services corporation and performed a FISMA Compliance gap analysis to aid the business pursuit decisions and compliance requirements.

Timothy served as a member of a Cyber Forensics team tasked to provide an analysis of financial services technology provider, FIS, Information Security Incident Response policies and standards, Information Security Management documentation and internal compliance. Timothy conducted the analysis in comparison to practices recommended by the Carnegie Mellon Software Engineering Institute (SEI) Handbook for Computer Security Incident Response Teams (CSIRTs), and the NIST Special Publication (SP) 800-61 Revision 2, Computer Security Incident Handling Guide.

Timothy performed Advanced Persistent Threat (APT) research for PricewaterhouseCoopers networks, analyzing the exploits and malware utilized and target networks with the FireEye Malware Protection System and advanced manual traffic analysis techniques to identify unusual network activity and vulnerability exploitation attempts. Timothy has significant experience developing reports of malware analysis findings for senior executives and multiple levels of the organization, which summarize the findings, risks, and appropriate mitigation.

Timothy developed a Quality Management program for HP's Public Sector Enterprise Program Management Office (PMO), which provided the processes and procedures to manage quality assurance and control across 40 congruent Information Technology projects based on the PMI Project Management Body of Knowledge (PMBOK), Capability Maturity Model Integration (CMMI), and Information Technology Infrastructure Library (ITIL) v3 Information Technology Service Management (ITSM) practices.

**Information Security Analyst**, **Science Applications International Corporation (SAIC),**

Timothy provided IA/ Computer Network Operations (CNO) security consulting, consisting of; risk assessments, information security research, penetration and vulnerability analysis of various IA technologies for the Department of Defense (DoD) at the Army Research Laboratory (ARL) in White Sands Missile Range, New Mexico, applying the DoD and Defense Information Systems Agency (DISA) security procedures.

Timothy performed information security research for the ARL Survivability and Lethality Analysis Directorate (SLAD), analyzing military system design and interface control documentation identifying potential vulnerabilities and susceptibilities within proposed communication nodes, networks, services, devices, and interfaces.

Timothy was responsible for the front-end design and back-end transaction processing, reporting, and data analysis of a MySQL database, which included database administration, performance, availability, and compliance with DoD security standards based on a Linux Apache MySQL PHP (LAMP) platform. Timothy was also assigned as the lead web application developer with duties that included testing, debugging, and designing web based reports and forms utilizing HTML, PHP, SQL, JavaScript, CSS and XML. The web application software he helped develop assisted in the research and development of computer exploits, security tools, and countermeasures.

### 2.1.9 Louis Mays, Subject Matter Expert

**Certifications**

- GIAC Security Essentials (GSEC) Certified
- Tripwire Enterprise Advanced Training Certified

**Degree/Education**

- BS, Electrical Engineering, Alabama A&M University

**Total Years of Experience:**

8+ Years

**Relevant/Key Qualifications**

Louis is a cyber **s**ecurity professional offering 8+ years of IT experience. He supports the NERC/CIP cyber security program at the SDGE. He performs cyber security roles and responsibilities to ensure the cyber security program follows NERC/CIP standards.

**Relevant Experience**

**Cyber Security CIP Operations Specialist**

Louis served as an engineer for monitoring digital network systems which utilize cyber security software/tools (SIEM, Firewalls, IDS/IPS, Endpoint security). He was responsible for performing vulnerability management on assets based on CVEs on NVD (National Vulnerabilities Database). As an engineer, Louis was also responsible for updating anti-virus definitions for anti-virus software, monitor SIEM logs, endpoint protection, and create/develop contingency plans on digital network systems.

**Cyber Security Lead Engineer**

Louis served as an engineer to support and maintain the Southern Nuclear Company (SNC) Cyber Security Plan in accordance with NEI 08-09 “Cyber Security Plan for Nuclear Power Reactors”, Revision 6 and 10 CFR 73.54 “Protection of Digital Computer and Communication Systems and Networks” requirements. He was also responsible for ensuring digital critical systems and critical digital assets (CDA) are governed and protected consistent with the requirements of 10 CFR 73.54 under the SNC Cyber Security Plan.

### 2.1.10 Dr. Joseph Baugh, Subject Matter Expert

**Degree/Education**

- PhD, Capella University
- Dr. Baugh's dissertation [*Deregulation and Management Strategies: A Case Study of Georgia System Operations Corporation*, In ProQuest Dissertations and Theses Global database: UMI# 3296749] explored organizations in transition via an examination of the impact of deregulation and other market forces in the electrical utility industry on management strategies, organizational structures, and organizational cultures at a non-profit generation and transmission electrical cooperative.
- MBA, Eller College of Management, University of Arizona
- BS, Computer Science, University of Arizona

**Total Years of Experience:**

25 Years

**Relevant/Key Qualifications**

Dr. Baugh is an expert in assisting Guidehouse energy clients with cyber and physical security solutions for generation, transmission, and distribution systems. Prior to joining Guidehouse in 2019 as a consultant working on cyber and physical security projects (with a focus on CIP-002, CIP-012, CIP-013, and CIP-014 projects), Dr. Baugh worked at WECC as a Senior Compliance Auditor and performed cyber security compliance audits and investigations at WECC utilities and other registered participants in the Western Interconnection for compliance with the NERC Critical Infrastructure Protection (CIP) Reliability Standards, including cyber security and physical security protective measures. He provided extensive compliance outreach and training in multiple topics including compliance programs, tool development, and program implementations, Supply Chain Risk Management, and emerging Reliability Standards. He also worked at a generation and transmission utility in Arizona, where he gained extensive experience in power system operations and maintenance, energy markets and scheduling, information system technology, cyber and physical security practices, and forensic investigations.

**Relevant Experience**

Dr. Baugh continues to work with client projects related to business process evaluation to support the development of client process improvements and internal skill sets. He aligns projects with the NIST Cybersecurity Framework, NIST cyber and physical security controls, and common capability maturity models, (e.g., CMMC and C2M2). Dr. Baugh worked closely with Guidehouse clients to assess risk management and compliance needs, identify gaps, develop high-quality solution designs and programs to meet needs and fill gaps, and manage client projects to implement effective solutions across multiple complex workstreams and business units. To accomplish these key objectives, he communicates effectively with client and Guidehouse management teams to keep them informed and aware of project development issues, project status, and issues associated with project change management.

**Western Electricity Coordinating Council**

Dr. Baugh served as a Senior Compliance Auditor leading and performing compliance audits and other investigations with WECC members and other registered participants in the North American electrical grid to ensure compliance with NERC Critical Infrastructure Protection CIP

Reliability Standards, including cyber security and physical security protective measures and controls. Dr. Baugh applied his academic research and data analysis skills to develop and implement qualitative studies, such as his focus on the CIP v5 transition, the CIP v5 implementation, the system categorization IRC 2.12 Transmission Control Center issue, and Supply Chain Risk Management topics. These studies provided guidance to the Electrical Reliability Organization (ERO) and supported policy changes in key areas. Dr. Baugh regularly presents the results of his professional and academic research in domestic and international venues.

**Arizona Electric Power Cooperative - Power Trading Projects**

When the AEPCO Power Trading Department was outsourced to ACES Power Marketing, Dr. Baugh accepted a new role at AEPCO, where he developed start-up programs for new trading and scheduling services customers, a Physical and Financial Gas Hedging program, and managed special projects, such as the Billing Unit Model software development project.

Arizona Electric Power Cooperative

Dr. Baugh served as a Power Trading Services Manager where he supported the Power Traders and Schedulers as part of the Energy Marketing function at AEPCO. He is experienced with common tagging systems and practices, forecasting load, negotiating purchase power agreements, and establishing effective power schedules to meet daily, weekly, and monthly load forecasts.

**Sierra Southwest Cooperative Services**

Dr. Baugh served in various IT Management roles within Sierra Southwest. Throughout a series of roles, Dr. Baugh managed the cooperative’s Tier 2 Internet Service Provider, the Network Services team, the IT Program Management Office, and finally the IT Support Services Department before moving back into AEPCO Power Operations as the Power Trading Services Manager.

### 2.1.11 Chris Murphy, Subject Matter Expert

**Certifications**

- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Internal Control Certificate (COSO)
- Physical Security Professional (PSP) – Bootcamp attended (not certified yet)

**Degree/Education**

- MS, Cybersecurity Dual-Major in Cyber Forensics and Cyber Operations, Utica College of Syracuse University
- BS, Organizational Security and Management (Physical Security)
- AS, Herkimer Community College

**Total Years of Experience:**

20 Years

**Relevant/Key Qualifications**

Chris Murphy is a Managing Consultant with the Risk, Compliance and Security Team in Guidehouse's Global Energy, Sustainability, and Infrastructure Practice. He has 15 plus years of professional experience in the Cyber Security, Information Technology (IT) and Management. A versatile, efficient, and reliable leader with excellent analytical abilities, technical skills, and the ability to learn new technologies. Strong background in general and forensic report writing. Recognized for building great client relationships and long-term loyalty.

Prior to joining Guidehouse, Chris was a CIP Compliance Auditor at SERC Reliability Corporation (Regional Entity) since 2017, where he conducted and lead NERC CIP Compliance engagements (Audits, Spot-Checks and Self Certifications), performed Risk Assessment and Mitigation (RAM) activities and served as a CIP liaison (SME) for Registration/Certification engagements. Chris was also a Program Manager for Entity Outreach and SERC's IT/Cybersecurity department. Areas of expertise included: Regulatory Compliance Audit Support, Cybersecurity, NERC Reliability Program Development and Implementation, and Project Management.

**Relevant Experience**

**Guidehouse**, **SERC Reliability Corporation**

At SERC Reliability Corporation, Chris served as the Critical Infrastructure Protection(CIP) Auditor , Program Manager Outreach & Information Technology, and Associate Critical Infrastructure Protection Auditor . He developed and refined CIP Auditing / Spot-Check approaches as well as methods for proper control of Cyber Security related information. He also served as a Cyber Security Subject Matter Expert to facilitate internal training, an Audit Team Leader/audit team member during the CIP Audits and Spot-Checks of entities within the SERC Region. Chris served as the Administrator for SERC's Protected Entity Information (PEI) data locker and the CIP-Up Electronic File Transfer (EFT) environment. Chris supported identification and analysis of emerging risks that could potentially impact the Bulk Electric System in conjunction with threat intelligence, events analysis, and compliance assessments. He also managed SERC's information technology and computer systems and provided assistance in CIP and Operations/Planning efforts.

### 2.1.12 Gary Vienna, Subject Matter Expert

**Certifications**

- SDG&E Safety Supervisory Award
- Certified Information Systems Security Professional (CISSP)
- Palo Alto Networks Certified Network Security Administrator (PCNSA)

**Degree/Education**

- MS, Information Systems, Grantham University, with honors
- BS, Computer Science, Grantham University

**Total Years of Experience:**

25 Years

**Relevant/Key Qualifications**

Gary joined Guidehouse in 2021 as a managing consultant with the Reliability, Compliance, and Security team. He brings 25 years of operational/information technology, cyber security, and information systems with project management experience. Most recently, he managed Sempra

Energy's Network Operations Center and SCADA Operations where he gained extensive knowledge of information systems, SCADA, network operations, NERC CIP compliance, and cyber security technology service process. He is published author and Adjunct Professor for California State Long Beach in Long Beach California.

