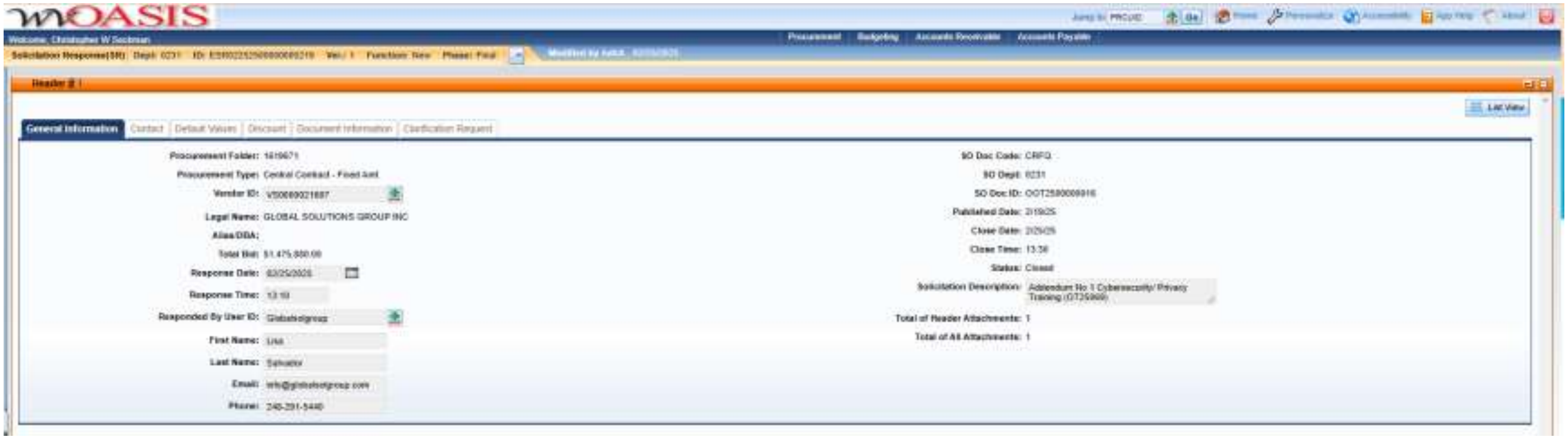
West Virginia
Purchasing Division

2019 Washington Street, East
Charleston, WV 25305
Telephone: 304-558-2306
General Fax: 304-558-6026
Bid Fax: 304-558-3970



Welcome, Christopher W Seckman

Solicitation Response(SR) Dept: 0231 ID: ESR02252500000000219 Ver.: 1 Function: New Phase: Final

Modified by [illegible]

Header # 1

Procurement Folder: 1619671

Procurement Type: Central Contract - Fixed Amt

Vendor ID: VS0000021887

Legal Name: GLOBAL SOLUTIONS GROUP INC

Alias/DBA:

Total Bid: $1,475,800.00

Response Date: 02/25/2025

Response Time: 13:10

Responded By User ID: Globalsolgroup

First Name: Lisa

Last Name: Salvator

Email: info@globalsolgroup.com

Phone: 240-291-5440

SO Doc Code: CRFQ

SO Dept: 0231

SO Doc ID: OOT2500000916

Published Date: 2/19/25

Close Date: 2/25/25

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No 1 Cybersecurity/ Privacy Training (OT25069)

Total of Header Attachments: 1

Total of All Attachments: 1

Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder: 1619671

Solicitation Description: Addendum No 1 Cybersecurity/ Privacy Training (OT25069)

Proc Type: Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2025-02-25 13:30	SR 0231 ESR02252500000005219	1

VENDOR

VS0000021607
GLOBAL SOLUTIONS GROUP INC

Solicitation Number: CRFQ 0231 OOT2500000016

Total Bid: 1475880 **Response Date:** 2025-02-25 **Response Time:** 13:10:45

Comments:

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor
Signature X **FEIN#** **DATE**

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Privacy and Cybersecurity Training Solution	1.00000	YR	358084.000000	358084.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments:

Extended Description:

Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Privacy and Cybersecurity Training Solution-Optional YR2	1.00000	YR	365245.000000	365245.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments:

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Privacy and Cybersecurity Training Solution-Optional YR3	1.00000	YR	372550.000000	372550.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments:

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Privacy and Cybersecurity Training Solution-Optional YR4	1.00000	YR	380001.000000	380001.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Commodity Line Comments:

Extended Description:

Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

Technical and Price Proposal

Solicitation No.: CRFQ 0231 OOT2500000016
Cybersecurity Privacy Training
State of West Virginia

Due Date: February 25, 2025, 1:30 PM

Submitted to:
Toby L Welch
Buyer

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Submitted by:
Global Solutions Group, Inc.

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

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

US DoD Top-Secret Facility Clearance

CMMC C3PAO Candidate – ML3

Contracting Vehicles

GSA Multiple Awards Schedule Contracts

Contract Number: GS-35F-171AA
Categories: 511210, 54151, 54151HACS, 54151S

Contract Number: GS-03F-132DA
Categories: 493110RM, 518210DC, 518210ERM, 541611LIT, 541611O, 561439, 561990

Contract Number: GS-02F-025GA
Categories: 561320SBSA

8(a) Streamlined Technology Acquisition Resource for Services III (8ASTARS3)

Contract Number: 47QTCB21D0281

GSA OASIS+ MAC Small Business

Contract Number: 47QRCA25DSB10

Personnel 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 and proposal@globalsolgroup.com

Acknowledgement of Addenda, Questions and Answers, and other Modifications

GSG acknowledges Addendum 1 received on February 19, 2025.

Submit to:

Toby L Welch, Buyer

State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Email: toby.l.welch@wv.gov
Phone: (304) 558-8802

February 21, 2025

Toby L Welch, Buyer
State of West Virginia
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Subject: Global Solutions Group's Response to Sol No.: **CRFQ 0231 OOT2500000016** for **Cybersecurity Privacy Training**

Dear Mr. Welch,

Global Solutions Group, Inc. (GSG) hereby presents our proposal to provide Cybersecurity Privacy Training to the State of West Virginia (State).

GSG is a multifaceted technology company incorporated in the State of Michigan in 2003. We are headquarters in Oak Park, Michigan. ***We are an SBA 8(a) Certified Small Business, Certified Women Owned Small Business (WOSB), Certified Minority Business Enterprise (MBE), and Economically Disadvantaged Woman - Owned Small Business (EDWOSB).***

GSG is an ISO/IEC 27001:2022 Information Security and Cybersecurity, 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 expertise extends to a wide array of leading IT and cybersecurity technologies through partnerships with Fortinet, Splunk, Redgate SQL Toolbelt - Developer Tool, Twilio, Digital Certificate SFTP Server, AngularJS Extended Support -Developer Tool, Tenable, CrowdStrike, Laserfiche, AWS, ServiceNow, Tanium, CyberArk PAM, Invicti, Azure, Sonatype, Salesforce, Palo Alto, Adobe, SentinelOne, Trellix, Proofpoint, and Zoom.

GSG understands that the State is seeking a qualified vendor to provide customized cybersecurity and privacy training for approximately 25,000 end users. The training must be hosted on a vendor-managed Learning Management System (LMS), with an integrated phishing simulator. The solution should be scalable, track user progress, and ensure effective delivery of security and privacy education.

GSG Value-Add Service

GSG is teaming with KnowBe4.
GSG has a strategic partnership with **KnowBe4** hereafter referred to as the GSG Team. This partnership offers unique advantages to the State in their Cybersecurity Privacy Training requirement as detailed in the following proposal.

KnowBe4 is the world's first and largest new-school security awareness training and simulated phishing platform that helps manage the ongoing problem of social engineering. The KnowBe4 platform is user-friendly, intuitive, scalable, and customizable. The technical section of our proposal will provide more details about our solution. GSG's goal is to implement the most powerful yet easy-to-use platform available. GSG facilitates getting the KnowBe4 platform deployed twice as fast compared to their competitors. Our Customer Success team gets you going in no time, without the need for consulting hours. We help you keep your users on their toes with security at the top of their mind. With this integrated platform you can train and phish your users, see their Phish-prone percentage™ improve over time and get measurable results.

Our certified cybersecurity and IT specialists are here to provide a comprehensive approach to State’s Cybersecurity/Privacy Training 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 continuously enhance our professional credentials. 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.

GSG has completed over 1,000 Cybersecurity Projects over the last Ten Years

Below is a small sampling of customers supported on Cybersecurity Projects:

Virginia Retirement System	Penetration Testing Services
Department of Interior	Awarded a $25+ million BPA contract offering comprehensive cybersecurity services to DOI and other federal agencies
Jacksonville Aviation Authority	Network Penetration Testing
City of New Orleans	Cybersecurity Services
City of San Jose	Providing As-Needed Cyber Products and Services
City of Sunnyvale	Providing IT Strategic Planning, Process Redesign, and Performance - Professional and Technical Support Services
Fort Wayne–Allen County Airport Authority	Completed an IT Security Assessment
San Diego County Regional Airport Authority	On-call IT Cyber Services
Nevada Affordable Housing Assistance Corporation	Provided External Network, Web Application Vulnerability Scanning, and Penetration Testing
Department of Agriculture (USDA) Office of the Chief Information Officer	Completed a $10 million nationwide BPA for Cybersecurity Assessments and Penetration Testing
U.S. AbilityOne Commission	Completed a multiyear contract to provide Federal Information Security Management Act of 2014 (FISMA) Cybersecurity Audit Analysis Services

Point of Contact Details

Name: Lisa Salvador
Title: Vice President
Email: lisas@globalsolgroup.com and proposal@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 State is evaluating proposals. You may contact me at any time.

Regards,

Lisa Salvador

Lisa Salvador
Vice President

Table of Contents

1. *Company Overview*

1.1 GSG's Background and Qualifications

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.

GSG Fast Facts

Years in Business	22 years and incorporated in 2003
Headquarters	Global Solutions Group, Inc. 25900 Greenfield Road, Suite 220, Oak Park, MI 48237
Website	www.GlobalSolGroup.com
Size and Number of Employees	126
Socio Economic Status	• SBA 8(a) Certified Small Business • Certified Women-Owned Small Business (WOSB) • Certified Minority Business Enterprise (MBE) • Economically Disadvantaged Woman-Owned Small Business (EDWOSB)
ISO/IEC Certified Small Business	• ISO/IEC 27001:2022 Information Security and Cybersecurity • ISO 9001:2015 Quality Management System • ISO 20000:2018 Service Management System
Facility Clearance	• DoD Top Secret Facility Clearance • Certification Date: 03/06/2023
CMMC C3PAO ML3	Cybersecurity Maturity Model C3PAO – ML3 certification

	Feature	*Benefit*
★	ISO 27001 Certification ISO 9001 Certification ISO 20000 Certification	*Demonstrates adherence to best practices in information security management.*

GSG has considerable experience in providing cybersecurity services to a broad variety of private and public sector clients GSG is experienced in providing a wide range of IT services throughout the United States and worldwide to local, state, and federal agencies and corporations. We have earned a national reputation as a valuable partner that consistently exceeds customer expectations.

Over the past twenty-two years our business has grown through the development of our four core competencies across multiple business sectors:

Cybersecurity	**IT Services**	**Digital Transformation**	**Physical Security**
Penetration testing, risk assessments, incident response, and security audits.	IT general controls, IT risk assessments, and IT audit programs.	Enterprise content management, document imaging, and workflow management.	Security hardware/software, security engineering, and operational continuity planning.

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 added penetration testing, cybersecurity audits, and assessments as key facets of our business. Our cybersecurity expertise has led to major multi-year contracts with the AbilityOne Commission, as well as a multi-year, multimillion-dollar contract to provide operational assessment and penetration testing to all offices and agencies under the purview of the USDA nationwide.

GSG has Provided Cybersecurity Assessments and Penetration Testing for Over:

- **3,500** Offices and Agencies Nationwide
- **300,000** End Points
- **120,000** Workstations
- **200,000** IPs

GSG was awarded a major cybersecurity assessment contract with the U.S. Department of the Treasury, Office of the Inspector General. Our cybersecurity expertise and subsequent execution has led to major multi-year contracts providing Information System Security Line of Business (ISSLoB) support to the Department of the Interior and client agencies. GSG was awarded a major cybersecurity assessment contract with the U.S. Department of the Treasury, Office of the Inspector General. We recently completed a multi-year, multimillion-dollar contract to provide operational assessment and penetration testing to all offices and agencies under the purview of the USDA nationwide.

We have experience and expertise with industry standards and best practices including:

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

Our cybersecurity expertise has led to major multi-year contracts with:

$26 Million	$5.8M	$1.9M
Department of the Interior *Information System Security Line of Business (ISSLOB) Support Services*	**U.S. Department of Agriculture** *Operational Security Assessments, Penetration Testing and Web Security Assessments*	**Department of Treasury** *Cybersecurity Assessment Service Support*

GSG's cybersecurity team has successfully completed more than 1,000 projects including penetration testing, cybersecurity assessments, audits, vulnerability assessment, web application security assessment, and risk assessments.

Sectors Served

For the past twenty-one years, GSG has serviced the following sectors:

Government	Legal	Financial Services	Commercial	Education	Manufacturing	Healthcare	Non-Profit

Core Competencies

GSG continues to expand our core offerings to our customers. As technology continues to change, we also increase our staff training opportunities and encourage obtaining industry-leading certifications.

GSG Has Supported Four Key Technology Sectors Over the Past Twenty-Two Years:

CYBERSECURITY	• Penetration Testing • Policy and Procedure Development • Risk Assessment • Security Audits • Social Engineering Security Compliance	• Information Assurance • Incident Response Planning Operational Continuity Planning • Education and Training • Security Engineering	• Security Hardware and Software • Security Information and Event Management • Payment Card Industry Assessment
• DIGITAL TRANSFORMATION	• Enterprise Document Management Solutions • Laserfiche • OpenText	• Enterprise Content Management • Case Management • Workflow Management • Enterprise Records Management	• Document Imaging System and Services • Document Digitization • Customer Relationship Management Systems
IT SERVICES	• Cloud Hosting • Licensing • Implementation • IT Support • Help Desk • Backup	• Disaster Recovery • Database Management • SharePoint • IT Managed Services • Telephony • Network Administration	• IT Staffing • Network Architecting • Hardware • Firewalls • SQL
PHYSICAL SECURITY	• Security Cameras/CCTV • Entry Systems • Access Control	• PIV • Personal Identification Systems	• Proprietary alerteerTM Security Monitoring Software

Cybersecurity-Related Services

▪ Penetration Testing	▪ Incident Response Planning	▪ Security Information and Event Management (SIEM)

- Physical/ Electronics Security
- Policy and Procedure Development
- Privacy Support Planning
- Risk Assessment
- Risk Management Framework
- Security Audits
- Security Configuration and Testing
- Security Engineering
- 24/7/365 Security Operation Center (SOC)
- Assessment and Authorization
- Assessment, Integration, Automation
- Chief Information Security Officer as a Service/vCISO
- Identity/Access Management
- Incident Response (IR) and Management Support
- Intrusion Testing
- Operational Continuity Planning
- IoT
- Payment Card Industry Assessment
- Cybersecurity Infrastructure
- Distributed Control Systems
- Education and Training
- Embedded/IoT Services and Systems Hardening
- Firewall Implementation, Configuration, and Testing
- ICS, SCADA Information Assurance
- Security Testing, ADAS, CVIP
- Social Engineering
- Training and Awareness
- Vulnerability Assessment
- Web/Mobile Application Testing
- Security Compliance PCI–DSS, NIST, FISMA, HIPAA, CJIS, ISO, GDPR
- Family Educational Rights and Privacy Act (FERPA)
- Authorization to Operate Authorization to Connect
- Interconnection Security Agreement
- CMMI Support Assessment and Consulting

Strategic Partners

GSG has several carefully chosen strategic partners including partner programs and firms where we are Value-Added Resellers (VAR). Each of our partner companies are leaders in their own IT space and collectively give GSG a direct line of access to leading IT developments which can increase productivity, reduce potential outside issues and provide security solutions. For our client, this means insight into trends, faster updates and patches, and direct support for issues.

Our expertise extends to a wide array of leading IT and cybersecurity technologies through partnerships with Fortinet, Splunk, Redgate SQL Toolbelt - Developer Tool, Twilio, Digital Certificate SFTP Server, AngularJS Extended Support -Developer Tool, Tenable, CrowdStrike, ServiceNow, Tanium, CyberArk PAM, Invicti, Azure, Sonatype, Laserfiche, AWS, Salesforce, Palo Alto, Adobe, SentinelOne, Trellix, Proofpoint, and Zoom.