## Relevant Experience

**San Diego Gas and Electric**

As Lead of Network Operations Center, managed the Information Technology/Systems and Operations team that oversaw the electric generation, transportation and distribution (electric/gas) for all Southern California:

Managed the Cyber Security of Operational Technology and SCADA networks
Created governing documentation to guide Network/SCADA Architecture decision making and communicate to the business
Managed and supervised network-related NERC CIP compliance activities within electrical substations, generation plants, and control centers
Directed project management and change management for the OT/SCADA network
Provided leadership and mentoring for personnel in the Network Operations Center
Prepared near and far future planning to anticipate the business needs for both SCADA and Operation Technology (OT) to interface with legacy equipment
Recommended technology and sourcing strategy to project managers, principal technologists, or infrastructure leads
Provided customer service to build relationships with internal and external partners
Investigated the value add for technologies and recommend solutions to the business in Operational Technology/SCADA and Compliance
Lead Manager of the NERC CIP Team), responsibilities included:
Overseeing the development and enforcement of NERC CIP standards Version 3 and Version 6
Conducting audits for the adherence of NERC CIP standards
Coordinating with the business in the implementation of NERC CIP Standards
Monitoring all Electronic Security Perimeters (ESP) and Physical Access Perimeter (PAC) for security and governance. Supervising the development of SOP in the areas of Incident Response, Security Configuration Management, and Threat Management

**Emmanuel Faith Community Church**

As IT/IS Manager, oversaw the help desk, infrastructure upgrades, IT project management, and leadership and direction in future IT systems development. Trained end users in new product use, and trained network engineers in sustainment. Developed techniques to employ social media as a communication tool, and trained information workers in effective use.

**Computer Science Corporation**, **Camp Pendleton**

As Web Manager on the Information Assurance Management Team, supervised five web software developers worldwide. Developed three synchronized "business in a box" portable datacenters including VoIP, fax, three types of digital messaging systems, tactical data mapping, file sharing, and collaboration workspace.

**US Marine Corps**

As IT Director for Marine Corps Systems Command, managed tactical software development for ship and airborne data links and security with both Linux and Windows systems. Supervised a team that integrated all Marine Corps commands into one integrated managed system, saving the government tens of millions of dollars.

### 2.1.13 Adam Daly

**Certifications**

- Engineer in Training Certification: 15-886-16
- Six Sigma Green Belt

**Degree/Education**

- Master of Business Administration, David Eccles School of Business, University of Utah
- Master of Science, Mechanical Engineering, University of Utah
- Bachelor of Science, Mechanical Engineering, University of Utah

**Total Years of Experience:**

Insert here

**Relevant/Key Qualifications**

As a senior consultant with Guidehouse's Global Energy, Sustainability & Infrastructure Practice, Adam supports the assessment and development of business strategies, organizational structures, and business processes for utility clients. He conducts assessments and evaluations of client business processes and internal controls as well as compliance as it relates to NERC Reliability. Upon evaluation of these processes he designs, recommends, and implements process improvements throughout power system operations. His process improvement and project management experience allow him to manage projects from inception to completion while ensuring the deliverables of all parties involved provide the most effective client solutions. He has demonstrated success in data driven decision making, allowing for fair assessment of all available project options; analyzing processes and developing programs and tools to support continuous quality improvement; evaluation of compliance as it relates to NERC Reliability and its associated standards; and intercompany communication allowing for smooth transitions and overall project buy-in.

**Relevant Experience**

**Guidehouse**

***NERC Compliance and Audit Preparation***

Adam managed and assist with the preparation of several large and medium utility compliance audits by assessing program documentation and evidence to determine compliance with NERC Critical Infrastructure Protection (CIP) and Operations and Planning (O&P) Reliability Standards. Adam supported mock audits by coordinating all efforts with compliance managers and client personnel, to ensure audit readiness. Adam developed compliance cheat sheets to be used by client personnel before an audit/audit interview to verify compliance and personal preparedness.  He assisted with the preparation and refinement of Reliability Standard Audit Worksheets (RSAWs) development, by providing guidance on document content and file management.

Adam supported coaching of client personnel on audit techniques and interview readiness, with focus on areas that are typically scrutinized by the regulator performing the audit. Responsible for identifying internal controls that support ongoing compliance with NERC Standards.

***CIP Verification Managed Services***

Adam reviewed and verified NERC CIP compliance with baseline changes to the clients NERC CIP infrastructure. Worked with client SME's to expedite the problem ticket process in an effort to reduce the total number of tickets outstanding. Adam verified client developed automation script was performing the necessary actions and was not producing errors or additional work for the compliance team.

***Control Program Evaluation, Development/Strengthening, and Management***

Adam was the key project management role of an enterprise-wide risk assessment and internal controls mitigation at one of the largest publicly owned utilities. This project is directly overseen by the utility CEO and Board Committee. He led subject matter expert interviews to identify both documented and undocumented controls in internal policies and procedures. Adam generated recommendations based on document review and subject matter expert interviews to assist the business units in their effort to achieve policy and process excellence. He developed controls database to allow client to have record of current controls as well as to assist with the continued effort to create more controls to protect the business and its employees. He assisted client in continued development of a world class control program via documenting and expanding upon existing processes, while mapping controls (both documented and undocumented) to the stages in said processes.

**Sweet Candy Company**

Adam was a member of the Process Improvement Team (PIT) working towards making production more efficient through continuous improvement projects and standard operating procedures. He analysed capital improvement projects and advise on their impact on production capacity, existing equipment, staffing and ROI.

Adam monitored data associated with key sales accounts using MXP and RetailLink while determining product upsells and consolidation to improve revenue. He implemented a production coordinator program which greatly improved cross departmental communication. Adam learned to navigate the ambiguity of a family owned and operated business that is 120 years.

### 2.1.14 JOSHUA K. KATUKA, Subject Matter Expert

**Certifications**

- CompTIA Security+
- Project Management Professional
- CISM
- CISSP – In Progress
- AWS Solutions Architect – In Progress

**Education**

- Masters in Information Systems University of Utah Dec 2020; Emphasis in Cyber Security
- Bachelor of Science Brigham Young University Dec 2016; Major: Computer Science

**Relevant/Key Qualifications**

Cybersecurity: Security Incident Handling and Response, SIEM Management, Audit and Compliance, Firewall IDS/IPS,

Vulnerability Assessment and Management, (Cloud) Security Monitoring

Audits: NIST, FEDRAMP, NERC CIP, DoD, ISO27001, SOC 1-3, Internal Controls Review

Cloud Services: AWS (EC2, S3, DynamoDB, CloudWatch, Elastic Cache, Guard Duty, IAM, Lambda), Azure, Google

Cloud

Programming: Python, Java, C++, JavaScript, HTML, CSS

OS Platforms: Linux (Ubuntu, Mint, Fedora), Unix, macOS, Windows 10

SCM/DevOps Tools: GIT, Jenkins, Docker, Kubernetes, Graylog, RedisLabs, Opsgenie and Jira, Prisma Cloud,

Crowdstrike, Sumo Logic

Enterprise Software: Microsoft Office 365, Slack, Teams, Zoom, Lucid Chart, WebEx, Salesforce CRM

## Work Experience

### Senior Cybersecurity Consultant Guidehouse

Support the risk, compliance and security team with assisting 6+ clients to create cyber security policies, enforce regulation and assist in compliance with various cyber systems. Perform various vulnerability tests and assessments which include but are not limited to network mapping, vulnerability scanning, phishing assessments, wireless assessment, OS security assessment and penetration testing. Assess security gaps in current operating procedures against standards and best practices. Assist in configuration of networks, policy implementation, threat remediation and forensic analysis. Act as liason between auditors and IT SME's providing customer consultation involving gathering and validating evidence, exposure, remediation and risk posture to comply with NERC, NIST and CIP standards.

### Terminal Area Security Officer United States Army

Served as Terminal Area Security Officer (TASO) and Information Management Officer (IMO) in an MTOE finance unit. Ensure NIPR/SIPR systems are in compliance with Information Assurance Vulnerability Assessments (IAVA), provide desktop support including diagnosing and resolving workstation operating system, software and hardware problems. Served as a Unit Movement Officer (UMO). Prepare, arrange and coordinate unit for deployment, safe and efficient movement of personnel equipment and manage and maintain accountability of inventory.

### DevSecOps Engineer RainFocus

Executed on-call deployment, support and monitoring of application stacks. Worked on Amazon cloud hosting (EC2, Lambda, EBS) and AWS administration using AWS dashboard and SDK. Used Kubernetes to orchestrate deployment, scaling and management of Docker containers. Responsible for debugging and resolving hardware, software, network issues, build and deploy failures. Travelled onsite 10-15% of the time for running logistics, coordination and client services at corporate events. Established and maintained policies, procedures and infrastructure to comply with ISO27001 compliance regulation.

**Financial Management United States Army Reserves**

Clearance: Secret. Perform duties specific to budgeting, disbursing, accounting and CVS. Worked/configured/troubleshoot active directory and a number of military software (mms, DDS, ECC reader, Oracle dB). Designed POC for migrating military finance ERP system to cloud.

**Sr. Technical Consultant Sonus Software Solutions Inc.**

Responsible for on-boarding, managing, consulting and developing relationships with 12 enterprise clients across 23 states. Created systematic approach to streamline existing and set-up new IT processes and migration of infrastructure to cloud (AWS and Azure). Travel 30% monthly to local and international sites to meet with IT/Engineering managers to scope project requirements and conduct monthly reviews. Coordinated, collaborated and monitored on-going projects and served as liaison between developers and clients/end-users.

**CloudOps Engineer Brigham Young University**

Design, deploy and migrate data, network and systems management applications from on premises into AWS. Achieved user satisfaction rating of 4.9/5.0; commended for quickly resolving complex issues such as system crashes, network slowdowns, connectivity problems, applications failures and more. Worked closely with management to hire technical engineers to work on upcoming projects involving software migration, application development and tier 2&3 support.

### 2.1.15 Bernice Bryant, Subject Matter Expert

**Certifications**

- Project Management Professional
- AWS - Certified Security Specialty, Certified Solutions Architect
- Azure Certified Administrator Associate
- CompTIA Security+ Certified
- CompTIA Linux+ Certified
- CompTIA Network+ Certified

**Degree/Education**

- BS, Cuttington University, Liberia
- BS, Cyber Security, Devry University

**Total Years of Experience:**

8 Years

**Relevant/Key Qualifications**

Bernice has over 8 years of Information Technology, Systems Security Engineering, Cybersecurity, and Program Management experience; where she was able to use her excellent communication and liaison skills. She designed and implemented cyber systems in a collaborative team environment and provided critical information assurance technical support, solutions for new applications, and recommendations to improve systems security policies and procedures in other environments including DoS.