Microsoft GOLD CERTIFIED Partner ORACLE PARTNERNETWORK	As a Microsoft Gold Certified Partner and a member of the Oracle Partner Network, GSG can provide a comprehensive range of services including network maintenance and support, system engineering, and troubleshooting.
IBM Security Certified MSSP Elite Partner Elite Cyber Defender	For a variety of IBM Cybersecurity software and hardware products, we are an IBM Certified Managed Security Services Provider (MSSP). GSG has an active Embedded Solution Agreement with IBM, which allows them to offer IBM solutions such as IT Security and Cloud. Many members of GSG's team are certified in IBM Cybersecurity technologies such as QRadar, Resilient, and Guardium.
Microsoft Azure aws	We are Amazon Web Services and Microsoft Azure Certified Partners, so our team can provide a wide range of Cloud-based solutions.
FORTINET	We are a member of the Fortinet Partner Program, giving our team access not only to their highly regarded endpoint security products, but their Security-as-a-Service FortiCloud, FortiManager Managed Services, FortiSIEM, and Forti Sandbox services.

MANDIANT	As a Mandiant partner, we are plugged into an industry-leading threat intelligence network. We can provide Mandiant-managed defense system, including Rapid Response to reduce the impact of a security incident. This service avoids the added cost of on-site IR with a swift investigation to stop incidents. Mandiant also provides support to contain potentially compromised assets and guidance for an effective response.
cisco Partner	As a Cisco Partner, we are an authorized integrator of Cisco network architecture and components including routers, wireless, Cisco Digital Network Architecture (CiscoDNA), Cisco Smart Building Solutions, Cisco Mobility Solutions, and other innovative and cost-effective IT technologies.
Trellix	Through our partnership with Trellix, we have access to the combined resources of FireEye and McAfee - two of the industry leaders in IT security. They offer technologies that apply threat intelligence, automation, and case management in a unified security operations platform. They also provide State-Of-The-Art Endpoint Security and Email Security.
tenable	Providers of the leading Cyber Exposure Platform, Tenable is a comprehensive risk-based vulnerability management solution, Tenable.ad, which discovers and prioritizes weaknesses within Active Directory domains and provides the capability to detect and respond to AD attacks in real time.
Laserfiche	Laserfiche is the leading enterprise content management, business process automation, workflow, records management, document imaging and webform software solution.

GSG Value Proposition

The following table outlines how GSG differentiates from other consultants:

GSG Unique Experience	Relevancy to the State
☑ RELEVANT CORPORATE EXPERIENCE	
GSG has experience with: ♦ Long-term, complex security assessments. ♦ Fixing vulnerabilities to improve compliance with regulatory requirements or security standards such as PTES, NIST, HIPAA, PCI DSS, and ISO 27001/27002. ♦ Strong knowledge base of the industry due to work on multiple projects. ♦ Improved and more reliable measures of confidence in cybersecurity requirements. ♦ Oversight of contract performance and quality assurance using industry standard techniques.	♦ Our team has over ten years of experience in cybersecurity, having successfully completed more than 1,000 projects. These include penetration testing, cybersecurity assessments, audits, vulnerability assessments, web application security assessments, risk assessments, etc. ♦ GSG can manage and meet the demands of the State's required cybersecurity services. ♦ GSG will identify exposures in your application configurations and network infrastructure and using proven process and industry standards resolve those issues. ♦ GSG understands the importance of IP, sensitive, and confidential data. ♦ Highlights real risks of an actual hacker successfully breaching your defenses.

GSG Unique Experience	Relevancy to the State
✓**Highly Qualified Staff**	
Our key personnel: ♦ Averages **fifteen years** of experience in cybersecurity and IT security support. ♦ Our staff has extensive knowledge of all aspects of IT Consulting, IT Security Assessments, Penetration Testing, Vulnerability Assessment, etc., for public and private organizations, including requirements for IT environments. ♦ Has worked together as a team on over forty assignments. ♦ Has performed hundreds of web application assessments and network penetration tests.	♦ The same Key Staff proposed for the State recently implemented continuous monitoring Configuration Baseline standards enterprise-wide for 2,000 endpoints and servers for the Department of Labor. ♦ This showcases our ability to work on large projects under tight timelines and deliver a timely work product for our client.
✓**Ability to Provide Targeted Quality Services**	
♦ With an approach tailored to meet the State's requirements, our team continuity utilizes the industry's 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 uninterrupted services and security of data that meets all cybersecurity standards.

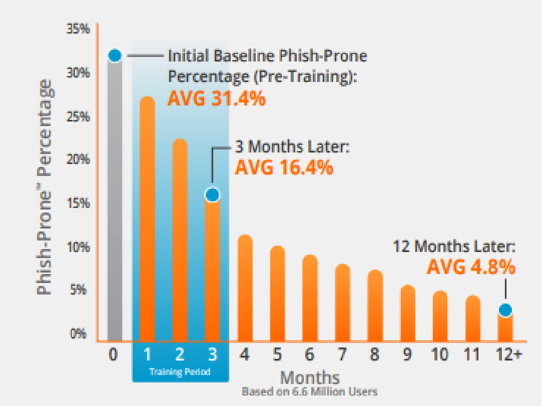
CMMC C3PAO Certification	Ensures the highest government security standards are met.
ISO 27001 Cybersecurity Standards	Demonstrates best-in-class risk management.
24/7 Security Monitoring with AI-based Threat Detection	Provides real-time alerts and automated threat mitigation.
Customized Employee Cyber Training	Reduces human error-related security risks by 40%+.

1.2 *KnowBe4: Qualifications and Unique Features*

KnowBe4 is the provider of the world's leading security awareness training and simulated phishing platform. The GSG Team will assist the State in managing the ongoing problem of social engineering with our expert partner, KnowBe4, offering the most robust and customized solution. With world-class, user-friendly, new-school Security Awareness Training, KnowBe4 gives you self-service enrollment, and both pre- and post-training phishing security tests that show you the percentage of end-users that are Phish-prone. **KnowBe4's** highly effective, frequent, "double-random" Phishing Security Tests provide several remedial options in case an employee falls for a simulated phishing attack.

The multiple unique and customizable features of KnowB4 make it the best solution for the State's security awareness training needs.

In a recent Industry Benchmarking Report, **KnowBe4** security awareness training reduced Phishing related incidents from 31.4% (pre-training) to 4.8% (post-training) in twelve months.



The **KnowBe4** awareness training has four parts:

❶Baseline Testing	❷User Testing and Training	❸User Phishing	❹Result Analysis
Through simulated phishing attacks, baseline testing is created assessing user's percentage vulnerability to attacks.	The largest library of security awareness training content includes interactive modules, videos, games, posters, and newsletters.	Best-in-class, fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates. Follow-up training using multiple formats.	Enterprise-strength reporting, showing stats and graphs for both security awareness training and phishing, ready for management.

The are ten distinct advantages to using **KnowBe4** over other products. Below is a summary of the major features and their benefits.

Customizable	The KnowBe4 platform is designed with intuitive navigation and an easy user interface that takes minimal time to deploy, manage and understand. You can schedule regular Phishing Security Tests using one of more than 10,000 "known-to-work" templates or create your own custom phishing templates.
ModStore Library	The ModStore library is constantly refreshed with unique phishing and training campaign combinations that you could set up an entire year's campaign with a 'set-it-and-forget-it.'
Real-World Phishing Simulations	KnowBe4 enables REAL phishing simulations that teach users how to watch out for phishing scams from user favorites: LinkedIn, Twitter, Amazon, Office 365, Dropbox, etc. With over 1,000 templates and scenarios, the tests stay fresh.
Security Awareness Training Content	The world's largest library of over 1,000 security awareness training content: interactive modules, videos, games, posters, and newsletters.
Active Directory Integration	Active Directory Integration allows user data synchronization to save time by eliminating the need to manually manage user changes. Once the ADI is configured, users will be added, changed, and archived coordinated with changes made within AD automatically.
Smart Groups	The powerful Smart Groups feature allow tailored phishing campaigns, training assignments, remedial learning and reporting based employees' behavior.

Specialized Tools	**Compliance Plus** allows compliance training campaigns and awareness training with easily customizable content. **PhishER** that saves time doing email triage.
Faster Deployment	The KnowBe4 platform is easily deployed into production, typically twice as fast as our competitors.
ISO Certified Facility and PCI Compliant	KnowBe4 uses Amazon's Web Services to host: they are a fully compliant and ISO certified facility and PCI compliant and SCORM from day one.
Frequent Releases of New Features	New features are released every month for the most up-to-date and cutting-edge features and functionality.

Baseline Testing

We provide baseline testing to assess the Phish-Prone™ percentage of your users through a free simulated phishing attack.

User Testing and Training

The world's largest library of security awareness training includes interactive modules, videos, games, posters, and newsletters. Automated training campaigns with scheduled reminder emails.

User Phishing

User Phishing uses fully automated simulated phishing attacks, thousands of templates with unlimited usage, and community phishing templates. Follow-up training uses multiple formats

Result Analysis

One of the strongest features about KnowBe4 is the ability customize with time-saving tools:

- Smart Groups for AD-HOC reporting.
- Automated Security Awareness Program to create your fully mature, customized program.
- Active Directory Integration for easy and fast user management.
- When your users start reporting more "phishy" emails through the free Phish Alert Button, you can now add PhishER, which allows the Incident Response team to quickly identify and respond to email threats faster.
- The Virtual Risk Officer (VRO) functionality shows your Risk Score by employee, group, and your whole organization.
- ModStore keeps the security awareness training library stocked with fresh content.
- The new Advanced Reporting feature which dramatically expands instant detailed reporting on a host of key awareness training indicators. About 30% of data breaches are caused by repeat offenders from within the organization. It highlights a continued problem: Risk accumulates over time when proper education and reporting do not happen.

Training Content	Level I	Level II	Level III
Training Modules	10	34	147
Micro Modules	1	24	119
Videos (90 sec-5 min)	8	64	466
Posters/Images	38	47	216
Newsletters/Security Documents	3	31	243

Games		2	26

KnowBe4's game-changing partnerships with The Security Awareness Company, Popcorn Training, Exploqii, Canada Privacy Training, Twist and Shout, El Pescador, CLTRe, Saya University, Lawpilots, and MediaPRO allows you to manage the ongoing problem of social engineering significantly better.

In your fight against phishing and ransomware you can deploy the best-in-class phishing platform combined with the world's largest library of security awareness training content, including over 1,000 interactive modules, videos, games, posters, and newsletters.

<u>KnowBe4 – Training Topics:</u>

Features	Silver	Gold	Platinum	Diamond
Unlimited Phishing Security Tests	✓	✓	✓	✓
Automated Security Awareness Program (ASAP)	✓	✓	✓	✓
Security 'Hints & Tips'	✓	✓	✓	✓
Training Access Level I	✓	✓	✓	✓
Automated Training Campaigns	✓	✓	✓	✓
Brandable Content	✓	✓	✓	✓
Assessments	✓	✓	✓	✓
Phish Alert Button	✓	✓	✓	✓
Phishing Reply Tracking	✓	✓	✓	✓
Active Directory Integration (ADI)	✓	✓	✓	✓
SSO/SAML Integration	✓	✓	✓	✓
Industry Benchmarking	✓	✓	✓	✓
Virtual Risk Officer™	✓	✓	✓	✓
Advanced Reporting	✓	✓	✓	✓
Training Access Level II		✓	✓	✓
Monthly Email Exposure Check		✓	✓	✓
Vishing Security Test		✓	✓	✓
Smart Groups			✓	✓
Reporting APIs			✓	✓
User Event API			✓	✓
Security Roles			✓	✓
Social Engineering Indicators (SEI)			✓	✓
USB Drive Test			✓	✓
Priority Level Support			✓	✓

Training Access Level III				✓
AI-Driven Phishing				✓
AIDA™ Artificial Intelligence-driven Agent BETA				✓
Compliance Plus - Optional Add-on	✓	✓	✓	✓
PhishER™ - Optional Add-on	✓	✓	✓	✓

2. *Relevant Experience*

GSG offers twenty-two 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.

A sample of GSG cybersecurity initiatives is listed in the following table.

Large Federal Contracts	
Contract Description	*Agency/Organization*
$26M Cybersecurity Services	Department of the Interior
$1.9M Cybersecurity Assessment Support	Department of the Treasury
$9.8M Penetration Testing, Web Security	Department of Agriculture
Other Cyber-Related Contracts	
Contract Description	*Agency/Organization*
Network Disaster Recovery Plan	Suburban Mobility Authority for Regional Transportation
Cybersecurity Consulting	National Cooperative Purchasing Alliance
Cybersecurity Services	Department of the Interior Michigan Economic Dev Corp. City of New Orleans Commonwealth of MA State of NM Human Services Golden Gate Bridge Hwy
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/Risk Assessment	Detroit Wayne Integrated Health
Security Information/Event Management	University 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.
Upgrading IT Infrastructure	Montana State University
Wireless Penetration Testing	U.S. Department of Agriculture

The following past performance citations demonstrate our previous work for clients where we provided similar services:

Virginia Retirement System (VRS)	
Relevance to Technology Assessment	GSG's penetration testing services align with the State's cybersecurity needs by providing thorough assessments across web applications, networks, and physical/social engineering, which directly contributes to identifying and addressing vulnerabilities that could affect privacy and security protocols.
Relevance to RFP	GSG's services support the RFP requirements by offering specialized assessments that enhance security, ensuring alignment with mandatory training topics like social engineering threats, data protection, and identity theft, which are critical for developing a robust Privacy and Cybersecurity Training Solution.
Success Story	GSG successfully conducted security assessments for VRS, including web application testing, source code reviews, and network penetration, leading to comprehensive remediation strategies that strengthened clients' cybersecurity posture and enhanced training modules around security threats and social engineering.
Boston Public Health Commission (BPHC)	
Relevance to Technology Assessment	GSG's comprehensive cybersecurity vulnerability assessment directly aligns with the need to evaluate security controls, identify vulnerabilities, and test critical systems as required by the technology assessment. Their thorough testing across network infrastructures, application security, and social engineering provides essential insights into improving security posture.
Relevance to RFP	GSG's services align with the RFP requirements by ensuring that penetration testing, vulnerability scanning, and social engineering assessments support the development of a robust, customizable Privacy and Cybersecurity Training Solution for the State. These services enhance training topics like phishing, password guidelines, and social engineering.

Success Story	GSG successfully delivered a cybersecurity vulnerability assessment for BPHC, identifying critical risks across their infrastructure. Their penetration testing and social engineering strategies helped remediate vulnerabilities, ensuring compliance with industry standards like NIST and HIPAA, which directly contribute to comprehensive cybersecurity training initiatives.
Department of Treasury (DoT)	
Relevance to Technology Assessment	GSG's comprehensive cybersecurity services, including vulnerability assessments, penetration testing, and RMF implementation, directly support the goal of enhancing network security and addressing potential risks. These services ensure compliance with federal standards like FISMA and NIST, crucial for effective technology assessments.
Relevance to RFP	GSG's cybersecurity services align with the RFP requirements by providing the foundational support needed to develop a robust, customizable Privacy and Cybersecurity Training Solution. Their focus on risk management, vulnerability remediation, and threat analysis supports training topics such as phishing prevention, access control, and security threat understanding.
Success Story	GSG successfully assisted DoT in enhancing their cybersecurity posture by conducting thorough security assessments and implementing RMF best practices. Their detailed documentation, including risk assessments and POA&Ms, directly supports the creation of a tailored, compliant training solution for organizations like the State.
City of New Orleans	
Relevance to Technology Assessment	GSG's cybersecurity services, including NDR, EDR, SIEM, vulnerability assessments, and penetration testing, directly support the technology assessment by identifying threats, securing endpoints, and ensuring a comprehensive defense posture for enterprise infrastructures, such as the NOPD's systems.
Relevance to RFP	GSG's extensive cybersecurity offerings align with the RFP requirements for a customizable Privacy and Cybersecurity Training Solution, specifically in areas like threat identification, incident reporting, and securing networks and endpoints, which are critical training topics.
Success Story	GSG's partnership with NOPD demonstrates our ability to provide a wide range of cybersecurity services, including incident response, threat remediation, and SIEM, showcasing their capacity to meet the privacy and cybersecurity training needs of large organizations like the State.
U.S. AbilityOne Commission	
Relevance to Technology Assessment	GSG's independent evaluation of IT security systems, aligned with FISMA and NIST standards, ensures a comprehensive risk-based approach to cybersecurity. This aligns with the need to assess and identify security weaknesses, which is essential for the technology assessment in the RFP.
Relevance to RFP	GSG's focus on cybersecurity analysis and vulnerability resolution supports the RFP requirement for a customizable training solution in areas like security threat understanding, incident reporting, and data protection, ensuring compliance and preparedness for cybersecurity challenges.
Success Story	GSG's work with IT security evaluations for federal agencies, including detailed FISMA reporting, demonstrates their expertise in identifying risks and implementing effective cybersecurity measures, which aligns with the need for robust Privacy and Cybersecurity Training Solution for large organizations.