**Relevant Experience**

**Guidehouse**

As a Senior Consultant in the Cybersecurity Solutions practice, leveraging Microsoft Defender for Cloud Applications (MDCA), Bernice and her team support, protect, manage, and run advanced threat detection across DoS cloud environment for a seamless access to a full suite of applications, as well as visibility and control over sensitive data. By scanning user activities, anomalies are detected. These detections use learning machine algorithms designed to profile the users and sign in pattern to reduce false positives. Using Identity Provider- Okta, users are authenticated and redirected to MDCA before accessing your application. It investigates activities and enforces policies by blocking certain actions e.g., copy/cut/paste. It also protects against DLP – the use of sensitive information/data. MDCA uses two connectivity methods to connect to applications – App Connectors which is API connection. This uses HTTPS to encrypt traffic between the app connections and MDCA. SAML 2.0 protocol is used to authenticate. The reversed proxy or conditional access control is the second method. It protects the user and the application. It also protects against potential malware. MDCA generates log activities, creates alerts by monitoring and correlates logs information in Splunk. Perform Security Assessment Report (SAR) with plan of action and milestones (POA&M) to facilitate and obtain Authority to Operate (ATO).

**4D Cloud Technology Solutions**

As a Cloud Information Security Engineer (Technical Scope including Amazon Web Services, HTTP, SAML 2.0, Okta SSO, AWS CloudTrail, Nessus Scanners, Ansible), Bernice worked closely with Cloud Architects, Engineers, and Security Specialists to design, configure, and developed security solutions with systems hardening collection tools for 4D Cloud Technology Solutions platform. Configure AWS network services and worked with team members to create secure VPC and subnets. She provided effective use of application connecting web APIs to enable the development of HTTP services. Bernice also provided technical solutions for ensuring optimal security of software and system technologies – from the physical, virtual, to application, using IaaS, PaaS, SaaS and service layers as required. Bernice has experience working experience in continuous integration practices and tools as well as experience designing and implementing penetration test case specifications for our platform.

She supported the integrated cloud platform with firm’s identity and Access Management systems (Active Directory and SSO), and leverage industry best practices for authentication and authorization. Bernice has a deep understanding of services and architecture required to build secure cloud computing platforms focusing on encryption of data at rest and in transit. Experience with APIs and web security, TCP/IP, networking, firewalls, encryption, intrusion detection systems, web filtering, authentication, and authorization methodologies. Leverage IAM and GuardDuty experience to properly secure our environment. Hold bottom-line accountability for devising and implementing scalable solutions in response to vulnerability reports to protect data from cyber-attacks and mitigate risks. Assist with the implementation, modification, and improvement of Risk Management Framework (RMF). Ensured project teams comply with regulatory compliance and best practices. Lead team on large scale programs that span the enterprise to deploy and manage various cloud security applications and agents.

Performed regular patching, updating of instances, and working with client companies to properly secure their data. Experience with security scanning (Nessus) and SCCM for patching and pushing packages to workstations and servers. Installed McAfee for antivirus endpoints protection on Linux and Windows operating systems (OS) in our environment. Leveraged knowledge of Data Loss prevention principles and applied knowledge to my daily cloud security work. Supported federal engagement ATO security process to move from development to production. Fully participated with teams to complete tasks in a timely manner. Identified opportunities for improvement and drove those improvements throughout the enterprise.

### B.G. Solutions

As a Cloud Security Engineer (Technical Scope: AWS Platforms, Terraform, CloudFormation, SSO, API Gateways, Nessus, Ansible), Bernice applied technical knowledge to protect network infrastructure from security risks. Responsible for applying NIST, RMF guidance, DISA, STIGs Privacy Act, and HIPPA regulations, instructions, manuals, checklist, and guides for cyber security. Effectively worked both independently and within cross functional project teams that spans multiple time-zone. Integrated AWS cloud with our on-premises services.

Utilized CloudTrail, logs and other monitoring tools documentations to present weekly monitored and incident report analysis. Worked on Projects ensuring key milestones were being met. Maintained alert systems, pinpointing risks, and responding quickly to vulnerabilities. Consulted on cross-functional projects to coordinate activities at all stages of systems development lifecycle. Worked with various risk and information security teams in presenting recommendations for improvement to technology subject matter experts and management. Developed horizontal view of risk management across multiple technology domains. Improved efficiency of security processes on both Linux and Windows platforms and recommended security controls of cloud operating model.

Developed and executed Cloud Information Security strategies to proactively identify risk and drive remediation. Leverage policies and guidance to ensure compliance with all local and federal regulations. Monitored full lifecycle for projects including performing penetration testing, troubleshooting access problems, and analyzing data. Experienced with BigFix for patching and Nessus scanner for vulnerabilities alerts; used SCCM for pushing packages to servers and workstations. Liaise with key stakeholders to aid design of appropriate solutions.

### PACO Technologies

As a System Network Administrator (Technical Scope: Amazon EC2, AWS CLI, AWS GUI, VMware, vSphere 6, VMWare ESXi), Bernice kept network infrastructure up to date and secure. Worked with wired and wireless data network providers to debug and resolve customer affecting service issues. Monitored VPN tunnels, logs on Cisco ASA firewalls. Monitored network and systems to improve performance. Checked logs and audit network systems. Assisted technical support staff and end- users to manage basic and expedited support for all network related issues.

Provide high quality level 3 support service focusing on Microsoft and Linux network services, IP routing, switching and firewalls (layer 1 through 7), LAN/WAN architecture, switch management and server builds. Experience with the configuration of DNS, DHCP, subnet, NAT Gateway, IGW, protocol and rules. Monitored network traffic and reported potential threat. Worked with end-users to ensure a protected network. Backup management reporting and recovery. Define network policies and procedures. Ensured network security and connectivity.

### STES Technology

As a Systems Administrator (Technical Scope: Ansible, Linux, Windows, Apache, Tomcat, VMWare ESXi, Samba, RHEL, CentOS), Bernice installed and configured software and hardware on both Linux and Windows platforms. Created new users, reset user passwords, unlock user accounts, and disable accounts when required. Added computers to domain, put groups in OU and give permissions in Active Directory (AD).

Worked with teams to create a robust backup and disaster recovery plan for a highly available, scalable, and fault tolerant infrastructure. Ensured security of the system through access control, backups, patching, firewalls, and using best practices. Used automation tools such as Terraform and Ansible for efficiency and the avoidance of human error.

Monitored and managed network servers and their performance and maintained systems according to requirements. Set up workstations, devising and implementing scalable solutions in response to vulnerability reports to protect data from cyber-attacks and mitigate risks. Leveraged policies, procedures, and best practices to ensure compliance with all local and federal regulations. Monitored full lifecycle of projects which included: performing penetration testing, troubleshooting access problems, and analyzing data. Liaised with key stakeholders to aid design of appropriate solutions. Participated in diagnosing and developing solutions for unhealthy Windows and Linux servers. Employed YAML packages to streamline and automate repetitive processes. Managed and monitored roll-out of applications.

### 2.1.16 Ali Saif, Subject Matter Expert

**Certifications**

- CompTIA Security +
- Certified Information Systems Security Professional (CISSP)

**Degree/Education**

- BS, Electrical Engineering, Alabama A&M University

**Total Years of Experience:**

5+ Years

**Relevant/Key Qualifications**

Cyber Security professional offering 8+ years of IT experience. I support the NERC/CIP cyber security program at the SDGE. I perform cyber security roles and responsibilities to ensure the cyber security program follows NERC/CIP standards.

**Relevant Experience**

**The C.A.S.E Group**

As a Cybersecurity Business Analyst, Ali supported a consultative project engaging in Continuous Diagnostic & Monitoring (CDM) implementation for the Internal Revenue Service (IRS), which provides tools & capabilities that identify cybersecurity risks on an ongoing basis, prioritizes these risks based upon potential impacts, and enables cybersecurity personnel to prioritize mitigation of the most significant problems for the organization. Ali assisted with the strategic deployment of Risk Monitoring-based software, such as SailPoint, Archer, CyberArk, and Splunk to assist organization in achieving desired IT security posture with regards to Identity & Privileged Access Management. Ali aligned CDM standards, frameworks and security with overall IRS business and technology strategy to help achieve organizational goals.

**Deloitte & Touche**, **LLP**

As a Cyber Risk Consultant, Ali supported the assignment, implementation, and assessment of Federal Cybersecurity Security & Privacy Framework & Standards (NIST 800-30, 800-53, & 800-53A) under the IRS regarding National Institute of Science and Technology (NIST) Security & Privacy Requirements Gathering & Analysis, and basic Risk Management approaches. Ali supported and enhanced security team accomplishments and competence by planning delivery of solutions, including the preparation of system security reports by collecting, analyzing, and summarizing data and trends. Ali participated in firm initiatives such as proposal development, community service, and campus recruiting efforts at the University of Maryland.

**Deloitte & Touche, LLP**

As an Information Technology Intern, Ali documented problems and resolutions for knowledge bases, original equipment manufacturer (OEM) vendors, and service desk tickets. Ali provided PC hardware and software deployment and support. He also adhered to policy and Service Level Targets through accurate recording of service activities, asset transactions, data retention, and PC compliance activities. Ali participated in team building activities, such as attending Deloitte University for their annual intern conference.

### 2.1.17 Beverly Nyarko, Subject Matter Expert

**Certifications**

- CompTIA Security Plus +
- Certified Information Security Manager (CISM)

**Degree/Education**

- BS, Information Technology, Howard University

**Total Years of Experience:**

10 Years

**Relevant/Key Qualifications**

Beverly Nyarko has performed assessment of information systems, based upon the Risk Management Framework (RMF). She has experience conducting security control assessment based on NIST SP 800-53A. Beverly has a familiarity of authorization tools and risk management tools and is capable of developing and maintaining assessment process documentation and continuous monitoring of existing systems with approved ATO. She has conducted IT controls risk assessments that include reviewing organizational policies, standards, procedures and NIST guidelines. Beverly has experience ensuring non-compliance of security control is remediated using the Plan of Action & Milestones (POAM) process.

**Relevant Experience**

**Guidehouse**

Beverly is a Senior Cybersecurity Consultant with a working knowledge of NIST 1-800-53 controls, Assessment and Authorization process, POAM management, System Security Plan. Beverly also has a working knowledge of technology key performance indicators and cybersecurity vulnerabilities critical to identifying impactful capabilities and standards for securing government stakeholder’s critical assets, including new or refined assessments, baselines and/or technical requirements for various services. Beverly understands compliance requirements, standards, and guidelines governing security within the Federal Government (e.g., NIST publications, FISMA, and OMB memoranda) and has demonstrated an ability to apply fundamental cybersecurity principles and concepts to tasks and projects. Beverly have experience with cybersecurity risk management, research and development, and leading practices. As a result of those experiences Beverly is skilled at effectively prioritizing workload to meet deadlines and work objectives.

**Goldbelt Hawk LLC**

Beverly performed Security Assessment (Assessment and Authorization(A&A) on moderate information systems as part of an active third-party assessment organization in accordance with the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). She completed comprehensive test plans for identified security controls following NIST 800-53, FedRAMP guidance, and or agency-specific guidance. She produced complete, accurate, and timely findings reports (SAR, RAR, POAM, ATO Briefing, etc.). Beverly promoted an environment of continuous process improvement, learning and team collaboration. Beverly is familiar with information security and assurance principles and associated supporting technologies.