Kansas Department of Health and Environment (KDHE)	
Relevance to Technology Assessment	GSG's Application Security Assessment for EpiTrax, including static analysis, role-based access control testing, and vulnerability exploitation, highlights their expertise in identifying and mitigating security threats, which is directly relevant to ensuring secure systems for the technology assessment.
Relevance to RFP	GSG's application security testing methodology, including manual verification and vulnerability exploitation, aligns with the RFP's need for comprehensive cybersecurity training solutions on topics such as threat identification, access control, and incident reporting.
Success Story	GSG's successful work with the KDHE on securing the EpiTrax application demonstrates their ability to evaluate and secure complex systems, aligning with the need for robust cybersecurity measures in large-scale enterprise environments.
Detroit Wayne Integrated Health Network (DWIHN)	
Relevance to Technology Assessment	GSG's vCISO services, focusing on comprehensive risk assessments, governance, and security management, are highly relevant to the technology assessment by providing a holistic review of existing IT security systems, including compliance, risk management, and incident handling.
Relevance to RFP	GSG's vCISO expertise in managing information security governance, policies, and procedures directly aligns with the RFP's requirement for customizable, comprehensive cybersecurity training solutions, particularly in areas like access control, incident reporting, and risk assessments.
Success Story	GSG's success with DWIHN, developing a robust security culture through strategic risk assessments and security governance, showcases their capability to enhance security posture and compliance, meeting the needs outlined in the RFP for adaptable and effective cybersecurity training solutions.
Jacksonville Aviation Authority (JAA)	
Relevance to Technology Assessment	GSG's vulnerability assessments and penetration testing services across critical airport networks, adhering to FAA, TSA, PCI DSS, and CJIS standards, provide a robust evaluation of access controls and security policies, directly supporting the need for a comprehensive security training solution as outlined in the RFP.
Relevance to RFP	The testing and compliance framework used in this project aligns with the RFP's requirement for customizable cybersecurity and privacy training modules, specifically in areas like access controls, PCI-DSS compliance, and incident reporting.
Success Story	GSG's successful implementation of penetration testing and vulnerability assessments for JAA demonstrates its ability to ensure compliance with stringent security standards, which is essential for developing an adaptive and effective cybersecurity training solution, as required in the RFP.
San Diego County Regional Airport Authority	
Relevance to Technology Assessment	GSG's penetration testing and CIS Critical Security Controls (CSC) v8 assessments for specialized aviation security systems demonstrate its expertise in identifying vulnerabilities and implementing cybersecurity measures, aligning with the RFP's focus on customizable cybersecurity training and security compliance.
Relevance to RFP	The services provided in this project mirror the RFP's need for a comprehensive, adaptable cybersecurity curriculum, especially in areas like access controls, incident reporting, and compliance with security standards (PCI-DSS, HIPAA).
Success Story	GSG successfully conducted remote penetration tests and assessments for critical aviation security systems, delivering actionable remediation recommendations

	and detailed test logs, showcasing their ability to support the RFP's requirement for a robust and effective cybersecurity training solution.
Fort Wayne Allen County Airport Authority	
Relevance to Technology Assessment	GSG's comprehensive penetration testing and vulnerability assessments, including web applications, wireless assets, and social engineering tests, align with industry best practices for cybersecurity, highlighting their expertise in identifying and mitigating security threats, a key focus for RFP requirements.
Relevance to RFP	The testing methods used by GSG reflect the need for adaptable training in areas such as security threats, access controls, and social engineering prevention, which are essential components of the RFP's cybersecurity training solution.
Success Story	GSG's penetration testing successfully identified and mitigated vulnerabilities across critical systems, including physical access risks and wireless vulnerabilities, demonstrating the capability to deliver robust cybersecurity assessments and enhance security awareness, in line with the RFP's needs.
Lansing Board of Water and Light (LBWL)	
Relevance to Technology Assessment	GSG's penetration testing and digital forensic services directly address key cybersecurity challenges, such as identifying vulnerabilities, addressing misconfigurations, and remediating malware, all in line with the RFP's emphasis on secure systems and data protection.
Relevance to RFP	GSG's comprehensive testing services, including web, mobile, and SCADA vulnerabilities, align with the RFP's need for customizable, adaptive cybersecurity training, with an emphasis on understanding and mitigating security threats and improving user awareness.
Success Story	GSG's experience in performing thorough penetration testing, vulnerability assessments, and malware remediation showcases the ability to deliver tailored cybersecurity solutions, supporting the RFP's requirements for robust and proactive security measures.

We have had over fifty contracts in the last five years and below is a representative sample of contracts.

Agency Name	***Contract Title***	***Services Summary***
Cybersecurity – State Agencies		
Virginia Retirement System	Penetration Testing Services	Performed internal/external penetration testing, source code reviews, social engineering, and specialized assessments for firewalls, routers, and directories.
Texas Department of Information Resources	Cybersecurity Products and Services	Statewide procurement requirements for Cybersecurity Products and Services.
Kansas Department of Health and Environment	Security Assessment	Performed application security assessments to identify vulnerabilities and tested responses to manual and automated attacks.
Connect for Health Colorado	IT and Security Consulting and Services	Delivered IT and security consulting services including CISO, cybersecurity analysis, network security engineering, penetration testing, Cloud security support, forensic analysis, and red/blue team exercises.
North Dakota Information Technology	IT Security Professional Services	Provided services like application security, cyber forensics, IoT security, penetration testing, SIEM, and third-party risk management.

Agency Name	*Contract Title*	*Services Summary*
Michigan Economic Development Corporation	Cybersecurity Compliance Consulting Service	Offered compliance services such as gap analyses, POA&Ms, SPPRs, and remediation to meet NIST SP 800-171, DFARS, and CMMC standards.
Rhode Island Student Loan Authority	Adversarial Assessment	Conducted adversarial assessments, social engineering, and remediation for internal and external IT assets, including desktops, servers, and firewalls.
Massachusetts Executive Office of Technology Services and Security	Cybersecurity Health Checks	Providing Cybersecurity Health Checks to local government agencies under a state program. Services include assessment of existing access control policies and procedures, Backup and recovery strategy assessment, internal and external vulnerability scans, and related support.
State of New Mexico Human Services Department	Cybersecurity Services	Developed federally mandated documents like SSP, ISRA, and POA&M. Conducted security audits, software management, and provided risk assessment and improvement recommendations.
Kansas State Office of Information Technology Services	Cybersecurity, IT Consulting, and IT Managed Services	Provided an Information Security Officer, advised on risk management, and supported disaster recovery and continuity planning.
Commonwealth of Massachusetts	Data, Cybersecurity, Related Audit, Compliance, and Incident Responses Services	Provided data and cybersecurity services including audits, penetration tests, compliance validation, data breach investigations, and remediation.
Kansas Department of Corrections	Forensic Examination of File Permissions	Investigated unauthorized file permission changes, analyzed logs, and provided a report on violations of state and federal regulations.
State of Oklahoma	Information Technology Risk, Security and Compliance Products and Service	Delivered network security evaluations, vulnerability testing, technical installation, and training, ensuring compliance and optimal performance.
Kansas Board of Tax Appeals	Malware Recovery Services	Evaluated and mitigated malware infections, conducted forensic investigations, re-imaged workstations, and ensured proper antivirus operations.
Nevada Affordable Housing Assistance Corporation	Network Penetration and Vulnerability Testing Services	Conducted internal/external penetration assessments using tools from the Virtual Security Test Center (VSTC) to verify security controls.
Mississippi Department of Information Technology Services	Security Risk Assessment Services	Provide Cloud Compliance Assessment, Penetration Testing, Security Risk Assessment, and Security Program Assessment services.
Cybersecurity – Private Sector		
Detroit Wayne Integrated Health Network	Virtual Chief Information Security Officer	Provided vCISO services to manage security audits, deliver comprehensive risk assessments, and review the current information security posture.
Call Tower, Inc.	Threat Modeling, Vulnerability Assessments	Performed threat modeling, vulnerability assessments, and network/web application penetration testing to validate compliance with the industry's best practices and ensure system confidentiality, integrity, and availability.