**Think Tank**

Beverly assessed security controls in accordance with NIST 800-53 security standards, frameworks, laws, and policies. She coordinated groups (government and contractors) to ensure consistency and completeness of policies, procedures, processes, and strategies. Ensure compliance with the standards and organization requirements relative to specific assignments. She ensured the quality assurance of security assessment results in system security packages and non-compliance of security control is remediated using the Plan of Action & Milestones (POAM) process. Beverly was responsible for assessing and maintaining security controls for a FIPS 199 high category federal information system against Federal guidelines and policies. She developed and maintained System Security Plans (SSP), Contingency Plans, Business Impact Analyses (BIA), Plan of Action and Milestones (POAMs), and other security related documentation. Beverly stablished and satisfied information assurance and security requirements based upon the analysis of user, policy, regulatory, and resource demands. Beverly reviewed, monitored, and reported Plan of Action and Milestone (POAM) status to all stakeholders and follows up with appropriate personnel to ensure that POAMs are remediated and reported in a timely manner to the POAM Manager.

**Aitheras**

Beverly managed the information security function in accordance with the established policies and guidelines. She established and maintained information security policies, procedures, and guidelines pursuant Federal laws and regulations such as the Federal Information Security Act (FISMA). She assessed security controls using the NIST SP 800-53A publication guideline. Beverly supported in the creation of Security Assessment Plan (SAP) and SAR detailing the results of the assessment. She conducted meetings with the client to discuss client's material weaknesses identified in an assessment to gain an understanding and develop mitigation strategies for the findings. Beverly reviewed security policy documents and made recommendations on documentation consistent with NIST requirements and Utilize Risk Management Framework process in the routing of an ATO package. She conducted and performed continuous monitoring based on NIST Guidelines requirements. Beverly provided migration strategies and recommendations to key stakeholder.

**Cycomb**

Beverly provided security analysis and assist with the review of a federal client's security policy directives. She was responsible for risk management activities such as tracking Plan of Action and Milestones (POAM). She supported Assessment and Authorization (A&A) activities such security controls Pre-assessments. Beverly worked with stakeholders to ensure the identified weaknesses from vulnerability scans are remediated in accordance with defined remediation time frames and supported activities for Assessment and Authorization (A&A) of new systems, and Information Security Continuous Monitoring (ISCM), in compliance with NIST SP 800-53 controls within the Risk Management Framework (NIST SP 800-37). Beverly participated in client status meetings and submitted weekly/monthly status reports. She reviewed and approved the IS Security Control Assessment Procedures, the Security Assessment Plan (SAP), the System Security Plan (SSP), and the Security Control Traceability Matrix (SCTM). She conducted follow up meetings to assist ISSOs and System Owners to close POAM items and performed assessments of information systems, based upon the Risk Management Framework (RMF). Beverly conducted IT controls risk assessments that include reviewing organizational policies, standards, procedures, and NIST guidelines. Beverly performed evaluation of policies, procedures, security scan results, and system settings to address controls that are insufficient during conducting the A&A and Risk management Framework efforts. She created Security Assessment Report, and Security assessment Plan, and other documents per NIST 800 guidelines and participated in client status meetings and submit weekly / monthly status reports. Beverly created Plan of Action and Milestones (POAM) for vulnerabilities identified through the assessment and security scans.

## *2.2 Experience with Similar Governmental Entities*

### 2.2.1 Allegheny County – Cyber

| Contractor | Guidehouse | |
|---|---|---|
| Contract/Project Title | Allegheny County – Cyber | |
| Client Name | Allegheny County Department of Human Services | |
| Client Address | Human Services Building<br>1 Smithfield St.<br>Pittsburgh, PA 15222 | |
| Point of Contact | Name | Akosua Baiden |
| | Title | Assistant Chief Operations Officer |
| | Telephone | 412-350-3809 |
| | Email Address | Akosua.Baiden@AlleghenyCounty.US |
| Contract Information | | |
| Total Contract Value | $4,000,000 | |
| Period of Performance | July 1, 2022 - June 30, 2025 | |
| Description of Services/Scope of Work | | |

| Contractor | Guidehouse |
|---|---|
| Guidehouse is engaged to perform a broad array of cybersecurity advisory services for both on premise and cloud-based infrastructure and applications supporting the mission of Allegheny County DHS. The scope of our services includes cyber risk assessments and remediation road mapping, compliance and governance reviews (i.e., HIPAA, NIST, IT audit liaison support), policy development, and cyber workforce transformation.<br>The initial phase of our project includes a comprehensive current-state cyber assessment to develop an overall maturity profile using the NIST Cybersecurity Framework (CSF). Through inspection and observation of key cyber processes, workflows, and policy as well as inquiry with IT security and business process stakeholders, our team applies a scoring algorithm to measure cyber readiness and maturity against the following NIST Cyber Functions:<br>**IDENTIFY**: Our team assesses the organization’s ability to maintain an inventory of critical hardware/software and accurately document their system security architecture. We also perform a comprehensive review of their IT Governance and Risk Management programs.<br>**PROTECT:** Technology-focused assessment that evaluates configuration and deployment of protective technology such as identity and access management tools, source code repositories, data encryption, and system patching and maintenance.<br>**DETECT:** Evaluation of how people, processes, and technology work together to discover adverse events within their environment. Our team reviews security incident event monitoring (SIEM) technology, intrusion detection/protection systems, and firewall settings against hardened configuration baselines.<br>**RESPOND:** Focus on the organization’s ability to alert, investigate, and rapidly initiate mitigation and eradication efforts when threats are introduced to the environment.<br>**RECOVER:** Assesses the resiliency, contingency plans, and continuity of operations for a wide array of disruption scenarios.<br>After the current-state maturity profile is developed, our team will work closely with County stakeholders to establish a “target state” profile for each of the NIST CSF Functions. We will then shift into a remediation phase which will help the Department address control gaps and vulnerabilities through implementation of the people, processes, and technologies that align with DHS’s objectives, modernization strategy, and resourcing. | |

### 2.2.2 New York DOT IT and OT Assessments – Cyber

| Contractor | Guidehouse | |
|---|---|---|
| Contract/Project Title | New York DOT IT and OT Assessments – Cyber | |
| Client Name | New York State Department of Transportation,<br>Office of Traffic Safety and Mobility | |
| Client Address | 50 Wolf Road POD 5-3, Albany, NY 12232 | |
| Point of Contact | Name | Rebecca Gibson-Schott |
| | Title | Assistant Director, TSMO Program Development and Operations |
| | Telephone | (518) 457-1951 |

| Contractor | Guidehouse | |
|---|---|---|
| | Email Address | rebecca.gibson-schott@dot.ny.gov |
| Contract Information | | |
| Total Contract Value | $1,198,639 | |
| Period of Performance | November 1, 2022 – April 30, 2024 | |
| Description of Services/Scope of Work | | |

Guidehouse is performing a current state cybersecurity assessment of information technology (IT) systems with operational technology (OT) environments across regional

traffic management centers (TMCs) in New York – ten (10) TMC locations in all. Our team is developing a cyber maturity profile based on the NIST Cyber Security Framework (CSF), and will be delivering a future state roadmap for improving cyber posture across NYSDOT, and performing technical testing (diagnostics and vulnerability scanning) for hardware and communication infrastructure.

The initial phase of our project involves conducting onsite assessments at the TMC locations. The team delivers a discovery questionnaire to each location for the staff to review and complete. Once the questionnaires have been reviewed and discussed with the TMC locations, the team conducts an onsite assessment of the IT and OT infrastructures to identify and document cybersecurity gaps in policies and processes. Th identified risk findings are used to create a maturity profile using the NIST Cybersecurity Framework (CSF). The risk findings are documented and presented in a current state assessment report for each TMC location.

The second and final phase of the project will see the team take the current state assessment findings to inform a future state roadmap for implementing risk mitigation measures. The objective of the future state roadmap is to conceptualize the future of transportation with interviews of key transportation technologists and anticipate IT and TOC needs. The future state vision report and presentation will include:

- Expected entities that we will be leveraging the future IT and or OT/ITS infrastructure
- Layer 3 network capabilities and requirements
- 24/7/365 required operational capabilities
- Data center distribution, redundancy, and disaster recovery capabilities
- Vision for connected and automated vehicles, infrastructure to the vehicle, critical infrastructure, radios, etc.

### 2.2.3 Massachusetts State Lottery Commission (MSLC) - Security Readiness Assessment

| Contractor | Guidehouse | |
|---|---|---|
| Contract/Project Title | Massachusetts State Lottery Commission (MSLC) - Security Readiness Assessment | |
| Client Name | MSLC | |
| Client Address | 150 Mount Vernon Street, Dorchester, MA 02125 | |
| Point of Contact | Name | Thomas Cream |

| Contractor | Guidehouse | |
|---|---|---|
| | Telephone Number | 781-849-5543 |
| | Fax Number | |
| | Email Address | Tcream@masslottery.com |
| Contract Information | | |
| Total Contract Value | $325,000 | |
| Period of Performance | March 1, 2021 - June, 30, 2021 | |
| Description of Services/Scope of Work | | |
| Guidehouse performed the assessment prior to RTC Application going-live by following a rigorous assessment methodology based on NIST 800-53, MUSL rules, International Standards Organization (ISO)/IEC 27001:2013 standard along with the World Lottery Association (WLA) Security Controls Standard (SCS):2020. Team members brought years of experience in InfoSec, penetration testing, financial systems, financial fraud control, and the lottery industry. The team tested security controls throughout the Application using a variety of methods, including black box and grey box testing, review of fraud controls, configuration reviews, and other system and data security testing. Our final report provided detailed findings and remediation recommendations. | | |

# 3.0 Description of How Guidehouse Proposes to Perform the Services Detailed in Section 2 in Compliance with the Standards Detailed in Section 3

## *3.1 Information Technology Management Services*

Guidehouse provides world-class IT management services to public and commercial organizations of all sizes and missions. We leverage proven approaches to support enable organization-wide initiatives for federal, state, and local customers in planning, implementing, and managing key IT infrastructure and system deployments and related projects for updating and improving their IT security risk postures.

Guidehouse is fully qualified to assist Michigan Municipal Services Authority with this project and will leverage our team's experience and knowledge with managing IT service deployment and implementation.  We understand how organizations like Michigan Municipal Services Authority rely on available, reliable, and secure IT services to support the daily operations in supporting the people and business whose lives depend on the efficient delivery of those services. Our IT professionals have recognized and industry-standard IT certifications to effectively manage and support IT infrastructure components and services. Our teams partner with our clients to understand and learn the current IT infrastructures in place and identify any gaps where additional support is needed. We have worked with large federal and state government organizations including Department of Justice, New York State Department of Transportation, and others to manage, maintain, and upgrade IT services to improve the service and mission delivery of our clients.

Guidehouse relies on agile project management and ITIL-based framework that enables organizations to design, develop, deploy, maintain, and improve delivery of key IT tools, policies, and services. We have supported organizations with multiple teams using in-person and remote resources spread across numerous locations that include in-person and remote resources. Guidehouse also relies on its access to qualified and able IT professional resources to scale up on projects and initiatives requiring surge support to resolve complex IT problems in a short timeframe. To manage operations, we leverage various collaboration tools, such as Jira, SharePoint, and Microsoft Teams along with daily stand-ups, and Agile Sprint ceremonies to keep everyone informed on issues, risk, and priorities requiring our immediate attention. While Guidehouse employs an agnostic approach to IT tool and service deployment, we have access to multiple IT professionals and experts with experience and knowledge of deploying and managing IT services supporting on-prem and cloud-based technologies, tools, and related policies and procedures.

IT Infrastructure Network Management

Guidehouse will meet with the organization requesting IT management services to learn and gain an overview of the network components making up their IT infrastructure network. Our team will review the hardware devices (firewalls, servers, laptop and desktop devices) and software products (antivirus, OS, anti-malware) to determine the appropriate resources to support the network and software components. We will also review the portions of the IT infrastructures that are housed onsite at the organization’s facilities versus cloud-based at a third-party provider’s facilities. Guidehouse will also learn the tools used to conduct proactive monitoring and provide alerts to the organization on potential service degradation or disruption to the organization’s network and services and whether security incidents have occurred. This will enable Guidehouse and the organization to determine and map the appropriate number of in-person and remote resources required to provide and deliver the service at a high success rate.

Once the number of resources has been determined, Guidehouse will develop and present a detailed project plan outlining the key tasks for managing the IT services and the required metrics and deliverables to track and document the team’s actions. The project plan will also include processes for escalating issues to resolve that are impacting the organization’s ability to meet its mission and serves its citizens.

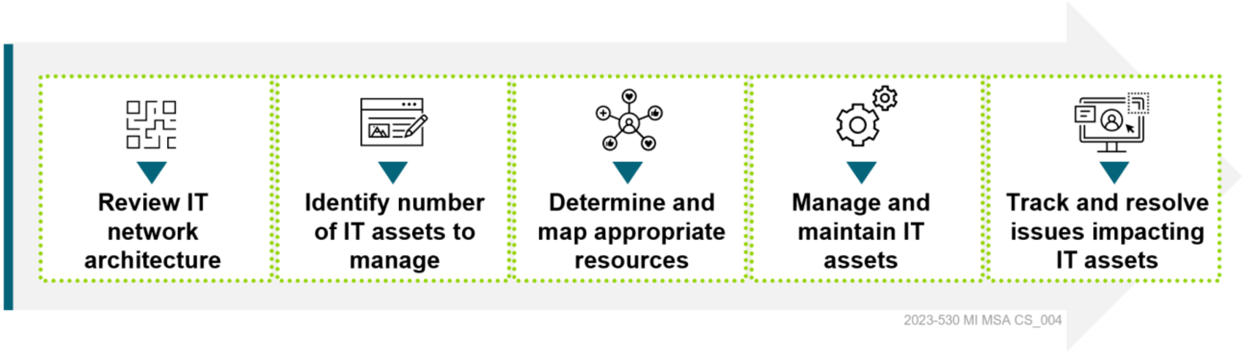

Review IT network architecture
Identify number of IT assets to manage
Determine and map appropriate resources
Manage and maintain IT assets
Track and resolve issues impacting IT assets
2023-530 MI MSA CS_004

**Figure 2. IT Management Service Process Steps**

## *3.2 Cybersecurity Assessment Services:*

Guidehouse is a leading global provider of consulting services to the public and commercial markets with broad capabilities in management, technology, and risk consulting, we help clients address their toughest challenges with a focus on markets and clients facing transformational changes, technology-driven innovation and significant regulatory pressure. Across a range of advisory, consulting, outsourcing, and technology / analytics services, we help clients create scalable, innovative solutions that prepare them for future growth and success.

Guidehouse is highly qualified to assist Michigan Municipal Services Authority with this project and already has significant experience conducting cyber security services including program level assessments, implementing technical solutions, and conducting cyber security trainings. Our cybersecurity professionals have multiple industry certifications including CISSP (Certified Information Systems Security Professionals). Guidehouse partners with its clients to assess, design, implement and train on robust security practices. Guidehouse has worked with several large and vertically integrated government entities such as Los Angeles Department of Water and Power, California Department of Water Resources, and New York Power Authority to make program level assessments, implement enhancements, and establish sustainable knowledge management and training programs. Further, across these areas, the Guidehouse team has worked with international entities such Dubai Electric and Water Authority, Abu Dhabi Distribution Company and Puerto Rico to make enterprise level cybersecurity improvements.

The Guidehouse team has recognized industry and reliability compliance experts. Our team has cybersecurity experts, not just in utilities and energy industry but also in healthcare and finance industries given a unique broad range of cyber security experience that is unmatched. Given our diverse cyber security experience, we are confident we can fully support the Authority in attaining its overall cyber security program development goals.

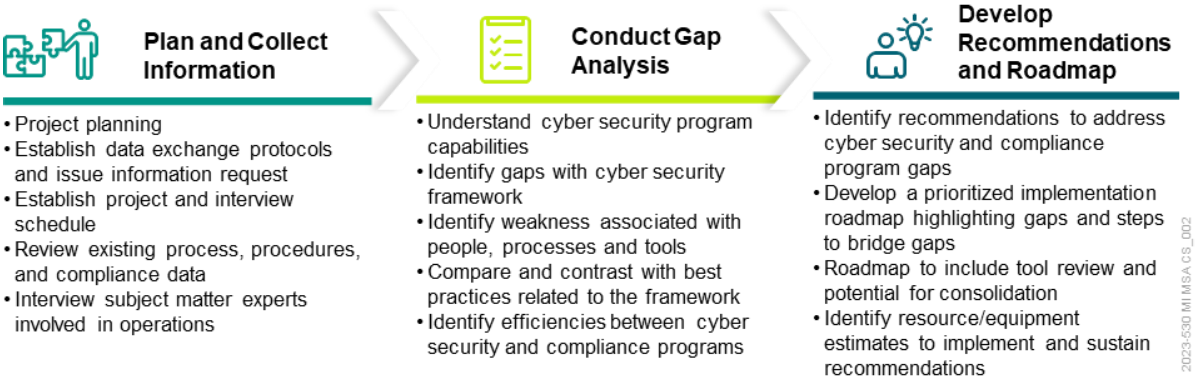
We bring a customer-focused approach aligned to your strategic objectives. We are not beholden to any specific system, tool, or product vendors. Our objective is to understand your business, and drive optimal enabling solutions, rather than forcing your business to adjust to vendor technology. Guidehouse offers best in class risk and cybersecurity consulting, combined with industry leading expertise in emergency management, disaster recovery, and system hardening. Our team includes experts with over thirty years' experience as cybersecurity and IT experts.

Cyber Security Program Assessment

Guidehouse will assess the Authority cybersecurity program and provide an independent assessment of current information technology security measures and provide recommendations, both short and long-term planning to increase the overall cybersecurity posture of the Authority. Additionally, Guidehouse will provide recommendations for information security best practices, guidance on best practices for designing, developing, and sustaining a strong cyber security program with associated metrics. The assessment will also review all tools in place, determine which tools are in line with best practice, and offer recommendations for tool consolidation where appropriate. Guidehouse will also assist with implementation of recommendations based on understood priorities and identified vulnerabilities.

This assessment will require information gathering through available documentation, off, and on-site collaborative discussions, and analysis to compare the current state against a desirable future state based for a best-in-class utilities cyber security program. Additional data points will be provided through reviews of, as available, vulnerability scans and other means.

Guidehouse team of experts will protect the Authority's data using encrypted secure sharing of data as needed and will remove any data as directed by the Authority at the end of the project/term. **Figure 3** highlights our approach to this project.



**Plan and Collect Information**

- Project planning
- Establish data exchange protocols and issue information request
- Establish project and interview schedule
- Review existing process, procedures, and compliance data
- Interview subject matter experts involved in operations

**Conduct Gap Analysis**

- Understand cyber security program capabilities
- Identify gaps with cyber security framework
- Identify weakness associated with people, processes and tools
- Compare and contrast with best practices related to the framework
- Identify efficiencies between cyber security and compliance programs

**Develop Recommendations and Roadmap**

- Identify recommendations to address cyber security and compliance program gaps
- Develop a prioritized implementation roadmap highlighting gaps and steps to bridge gaps
- Roadmap to include tool review and potential for consolidation
- Identify resource/equipment estimates to implement and sustain recommendations

**Figure 3. Cybersecurity Assessment Services Process Steps**

Plan and Collect Information

Guidehouse consultants are supported by a proven methodologies and tools which accelerate our work, align expectations and help deliver quality results.

Guidehouse initiates a planning process that will provide the information necessary for the success of the assessment project. We will initially discuss the project planning options with the Authority to determine:

- Secure data exchange
- Determination of the Authority's SMEs
- Protocols for data gathering

Guidehouse will provide a detailed project plan that will outline the tasks of each process step leading to the interim and final deliverables. Within the project plan, Guidehouse will work with the Authority to set interview schedules, project update meetings, and appropriate level of stakeholder communication.

Information gathering will consist of SME interviews, and documents/process relating to:

- Structure of the cybersecurity organization

– Functions covered and grouping of functions
– Cybersecurity areas for IT/OT
– Cyber security architecture
– Cyber security governance
– Integration of functions within department

▪ Risk management
▪ Incident response
▪ Cyber Threat Intelligence
▪ Disaster Recovery
▪ OT Cybersecurity

- Cybersecurity risk and vulnerability management:
  - Risk framework selection and implementation
  - Effectiveness of risk management practices
  - Integration of risk management into organizational decision making
- Any required compliance efforts and results
- Tools deployed and pending deployment
- Roles & Responsibilities of:
  - Groups within the cybersecurity organization
  - Cybersecurity governance committee(s)
  - Operational groups as it relates to cybersecurity and operations
- Cybersecurity metrics:
  - Selection of metrics appropriate at each supervisory level (group, organization, committee(s), board)
  - Efficiency of metrics as risk quantifier
  - Controls on metrics (for accuracy and completeness)
- Internal customer SLAs/SLOs
- Current risk assessment method

Data gathered will be securely stored in accordance with all data protection requirements.

Conduct Gap Analysis

Guidehouse will utilize the information gathered to understand the Authority's cybersecurity program capabilities and posture. Analysis based on both industry (NIST) and best practices to identify gaps within the cyber program. This includes identifying weaknesses associated with people, processes, and deployed tools.

In addition to the gap analysis, Guidehouse will review the data and categorize as IT, OT, compliance, and data that may be shared between the three cyber focuses. Reducing redundancies through consolidation and provide opportunities to increase efficiencies.

Understanding the Authority's cyber security program capabilities, risk tolerance, and overall cyber security culture will provide additional data points into the overall analysis and to identify any weaknesses. Guidehouse recognizes that each entity has unique strengths and areas of opportunities. These all factor into each review to identify gaps within the current cyber program and provide a benchmark for comparison with security best practices.

Additionally, Guidehouse will identify any weaknesses within the tools used by the Authority's security program. It is important to have a balance of tools to provide a suitable defense in depth strategy, but often, utilities will over purchase tools leading to a confusing array of redundant tools and processes. Guidehouse will evaluate all the security tools and provide expert feedback on any redundancies or areas of potential consolidation to remove duplicate tools and reduce OpEx spending.