Agency Name	*Contract Title*	*Services Summary*
Property & Environmental Management, Inc.	Cybersecurity Maturity Model Certification Gap Analysis	Conduct a gap analysis by comparing the current state vs. requirements for the CMMC Level 3 model. CMMC Level 3 covers virtually all the controls required for NIST 800-171.
Cybersecurity – Local/Regional		
Boston Public Health Commission	Cybersecurity Risk Assessment	Comprehensive network assessment, penetration testing, wireless scanning, database assessments, phishing/spear phishing simulations, and pretexting.
City of Grand Rapids	CISOaaS and Penetration Testing	CISO as a Service (CISOaaS) and penetration/vulnerability testing to enhance IT security operations and infrastructure.
Washtenaw County Purchasing	Cybersecurity Incident Response and Strategic Planning	Developed incident response plans, performed cybersecurity assessments, and identified risk areas in network infrastructure systems.
City of San Jose	As-Needed Cyber Products and Services	Advanced, on-demand cybersecurity services to strengthen the City's security posture.
City of New Orleans	Cyber Security Services	Penetration testing, endpoint/network detection and response, email security, and multi-factor authentication as part of enterprise cybersecurity services.
Housing Authority of the Birmingham District	Information Security and Computer Equipment Assessment	Network security evaluations, testing of internal/external networks, wireless vulnerabilities, physical access controls, and social engineering risks.
Gwinnett County Board of Commissioners	Information Technology and Internal Auditing Services	IT security audits using NIST risk management framework and risk assessments to prioritize internal audit work.
City and County of San Francisco	IT Audit Services	IT audits included network/application penetration testing, HIPAA compliance assessments, and IT General Controls (ITGC) evaluations.
City of Chicago Department of Assets Information and Services	Network Architecture Review/Assessment	Collaborated with Google | Mandiant for IT network architecture assessment, including active security evaluations and network reviews.
Maricopa County	Penetration Testing Services	On-demand penetration testing, executive-level reporting, risk assessments, and recommendations for security policy improvements.
City of Tucson	Cybersecurity Products, Solutions, and Services	Providing as-needed security solutions and tools, Identity and Access Management (IAM) solutions, data security and privacy, security consulting and advisory services, regulatory compliance and governance services, security architecture and integration services, and emerging technologies and future-proofing services.
City of Sunnyvale	Security Assessment	Security planning, audits, risk assessments, SIEM, SOC services, and implementing tools like intrusion detection and malware protection.
City of Visalia	Cybersecurity Assessment, Cyber Resilience Program, and Implementation Plan	Provide comprehensive and detailed review of the current environment and create a Cyber Resilience Program (CRP), as well as an implementation plan to improve the City's overall technology security posture.
Cybersecurity – Educational		

Agency Name	***Contract Title***	***Services Summary***
Lone Star College	IT Security Assessments	Performed email security, firewall audits/scans, network assessments, telephone vulnerability assessments, and penetration testing.
National Cooperative Purchasing Alliance	Cybersecurity Solutions, Malware, Ransomware Protection, and Other Services	Delivered cybersecurity solutions for malware/ransomware protection and related services for the Region 14 Education Services Center and NCPA entities.
Montana State University	Cybersecurity Compliance Assistance Services	Educated on cybersecurity threats, assessed environments, performed vulnerability scans, reviewed practices, and delivered compliance reports following NIST SP 800-171, DFARS, and CMMC standards.
Johnson County Community College	Information-Security Incident Management Audit Services	Audited Information Security Incident Management processes and provided recommendations for improvements and prioritizations.
Prince George's Community College	IT Security Services and Solutions	Consulted on IT Security Assessment and Services, including vCISO, vSOC, Data Breach Analysis, IT Security Planning, Network Design, and Penetration Testing.
Maryland State Department of Education	Security Specialist Contractor	Supported control assessments, updated Business Continuity and Contingency Plans, evaluated security posture, and recommended remediation.
Lancaster Independent School District	Cybersecurity Products and Services	Provide products and services supporting resource, asset, data protection and tracking, forensic and incident response, data security hardware/software, endpoint, network and cloud security, training and awareness, electronic and information resources accessibility, data back up, and system recovery.
University of Michigan School of Medicine	Security Information and Event Management (SIEM)	Led a SIEM project to evaluate and recommend a security solution for the University's campus computer system.
Grand Valley State University	Penetration Testing	Conducted penetration testing for PCI DSS v4.0 compliance, simulating real-world attack scenarios and identifying vulnerabilities.
Oakland County Academy of Media and Technology	Site Assessment and Managed Services	Provided 24/7 IT Managed Services, including infrastructure support for firewalls, routers, switches, and network installations.
Medical College of Wisconsin	IT Infrastructure Analysis and Updates	Assessed IT network, provided roadmap improvements, and implemented an Endpoint Detection and Response system.
Board of Education of Baltimore County	IT Security Services and Solutions (Security and Assessment Services)	Provided IT security services including vCISO, vSOC, vulnerability assessments, business continuity, disaster recovery, forensics, and risk assessments.
Putnam/Northern Westchester Board of Cooperative Educational Services	Cybersecurity Software and Services	Provide Cybersecurity Software and Services, including hardware components, to address school district digital threats and vulnerabilities.
Eastern Suffolk Board of Cooperative Educational Services	LAN/WAN and Cybersecurity Support	Provide Cybersecurity engineering and maintenance support, computer systems and network engineering support, IT operations maintenance and support.

Agency Name	*Contract Title*	*Services Summary*
MD State Dept. of Education, Div. of Rehab. Services	Cybersecurity Specialist Support	Developed System Security Plan (SSP), Risk Assessment Reports, Certification and Accreditation (C&A) packages, and Security Assessment Reports (SAR).
Cybersecurity – Transit and Utilities		
Lansing Board of Water and Light	Penetration Testing and Digital Forensics	Provided penetration testing and digital forensic services, tested applications for vulnerabilities, conducted forensic examinations, and assisted with malware remediation and system hardening.
Suburban Mobility Authority for Regional Transportation	Disaster Recovery Consultant	Developed a disaster recovery plan, including co-location, a secondary data center, cloud-based DR, and other DR technologies.
Capital Area Transportation Authority	Long-Range Technology Plan	Developed a long-term technology plan and multiple risk assessment strategies.
San Diego County Regional Airport Authority	On-call IT Cyber Services	Provided data breach investigation and response, vulnerability assessments, penetration testing, compliance testing, risk assessments, and network/system documentation.
Golden Gate Bridge Highway and Transportation District	On-Call Cyber Security Professional Services	Aligned business and cybersecurity objectives, developed IT strategy, created integration/configuration/testing plans, and designed state-of-the-art solutions.
Jacksonville Aviation Authority	Network Penetration Testing	Performed network penetration testing for twenty-five secure VLANs and ninety-five general-purpose VLANs, adhering to FAA Cybersecurity Strategy, TSA security requirements, and PCI-DSS policies.
Suburban Mobility Authority for Regional Transportation	Cloud-Based Email Security	Provided email security for 500 users, including malware/phishing detection, incident response, and technical support in collaboration with Trellix.
Fort Wayne–Allen County Airport Authority	IT Security Assessment	Performed internal/external network security assessments, reviewed device configurations, conducted wireless penetration testing, and resolved vulnerabilities.
Port Authority of Allegheny County	Security Assessment, Business Process, and Infrastructure Consultation	Assessed IT services, reviewed financial and system design, and recommended system upgrades to streamline business processes.
Sacramento Regional Transit District	Cybersecurity Consulting Services	Provided cybersecurity services including PCI assessments, compliance reporting, investigations, program development, and staff training.
Regional Water Resource Agency	Network and Cybersecurity Assessment	Developed the Cyber Resilience Program (CRP), conducted a risk assessment of networked Operational Technology (OT) systems including SCADA controls, telemetry, and networking devices, and provided cybersecurity recommendations.
Lincoln Electric System	Corporate Penetration Test	Assess the external network environment to discover and validate controls for external systems configuration, which may affect the security and privacy of the data. Perform email phishing and phone pretexting, internal penetration testing, and web application assessments.

Agency Name	*Contract Title*	*Services Summary*
Cybersecurity – Federal Agencies		
U.S. Department of Agriculture - Information Security Center	Wireless Penetration Testing	Conducted wireless penetration testing across eighteen agencies, involving reconnaissance, password cracking, spoofing, misconfiguration tests, and router/device exploitation.
U.S. AbilityOne Commission	IT Infrastructure Review of Security Features	Reviewed and tested security features, practices, and policies of hardware/software IT infrastructure. Delivered FISMA reports and presentations after thorough data analysis.
Department of the Interior Interior Business Center	Information System Security Line of Business Support Services	Supported six civilian agencies with technical testing, penetration testing, forensics, insider threat assessments, security documentation, and A&A services.
Cybersecurity and Infrastructure Security Agency	Priority Services Operational Support	Developed, provided, and supported modernized operational services including IT system development, daily service center operations, and smartphone application management.
U.S. Department of Health and Human Services – Health Resources and Services Administration	NPDB Cybersecurity Assessment Services for PCI-DSS Certification	Providing cybersecurity compliance assessment services to ensure PCI DSS compliance, including annual SAQ completion, quarterly ASV scans, annual penetration testing, gap analysis, onsite assessments, and additional testing, along with records management and project management for the NPDB Cardholder Data Environment.
Dept. of Agriculture Security Ops. Center	Penetration Tests	Performed penetration tests which included scanning TCP/UDP ports, identifying network services, and probing for exploitable vulnerabilities on each host.
Department of Agriculture - National Institute of Food & Agriculture	IT Security Assessments	Executed security assessments covering perimeter, network, web, host security, user awareness training, and SOC standard operating procedures.
Department of the Treasury	Cybersecurity Assessment Service Support	Conducted comprehensive cybersecurity assessments, documented findings in POA&M, and implemented mitigations. Offered services to meet federal compliance requirements.