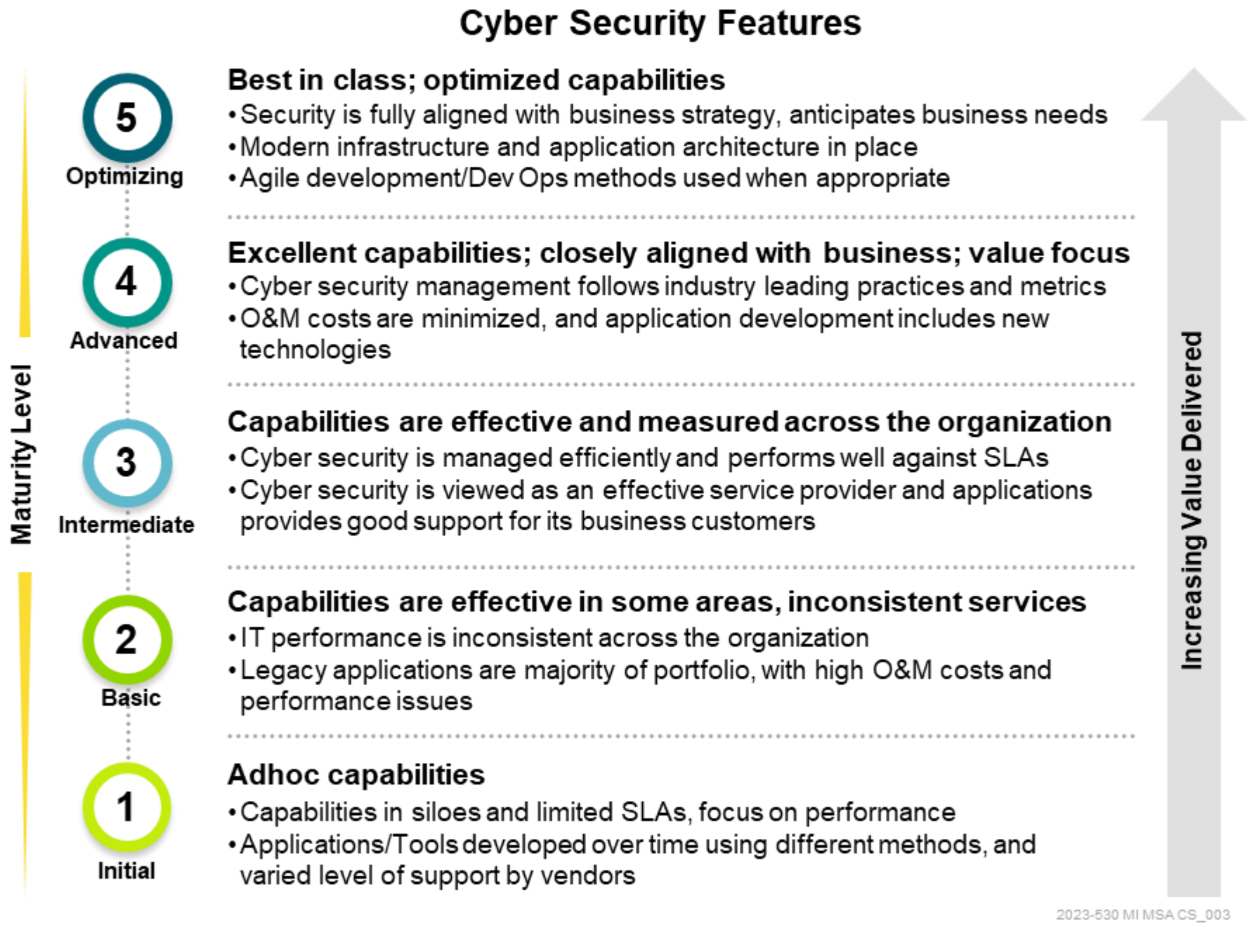

Cyber Security Features
Maturity Level
5
Optimizing
Best in class; optimized capabilities
•Security is fully aligned with business strategy, anticipates business needs
•Modern infrastructure and application architecture in place
•Agile development/Dev Ops methods used when appropriate
4
Advanced
Excellent capabilities; closely aligned with business; value focus
•Cyber security management follows industry leading practices and metrics
•O&M costs are minimized, and application development includes new technologies
3
Intermediate
Capabilities are effective and measured across the organization
•Cyber security is managed efficiently and performs well against SLAs
•Cyber security is viewed as an effective service provider and applications provides good support for its business customers
2
Basic
Capabilities are effective in some areas, inconsistent services
•IT performance is inconsistent across the organization
•Legacy applications are majority of portfolio, with high O&M costs and performance issues
1
Initial
Adhoc capabilities
•Capabilities in siloes and limited SLAs, focus on performance
•Applications/Tools developed over time using different methods, and varied level of support by vendors
Increasing Value Delivered
2023-530 MI MSA CS_003

**Figure 4. Cyber Security Features**

In addition to the comprehensive gap analysis, Guidehouse provides a compare with industry standards relevant to the Authority. NERC frameworks are included in the review to assure the future state of the Authority’s cyber security footprint is in-line with these frameworks. Additionally, this is another opportunity to minimize redundant processes and policies.

After the evaluation of the environment was complete, Guidehouse will prepare the following deliverables:

Typical deliverables would include:

1. Final report containing the following
    a. Current cybersecurity measures based on the Guidehouse review
    b. Recommendations based on the Authorities priorities for identified vulnerabilities
    c. Short- and long-term planning recommendations to increase overall cybersecurity posture
    d. Review of implemented and recommended best practices based on standardized frameworks such as NIST
    e. Gap analysis to recommended practices
    f. Prioritized steps to implement recommendations (with duration/resource estimates)
    g. Estimate of ongoing resources required to maintain recommended practices
2. Implementation Plan schedule

After review and approval of the review documents, Guidehouse will continue with assisting with the implementation of the recommended/approved changes to increase the overall cybersecurity posture.

The Guidehouse team of experts will work closely with the Authorities cybersecurity engineering and operations teams to implement recommendations these could include such implementations as:

1) Implementing changes based on vulnerability scans and observations
2) Modification / clean-up of boundary protection systems (firewalls/IDS)
3) Implementing architectural changes to improve overall cybersecurity posture
4) Amending documents such as policies/procedures to increase efficiencies and create documentary evidence of compliance as required

# 4.0 Other Information Required Under Sections 4(B), 4(C), and 4(D)

## *4.1 4(b) Mandatory Qualifications*

### 4.1.1 Capability to Perform the Services Proposed

Our mature project management approach to performing the work will be utilized from day one to track work progress, budgets, and deadlines. These include:

- During project kick-off, Guidehouse will establish project governance, meeting cadence and reporting process, all with client collaboration and approval.
- Our project and stakeholder management approach focuses on managing expectations throughout the project duration, including establishment of key milestones, stakeholder needs, influence and expectations, transparent communication and issue resolution, proactive risk management, and a consistent approach to quality management.
- Guidehouse will develop a project schedule and workplan which features a high-level view of the project phases. Guidehouse will detail the tasks, durations and responsibilities into a project management plan used to drive the work.
- Our project governance structure will include weekly touch points, stakeholder interviews, and regular executive briefings.
- Finally, Guidehouse will develop a Communication Plan that is informed by the governance and organizational structure and support effective project integration for the duration of the engagement through our systematic, well-defined communication forums.
- Guidehouse, as evidenced by our prior experience, aims to deliver services in a competent, professional and cost-effective manner. We understand the requirement to not subcontract without prior approval and will keep the Authority informed of our progress using the methods outlined above, if awarded.

## 4.1.2 Detailed Description of Guidehouse's Relevant Prior Experience

### 4.1.2.1 Department of Justice (DOJ) Cybersecurity Services Staff (CSS)

| Contractor | Guidehouse |
|---|---|
| Contract/Project Title | Department of Justice (DOJ) Cybersecurity Services Staff (CSS) |
| Contract/Project Information | |
| Total Contract Value | $12,901,576 – Original<br>$45,647,164 – Bridge<br>$16,141,746 – Bridge 2 |
| Period of Performance | October 2015 – June 2018 – Original<br>July 2018 – December 2021 – Bridge<br>December 2021 – September 2022 – Bridge 2 |
| Description of Relevant Services/Scope of Work | |
| Guidehouse provides program management, strategic planning, project management, engineering, operations, policy, and technical support to the DOJ OCIO. The team's support has enabled department-wide initiatives such as the deployment of Office 365, shaped the Department's ICAM strategy, implemented the Secure Enclave, assessed the Department's Data Center Strategy, guided the Technical Reference Architecture, and updated DOJ policies improving the security posture and the use of shared services all in support of the mission.<br>Team Guidehouse manages all operational aspects of the DOJ's Secure Enclave, which hosts the Department's Cybersecurity systems, including Splunk, Active Defense, Guardium, SailPoint, and BigFix. Over 7TB of data transverse the secure enclave daily, requiring a robust and flexible architecture design. Our activities included managing 25+ systems and 1000+ assets in the secure enclave, providing infrastructure enhancements through server deployment in lieu of the Solarwinds incident, and developing and implementing a DOJ Cloud Strategy. | |

### 4.1.2.2 Cook County, Illinois

| Contractor | Guidehouse |
|---|---|
| Contract/Project Title | Cook County, Illinois |
| Contract/Project Information | |
| Total Contract Value | $35,000,000 |
| Period of Performance | August 2017-Present |
| Description of Relevant Services/Scope of Work | |
| Guidehouse was originally contracted to provide IV&V services for a large-scale court management system implementation from Tyler Technologies. The team conducted regular deliverable reviews and provided recommendations on improved practices, project management, and risk assessments. As a result, the County further engaged Guidehouse to provide program management services for Tyler Technologies' implementation of the Integrated Property Tax System between three large County agencies. | |

| Contractor | Guidehouse |
|---|---|
| Guidehouse leads the PMO by reporting project status, identifying risks and issues, and providing actionable recommendations to mitigate risk on a high-profile engagement. Guidehouse advises client leadership on project objectives, scope and schedule to enhance program governance and engage stakeholder agencies across the implementation. The team continuously evaluates the implementer's approach and monitors testing to assess the overall quality of the implementation. Guidehouse conducts detailed analysis of implementer's business requirements documents to identify gaps, collaborates with vendor to execute tasks on schedule, and diligently supports key resource management issues from escalation to resolution. The PMO facilitates overall program decision-making to sustain the project's progress at-scale and meet critical deadlines unique to the complex and unique processes of property tax assessment and collection.<br>Additionally, based on discussions with the program team and the implementation vendor, key vendor deliverables over the lifecycle of the program were improved Guidehouse provided insight and process improvements such as, frequent goal setting and prioritization meetings, coordinated efforts to improve communication between the client and the vendor, and implementing templates and checklists to improve overall delivery. These deliverables included The Guidehouse team worked with the client and the vendor to improve quality and consistency of deliverables and design documentation. Key issues (and potential risks) were identified for each of these significant deliverables along with the impact to the program. | |