3. Key Personnel

GSG maintains a team of extraordinary cybersecurity professionals. The quality of our team is peerless, having executed multiple programs of similar scope and complexity.

All GSG's cybersecurity personnel:

- ✓ Have completed over **1,000** projects over the past **Ten Years.**
- ✓ Has over ten years of experience in providing cybersecurity and related services.

In addition to having degrees in relevant fields, they also carry one or more of the following certifications or their equivalent:

GSG's Cyber Related Certifications

CAP	**CCIP**	**CCSK**	**CGEIT**	**CDFE**
Certified Authorization Professional	Certified Core Impact Professional	Certificate of Cloud Security Knowledge	Certified in Governance of Enterprise IT	Certified Digital Forensics Examiner

CFCE Certified Forensic Computer Examiner	**CHFI** Computer Hacking Forensic Investigator	**CHSE** Certified HIPAA Security Expert	**CISA** Certified Information Systems Auditor	**CISM** Certified Information Security Manager
CRISC Certified in Risk and Info. Systems Control	**CSX** Cybersecurity Nexus Practitioner	**PCIP** Payment Card Industry Professional	**PFI** PCI Forensic Investigators	**ISSAP** Information Systems Security Architecture Professional
SANS 508 Advanced Forensics	**SANS 572** Advanced Network Forensics	**GSEC** GIAC Security Essentials	**GSEC** GIAC Security Essentials	**GCIH** GIAC Certified Incident Handler
GPEN GIAC Penetration Tester	**GCIA** GIAC Certified Intrusion Analyst	**GWAPT** GIAC Web Application Pen Tester	**GCFE** GIAC Certified Forensic Examiner	**GCFA** GIAC Certified Forensic Analyst

3.1 Staff Descriptions

	Name	Position	Yrs. Exp	Partial Certification Summary
Project Team	**Ajit Kumar Patel**	Project Manager	39	ITIL-ITSM, Six-Sigma Green Belt, Manufacturing Enterprise Leadership, Systems Engineering Development
	Vatsal Shah	Cybersecurity Technical Lead/Assessor/Trainer	20+	PCIP, CCSK, CISA, CEH, TL, CISSP, CISSP-ISSAP, GWAPT, OP
	Kumar Setty	Cybersecurity Assessor/Trainer	15+	CISSP, CISA, CCSK, ITIL, PCIP, AWS, HCISSP

Our team will be overseen by our Project Manager, Mr. Ajit Kumar Patel, who has over thirty-nine years managing complex IT and cybersecurity projects for both the public and private sector. Mr. Patel will be the 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.

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

Your GSG Team:

- ✓ Averages over fifteen years of experience completing similar work for government customers.
- ✓ Has advanced degrees and technical certifications.
- ✓ Has extensive experience with cybersecurity assessment.
- ✓ Has worked together on multiple cybersecurity contracts.

Project Team Experience by Key Member

Experience	*Skill/Knowledge Area*	Ajit Kumar Patel	Vatsal Shah	Kumar Setty
Cybersecurity Project Experience	Penetration Testing and Assessments	■	■	■
	Policy and Procedures	■	■	■
	Vulnerability Assessments	■	■	■

	Web Application Security Assessments	■	■	■
	Cybersecurity Audits	■	■	■
	Risk Assessments	■	■	■
	Incident Response	■	■	■
	Managed Defense	■	■	■
IT and Cybersecurity Technology Project Experience	HPE			■
	Micro Focus	■	■	
	Splunk			■
	IBM			■
	Palo Alto		■	
	Cisco, AWS, and Azure, Fortinet	■	■	■
Framework and Controls Experience	NIST Cybersecurity Framework	■	■	■
	Federal Risk and Authorization Management Program (FedRAMP)		■	■
	Payment Card Industry Data Security Standard (PCI–DSS)	■	■	■
	Open Web Application Security Project		■	■
	Center for Internet Security Critical Security Controls for Effective Cyber Defense		■	■

3.2 Relevant Experience of Individual Team Members

3.2.1 Ajit Kumar Patel — Project Manager

Ajit Kumar Patel — Project Manager	
Education	MS, Adv. Chemical Engineering, University of London BS, Chemical Engineering, London South Bank University, London
Certifications	Six-Sigma Green Belt Certification (Ford Motor) Manufacturing Enterprise Leadership Certification (EDS) Systems Engineering Development Certification (EDS)

Work Experience

Mr. Patel is an accomplished IT professional with thirty-nine years of experience in finance, manufacturing, and product engineering. Known for delivering IT solutions from project initiation to implementation and operational management, he is skilled in project management, process improvement, and client relations. Mr. Patel holds Six Sigma Green Belt and ITIL-ITSM certifications and is recognized for his integrity, systematic approach, and ability to build strong relationships across all organizational levels. His expertise spans leadership, business analysis, resource planning, and team development, consistently achieving high client and sponsor satisfaction.

- **Consumers Energy, Inc.:** Managed $10M+ portfolio, financial forecasting, and resource planning; coached project managers, coordinated with IT leads and PMO.
- **Fast Switch:** Led development of customer-facing 'Outage Map' for an energy provider, praised by client leadership; managed a multi-year upgrade of Outage Management System across eight departments.

- **Geometric Americas, Inc.:** Oversaw PLM solutions for manufacturing OEM; managed a project separating PLM systems post-divestiture, achieving high client satisfaction on time and within budget.
- **Ford Motor Company (Senior Program Manager):** Delivered a $3M development project and a $2M+ multi-phase project on time and under budget; provided program management for the global 'One IT' initiative, ensuring alignment with IT mission and principles.
- **Ford Motor Company (Operations Manager):** Managed production schedules and change management for an integrated software application; led 24/7 operations support team, streamlined over 500 nightly batch jobs, improving efficiency.
- **Logica, Inc.:** Led back-end releases for over forty modules during a major IT program's "Beta" launch; as Release Manager, improved processes and delivered modules positively recognized by clients.
- **Electronic Data Systems (EDS):** Managed $5M IT services portfolio for GM Truck Engineering; improved client satisfaction and delivery processes; supervised and supported 500+ client PCs as Engineering SE Supervisor.

Relevant Key Project Experience

City of Grand Rapids:

- Led the implementation of penetration testing and vulnerability assessments for IT support services, including CISOaaS and vulnerability scanning, aligning with the need for cybersecurity awareness and identifying emerging threats relevant to the training solution.

Jacksonville Aviation Authority:

- Managed external and internal penetration testing, focusing on critical compliance areas such as PCI, CJIS, and General Security, which aligns with the need for customizable training modules on cybersecurity and data protection.

City of New Orleans:

- Oversaw the implementation of cybersecurity services, including penetration testing, EDR, NDR, MDR, and firewall deployment. This project provided hands-on exposure to secure environments and aligns with incident response and cybersecurity training.

Consumers Energy, Inc.:

- Led projects for Michigan's largest energy provider, integrating cybersecurity protocols into GIS operations. Managed vulnerability assessments and risk analysis to ensure the protection of sensitive data, aligning with the training solution's need for compliance and threat identification modules.

State of Kansas:

- Oversaw security assessment services for EpiTrax, a public health surveillance system, including vulnerability assessments and security compliance. This experience supports the implementation of training focused on data classification, PII protection, and compliance (e.g., HIPAA, PCI-DSS).

Ford Motor Company:

- Managed IT security projects and knowledge transfer initiatives, ensuring secure systems development and proper handling of sensitive information. This is highly relevant to the training solution's focus on privacy awareness, security responsibilities, and incident reporting.