### 4.1.2.3 Office of Management and Budget (OMB) A-123 Information Technology (IT) Controls Assessment

| Contractor | Guidehouse |
|---|---|
| Contract/Project Title | Office of Management and Budget (OMB) A-123 Information Technology (IT) Controls Assessment |
| Contract/Project Information | |
| Total Contract Value | • **$1,786,616 (Support 2009 – 2012) / $396,061.65 (Interim 2012)**<br>• **$13,451,953 (2012 – July 2018)**<br>$16,158,645 (July 2018 – Present) |
| Period of Performance | February 2009 – Present |
| Description of Relevant Services/Scope of Work | |
| CIT Information Security Program Support<br>Since 2018, Guidehouse has supported the new CIT Information Security Program with day-to-day security operation monitoring, security control focus area improvements, and audit coordination and support, starting with collection and review of the artifacts requested from CIT during the GAO audit period. Once the GAO field testing concluded, Guidehouse coordinated a centralized tracker for all CIT self-identified observations during the GAO fieldwork and reviewed CIT Service Area remediation efforts for closure of the self-identified findings. For the GAO outbriefs, Guidehouse supported developing narratives for CIT leadership including the Service Area Managers, CIT CISO, Deputy Director and NIH CIO to address the potential | |

| Contractor | Guidehouse |
|---|---|
| programmatic and technical findings that GAO may issue. Once the preliminary Program and Technical findings were received from the GAO, Guidehouse coordinated the CIT responses to the findings and supported OCIO in responses, as well as CIT customers including eRA and ORS/ORF.<br>Guidehouse further is leading efforts at CIT to address three of the root causes of the technical findings, focusing in the areas of asset management, configuration management, and vulnerability management. From the program management findings, Guidehouse has taken stewardship of the ATO packages for all CIT systems from the previous contractors and is currently working with the Service Area teams to update the quality of the packages.<br>**HVA Preparation Assessments.** Guidehouse performed HVA assessments of the Clinical Research Information System (CRIS) and the eRA system. Guidehouse completed an in-depth assessment of the 97 control overlay controls including all NIH InfoSec Policy Handbook requirements through interview, policy and procedure review, reperformance testing of controls, analysis of the network monitoring capabilities, and configuration setting evaluation. Additionally, Guidehouse performed in-depth attack and penetration testing of both CRIS and eRA in a similar simulation to what DHS might perform as part of the Risk and Vulnerability Assessment (RVA). Guidehouse provided each system with a detailed report of the observations, identified recommendations for securing the systems, and met with security personnel and IC leadership to walkthrough each of the findings, and supported remediation efforts through attack and penetration testing and review of remediation activities. GAO made a statement to NIH complimenting the thoroughness and high quality of the preparation assessment documentation.<br>**Security Control Testing.** Guidehouse assessed and documented inheritability of the security controls from the NIH security program and major security projects at NIH. Our team tested and documented numerous security controls to assess NIH in the development and maintenance of policies and procedures for IT governance, risk management, program management, personnel security, systems and information integrity, communication protection, incident response, contingency planning, access control, certification and accreditation, security assessments, and privacy. Guidehouse's assessment included performing an analysis of NIH policies and procedures to determine if the documentation adequately addressed key security risks, and if Federal and HHS departmental standards were being incorporated into the NIH regulatory environment and were complied with and monitored by IT management.<br>**Remediation Support**. Guidehouse has supported the NIH OCIO in the completion of remediation activities for prior year A-123 reviews and external audits. Our team worked with Service Areas and ICs to address questions, explain new control requirements from NIH and HHS, and provided guidance on restructuring or refining remediation activities to address the root cause for issues regarding change management, vulnerability management, and asset management. | |

## *4.2 4(c) Administrative Component*

### 4.2.1 Understanding of the Work

Guidehouse is fully qualified to assist Michigan Municipal Services Authority with this project and will leverage our team's experience and knowledge with managing IT service deployment and implementation. We understand how organizations like Michigan Municipal Services Authority rely on available, reliable, and secure IT services to support the daily operations in supporting the people and business whose lives depend on the efficient delivery of those services.

### 4.2.2 Approach to Performing Services

The Guidehouse team has recognized industry and reliability compliance experts. Our team has cybersecurity experts, not just in the public sector industry but also in healthcare and finance industries given a unique broad range of cyber security experience that is unmatched. Given our diverse cyber security experience, we are confident we can fully support the Authority in attaining its overall cyber security program development goals.

### 4.2.3 Any Expenditures Guidehouse Expects Will Be Absorbed by the Authority (or a Participating Agency) with Applicable Fee or Rate

We do not anticipate any additional expenditures to be absorbed by the Authority.

## *4.3 4(d) Technical Component*

### 4.3.1 Sole Point of Contact for Guidehouse’s Provision of Services to the Authority and Other Personnel that Would Provide Services to the Authority or A Participating Public Agency, Including Educational Background, Certifications, and Professional Licenses Held

Jamie Hamilton will serve as our primary point of contact for this engagement. Jamie’s resume and credentials are included in section 2.

Jamie Hamilton

Phone: 313-774-1770

Email: jhamilton@guidehouse.com

### 4.3.2 Description of the Adequacy of Personnel to Handle Communications With the Authority and Participating Public Agencies

Guidehouse's engagement leaders are knowledgeable professionals bringing years of experience with leading transformations and managing large teams. We pride ourselves on a flexible and proactive approach that uses open communication channels and high levels of quality. This includes the formation and use of daily stand-ups, status updates, program sponsor briefings, and demos of functioning code/configurations as a mechanism for frequent feedback. Guidehouse will also develop a status reporting process that is acceptable to the Authority. With feedback from the Authority and project leadership, Guidehouse will design a project governance structure that includes weekly touchpoints with all necessary stakeholders. The frequent communications provided by this governance structure will enable a collaborative approach to conducting project tasks.

### 4.3.3 Description of the Level of Assistance that Will Be Expected from Authority or Participating Public Agency Staff

Our stakeholder management approach will also focus on several key factors, including early establishment of stakeholder needs, influence, and expectations, transparent communication and issue resolution, proactive risk management, and a consistent approach to quality management. Our team will also work with the Authority to establish a project sponsor on behalf of the Authority. This point of contact will assist with scheduling of meetings and other administrative needs our team will need to complete project tasks.

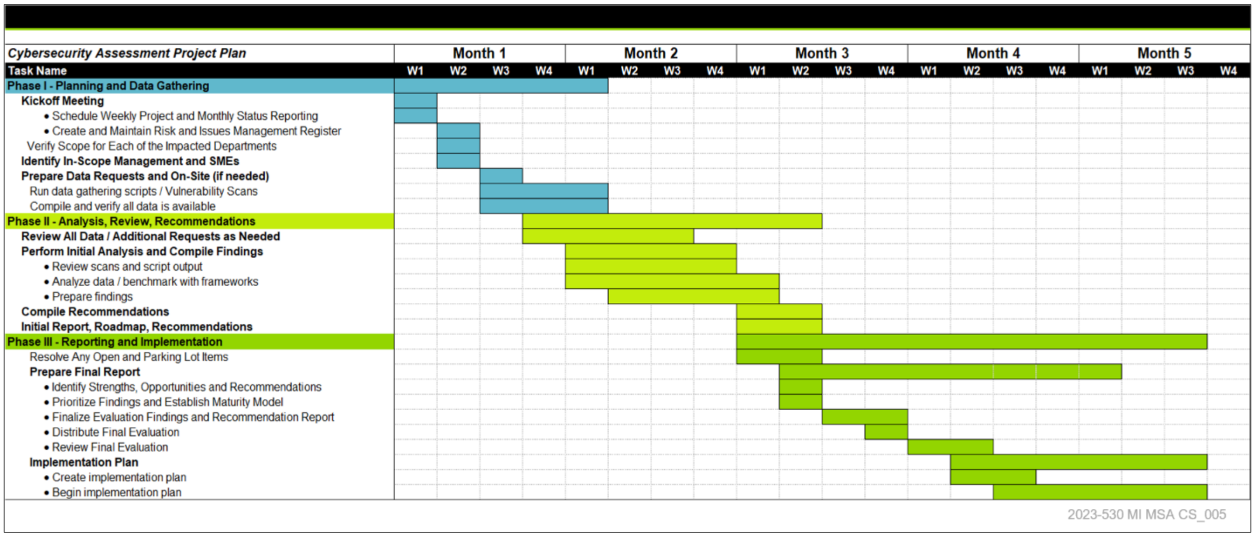
### 4.3.4 Proposed Model Work Plan and Schedule for A Potential Public Agency Client for Both Service Components Described In Section 2

#### 4.3.4.1 Work Plan

Guidehouse schedule to support the operational portion will be based on the needs of the Authority. Initially, Guidehouse will meet with the Authority to review the architecture of the specific site, any special mandates/compliance, and endpoint specifics. After, Guidehouse will provide a specific plan to ensure the operational needs are met on a timely basis. Additionally, Guidehouse will work closely with the Authority to integrate the Guidehouse team of experts into any ITSM solution in use, or propose methods to request, track and catalog operational work efforts. These will be used to provide metrics as to work performed, open issues, and impact to existing or pending projects.

### 4.3.4.2 Schedule

**Figure 5. Cybersecurity Assessment Project Plan**



### 4.3.5 Description of Similar Services Previously Performed for Governmental Entities, including a Contact Name and Phone Number for Each Governmental Entity Referenced

**Table 1. Similar Services Provided to Governmental Entities**

| Governmental Entity | Description of Similar Services | Contact Name | Phone Number |
|---|---|---|---|
| Allegheny County Department of Human Services | Guidehouse is engaged to perform a broad array of cybersecurity advisory services for both on premise and cloud-based infrastructure and applications supporting the mission of Allegheny County DHS. | Akosua Baiden | (412)-350-3809 |
| New York DOT IT and OT Assessments – Cyber | Guidehouse is performing a current state cybersecurity assessment of information technology (IT) systems with operational technology (OT) environments across regional traffic management centers (TMCs) in New York | Rebecca Gibson-Schott | (518) 457-1951 |
| Massachusetts State Lottery Commission (MSLC) - Security | Guidehouse performed the assessment prior to RTC Application going-live by following a rigorous assessment methodology based on NIST 800-53, MUSL rules, International | Thomas Cream | (781) 849-5543 |

| Governmental Entity | Description of Similar Services | Contact Name | Phone Number |
|---|---|---|---|
| Readiness Assessment | Standards Organization (ISO)/IEC 27001:2013 standard along with the World Lottery Association (WLA) Security Controls Standard (SCS):2020 | | |

### 4.3.6 Description of the Manner In Which the Respondent Will Retain and Dispose of Records Related to Its Provision of Services

Guidehouse only retains records related to our assessment of the work performed. Records related to the engagement retained on our systems will be purged at the conclusion of our engagement, unless otherwise requested by the Authority.

### 4.3.7 Statement that the Responder Maintains Comprehensive Liability Insurance and Workers' Compensation Insurance for Its Employees, and Cybersecurity Insurance for Its Activities

Guidehouse maintains General Liability, Auto Liability, Workers Compensation, Employers Liability, Professional Liability Insurance and Cybersecurity. Contact the legal department (SLGcontracts@guidehouse.com) to obtain a Certificate of Insurance for an awarded contract.

### 4.3.8 Description of Any Strategic Relationships the Responder Currently Has or Has Used that Could Bring Significant Value to the Authority or A Participating Public Agency

Team Guidehouse is Michigan-centric with numerous lifelong Michiganders on our team. Our team has worked with and supported almost every State of Michigan Department as well as 23 counties and 33 cities within the State. Whether proudly working in the Upper Peninsula or in downtown Detroit, few firms have either our Michigan public sector reach, our existing Michigan relationships or our Michigan scale.

We deliver exceptional results and have a proven track record on similar work with the State of Michigan. Michigan is a richly diverse place that is home to a wide variety of urban, suburban, rural, and tribal communities, the needs of whom are distinct. We already understand and have proven Michigan experience how to build an inclusive statewide approach for a successful technical assistance center and application support. We currently support the State of Michigan with grants compliance and monitoring for all the State's COVID stimulus funds.  Additionally, last year for the Michigan Department of Treasury, we implemented its technical assistance center and application support process for the Growing MI Business Grant Program. Our team administered over 8,300 applications, fielded over 59,000 emails and over 10,000 calls and facilitated multiple statewide webinars and educational learning sessions to over 3,700 registrants

## 5.0 Price Quote

Based on our understanding of your needs, we are including the following price quote. For your information technology management services, we anticipate sample deliverables to includes:

- Identify and facilitate meetings with IT service stakeholders
- Obtain and review current IT network architecture diagram containing current count of hardware and software assets
- Identify and document questions on IT hardware and software assets
- Develop project plan for managing, maintaining, securing, and repairing IT assets
- Understand the current infrastructure and circumstances
- Identify and facilitate meetings with IT stakeholder to discuss on-site and remote resource requirements and expectations
- Develop and draft IT resource management plan and timeline outlining roles and responsibilities for providing on-site and remote support services
- Identify and facilitate meeting with IT stakeholders to understand on-call resource requirements and expectations

For your cybersecurity assessment services, we anticipate sample deliverables to includes:

- Identify and facilitate meetings with stakeholders
- Review current risk assessments and mitigations in the plan
- Compare and contrast to industry best practices
- Identify recommendations to improve security
- Identify methods to enhance responsiveness to security vulnerabilities
- Develop recommendations to address risks

| ***Phase*** | ***Year one price*** | ***Year two price*** | ***Year three price*** | ***Year four price*** |
|---|---|---|---|---|
| ***Information technology management services*** | ***$115,176*** | ***$115,176*** | ***$119,207*** | ***$119,207*** |
| ***Cybersecurity assessment services*** | ***$98,881*** | ***$98,881*** | ***$102,342*** | ***$102,342*** |
| ***Total cost per year*** | ***$214,057*** | ***$214,057*** | ***$221,549*** | ***$221,549*** |

***Total cost over four years: $871,212***

This price quote is valid for a period of at least 60 days from the date of submission.

Jeffrey Bankowski
Partner, Guidehouse Inc.
1676 International Drive, Suite 800
McLean, VA 22102
Telephone (734) 644-0595

## 6.0 Legal or Regulatory Actions Pending Against the Responder

We are a party to a variety of legal proceedings that arise in the normal course of our business. While the results of these legal proceedings cannot be predicted with certainty, we believe that the final outcome of these proceedings will not have a material adverse effect, individually or in the aggregate, on our results of operations or financial condition.

# Appendix A. Reservation of Rights

Guidehouse

Submission of this proposal by Guidehouse, Inc., or any of its affiliates (the “***Contractor***”), is not an indication of Contractor’s willingness to be bound by all of the terms presented in the Michigan Municipal Services Authority (the “***Client***”) Notice of Request for Proposals, pertaining to Information Technology Managed Services and Cybersecurity Assessment Services (RFP 2023-1) (the “***RFP***”). This proposal in response to the Client’s RFP does not constitute a contract to perform services and cannot be used to award a unilateral agreement. Final acceptance of this engagement by the Contractor is contingent upon successful completion of Contractor's acceptance procedures. Any engagement arising out of this proposal will be subject to negotiation of a mutually satisfactory vendor contract including modifications to certain RFP terms and conditions and including our standard terms and conditions and fees and billing rates established therein.

Given our past history of successfully negotiating mutually agreeable terms with similar State and Local entities, we do not anticipate any difficulty in reaching a contractual agreement (the “***Agreement***”) that will enable us to provide the professional services which you are requesting, while protecting the interests of both parties.

Contractor kindly requests that the Client consider the following additions:

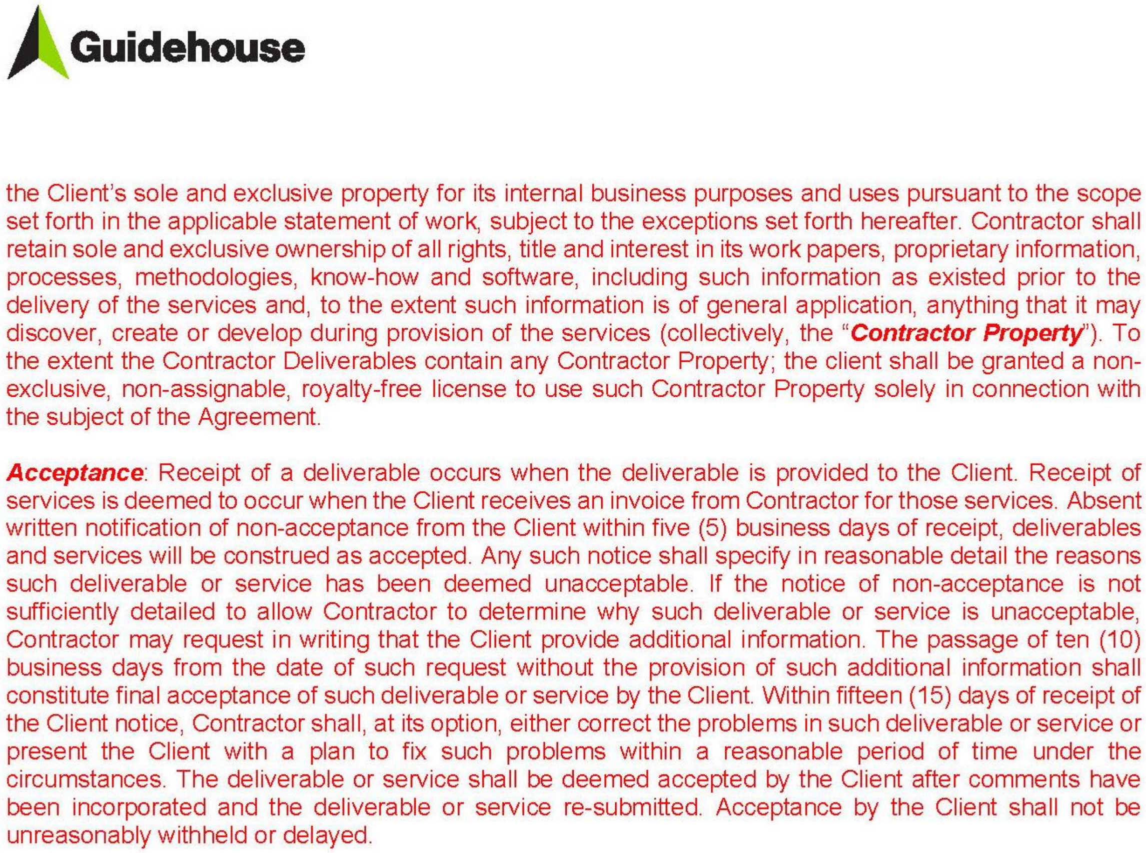
***Limitation on Liability:*** Notwithstanding the terms of any other provision, the total liability of Contractor and its affiliates, directors, officers, employees, subcontractors, agents and representatives for all claims of any kind arising out of the Agreement, whether in contract, tort or otherwise, shall be limited to the total fees paid to Contractor under the applicable statement of work. Neither Contractor nor Client shall in any event be liable for any indirect, consequential or punitive damages, even if Client or Contractor have been advised of the possibility of such damages.

***Consulting Services Disclaimer:*** Contractor will not audit any financial statements or perform any attest procedures in the course of performing the services under the Agreement. Contractor’s services are not designed, nor should they be relied upon, to disclose internal weaknesses in internal controls, financial statement errors, irregularities, illegal acts or disclosure deficiencies. Contractor is not a professional accounting firm and does not practice accounting. Contractor’s services will not include legal, engineering or architectural advice or services.

***Standard of Care and Performance:*** Contractor agrees that the services provided for under the Agreement will be performed in a professional manner in accordance with recognized professional consulting standards for similar services and that qualified personnel will be assigned for that purpose. In providing the services, Contractor and its personnel shall exercise reasonable care. Contractor cannot guarantee or assure the achievement of any particular performance objective, nor can Contractor guarantee or assure any particular outcome for the Client or any other person as a result of the Agreement or the performance of the services contemplated thereunder.

If, during the performance of the services, or within one year following completion of the Agreement, such services will prove to be faulty or defective by reason of a failure to meet such standards, Contractor agrees that upon prompt written notification from the Client prior to the expiration of the one-year period following the completion of the Agreement of any such fault or defect, such faulty portion of the services will be redone at no cost to the Client up to a maximum amount equivalent to the cost of the services rendered under the Agreement. The foregoing will constitute Contractor’s sole warranty with respect to the accuracy or completeness of the services and the activities involved in its preparation, and is made in lieu of all other warranties and representations, express or implied, including any implied warranties of merchantability or fitness for a particular purpose.

***Intellectual Property:*** Upon full payment of all amounts due Contractor in connection with the Agreement, all rights, title and interest in any information and items, including summaries, documents, reports and portions thereof Contractor provides to the Client (collectively, the “***Contractor Deliverables***”) will become



the Client's sole and exclusive property for its internal business purposes and uses pursuant to the scope set forth in the applicable statement of work, subject to the exceptions set forth hereafter. Contractor shall retain sole and exclusive ownership of all rights, title and interest in its work papers, proprietary information, processes, methodologies, know-how and software, including such information as existed prior to the delivery of the services and, to the extent such information is of general application, anything that it may discover, create or develop during provision of the services (collectively, the "***Contractor Property***"). To the extent the Contractor Deliverables contain any Contractor Property; the client shall be granted a non-exclusive, non-assignable, royalty-free license to use such Contractor Property solely in connection with the subject of the Agreement.

***Acceptance***: Receipt of a deliverable occurs when the deliverable is provided to the Client. Receipt of services is deemed to occur when the Client receives an invoice from Contractor for those services. Absent written notification of non-acceptance from the Client within five (5) business days of receipt, deliverables and services will be construed as accepted. Any such notice shall specify in reasonable detail the reasons such deliverable or service has been deemed unacceptable. If the notice of non-acceptance is not sufficiently detailed to allow Contractor to determine why such deliverable or service is unacceptable, Contractor may request in writing that the Client provide additional information. The passage of ten (10) business days from the date of such request without the provision of such additional information shall constitute final acceptance of such deliverable or service by the Client. Within fifteen (15) days of receipt of the Client notice, Contractor shall, at its option, either correct the problems in such deliverable or service or present the Client with a plan to fix such problems within a reasonable period of time under the circumstances. The deliverable or service shall be deemed accepted by the Client after comments have been incorporated and the deliverable or service re-submitted. Acceptance by the Client shall not be unreasonably withheld or delayed.