3.2.2 *Vatsal Shah — Cybersecurity Technical Lead/Assessor/Trainer*

Vatsal Shah — Cybersecurity Technical Lead/Assessor/Trainer	
Education	MS, Computer Science, University of Bridgeport
Certifications	Certificate of Cloud Security Knowledge V.4 (CCSK)

	Certified Information Systems Auditor (CISA) Certified Ethical Hacker (CEH) High Value Asset Technical Lead (TL) Training Certified Information Systems Security Professional (CISSP) Certified Information Systems Security Professional- Information Systems Security Architecture Professional (CISSP-ISSAP) GIAC Web Application Penetration Tester (GWAPT) High Value Asset Operator (OP) Training

Mr. Shah is a seasoned IT and Operations professional with over twenty years of experience, specializing in vulnerability assessment, penetration testing, auditing, and incident response management. His expertise includes secure network architecture, 802.11x (Wi-Fi), web applications, SCADA, Process Control Networks (PCNs), Programmable Logic Controllers (PLCs), physical and database security, application security, and regulatory compliance. Mr. Shah has strong technical skills in network technologies, operating systems, and IT infrastructure security controls.

Relevant Key Project Experience

City of Sunnyvale:

- Led comprehensive penetration testing efforts and recommended security enhancements for the City's data center, aligning with the need for cybersecurity awareness and access control training. Provided strategic input on integrating security solutions such as VPNs, EDR, and NGFWs to safeguard the City's IT infrastructure.

City of Roseville:

- Spearheaded a security assessment for water and wastewater control systems, incorporating vulnerability scanning and penetration testing. Developed security policies and procedures using the NIST framework, which directly aligns with the training solution's focus on risk management, compliance, and emergency response protocols.

San Diego County Regional Airport Authority:

- Conducted penetration testing and security control assessments for specialized aviation security systems. Evaluated compliance with PCI-DSS and other security standards, which directly relates to the need for customizable training on PCI-DSS compliance, security threats, and phishing prevention.

Lansing Board of Water and Light:

- Led penetration testing efforts for new enterprise applications, identifying vulnerabilities and ensuring secure deployments. This experience ties to the need for training on securing work areas, access controls, and safe computing practices for sensitive operational environments.

USDA Office of the Chief Information Officer:

- Conducted security assessments and penetration testing on high-value web applications for USDA agencies. This experience is highly relevant to the training solution's need for web application security, safe computing, and incident reporting training modules for government agencies.

Department of Treasury:

- Managed cybersecurity assessments for the Office of Inspector General (OIG), focusing on risk management and compliance with NIST standards. This project aligns with the need for training modules on compliance with federal frameworks, understanding security threats, and handling sensitive data.

U.S. Air Force:

- Conducted black-hat style penetration testing for the U.S. Air Force, identifying and exploiting vulnerabilities to strengthen overall cybersecurity. This experience is directly applicable to training on identifying and mitigating security threats, vulnerability scanning, and safe remote computing practices.

Fort Wayne-Allen County Airport Authority:

- Led a comprehensive IT security assessment, including network, application, and wireless penetration testing. The project provided detailed insights into vulnerability exploitation, which aligns with the need for training on secure computing, social engineering threats, and data classification.

Nevada Affordable Housing Assistance Corporation:

- Conducted network penetration and vulnerability testing, identifying and exploiting vulnerabilities to safely access systems. This project provides relevant experience for training on security responsibilities, threat identification, and incident reporting for organizations handling sensitive data.

3.2.3 Kumar Setty — Cybersecurity Assessor/Trainer

Kumar Setty — Cybersecurity Assessor/Trainer	
Education	MS, Software Engineering Carnegie Mellon MBA, University of Illinois, Chicago BS, Chemical Engineering, University of Rochester
Certification	CISSP — Certified Information Systems Security Professional CISA — Certified Information Systems Auditor CCSK — Certificate of Cloud Security Knowledge ITIL v3 Foundations Certification Payment Card Industry – Qualified Security Assessor Payment Card Industry Professional (PCIP) Stanford University — Software Security Foundations Certification AWS — Amazon Web Services Certified Cloud Practitioner HCISPP — Healthcare Information Security and Privacy Practitioner

Mr. Setty has more than **fifteen years of experience** in providing penetration testing in multiple sectors including the university, healthcare, finance, and technology sectors. Mr. Setty is highly adept in 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 with 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.

Relevant Key Project Experience

Halo Investing:

- Spearheaded the development of a robust IT security governance program for a fintech start-up. This included the creation of a comprehensive cybersecurity training program and policies, directly relevant to developing customizable training modules on security responsibilities, phishing prevention, and incident reporting.

Client Confidential (Healthcare and Fintech):

- Led the design and implementation of a cloud security framework for clients in healthcare and fintech. This experience supports the development of training focused on secure computing practices, data classification, and compliance with industry regulations like HIPAA and PCI-DSS.

Presence Health:

- Assessed and improved security and privacy for healthcare clients, focusing on HIPAA compliance and security assessments. This aligns with the need for training on privacy awareness, handling sensitive information, and HIPAA training modules.

Grant Thornton LLP:

- Directed audits and assessments for healthcare and mid-market companies, ensuring the protection of information in the cloud. This experience aligns with the need for training modules on cloud security, data protection, and compliance with security frameworks like HIPAA, PCI-DSS, and NIST.

PricewaterhouseCoopers:

- Managed IT security audits for large healthcare providers and Fortune 500 companies, ensuring network security and compliance with HIPAA and IT SOX. This experience directly supports the development of training focused on security threats, privacy principles, and compliance with industry standards like HIPAA and PCI-DSS.

Ford Motor Company:

- Oversaw IT security projects, ensuring the proper handling of sensitive information and the implementation of secure systems. This experience ties into training modules focused on privacy awareness, incident reporting, and security responsibilities for large organizations.

U.S. Department of Health and Human Services (HHS):

- Led privacy and security risk assessments for HHS, focusing on HIPAA compliance and privacy frameworks. This aligns with the need for training on handling Personally Identifiable Information (PII), HIPAA regulations, and privacy protection protocols.

Confidential Client:

- Innovated automated solutions for monthly security reviews, improving audit efficiency and reducing costs. This project contributes to the development of training modules on security controls, risk management, and compliance monitoring.

3.3 Experience and Capability of Key Personnel to Execute Roles and Responsibilities

GSG brings extensive expertise in cybersecurity, specializing in strategic oversight, defense mechanism implementation, and comprehensive security assessments. With over a decade of experience in identifying vulnerabilities, reviewing network traffic, and recommending proactive security measures, GSG professionals ensure the protection of critical infrastructure.

Our team is well-versed in securing hardware, software, networks, and systems, focusing on maximizing security through firewalls, file management, and email protection. GSG also emphasizes continuous cybersecurity education, offering engaging and effective training programs tailored to employees, partners, and vendors, equipping them with the knowledge to address a wide range of cyber threats.

The following table highlights each Key Personnel's specific roles and responsibilities, along with a brief summary of their work history where they performed similar work:

3.3.1 Ajit Kumar Patel — Project Manager

Key Responsibilities	Relevant Experience and Achievements	Client Names
Develop and implement cybersecurity training curricula	Led the design and implementation of adaptive cybersecurity and privacy training solutions, including training on security threats, phishing identification, password guidelines, and data protection.	• City of New Orleans

Key Responsibilities	Relevant Experience and Achievements	Client Names
Customize training modules for client-specific needs	Delivered customized training solutions on cybersecurity and privacy topics such as PII, HIPAA, PCI-DSS compliance, and social engineering threats. Training modules were tailored to meet client-specific regulatory needs.	• Gwinnett County Board of Commissioners
Integrate training solutions with client IT environments	Managed the integration of training solutions with existing IT systems (such as Active Directory) to ensure seamless access control and user management for training participants.	• City of Grand Rapids
Support compliance with industry standards (HIPAA, PCI-DSS)	Implemented and managed cybersecurity training aligned with industry standards such as HIPAA, PCI-DSS, and data classification, ensuring all employees were trained to handle sensitive information properly.	• State of Kansas IDIQ
Implement role-based training	Led the development and delivery of role-based cybersecurity and privacy training solutions, ensuring the training materials met specific organizational requirements for different job functions.	• Jacksonville Aviation Authority
Support scalable, large-scale cybersecurity training solutions	Oversaw the creation of scalable cybersecurity training solutions to support large organizations with over 25,000 employees, ensuring flexibility and ease of integration with existing Learning Management Systems (LMS).	• Consumers Energy
Develop and deliver compliance training for diverse topics	Delivered cybersecurity training for a wide range of topics, including incident reporting, social engineering, secure remote computing, and physical security, helping organizations comply with privacy laws.	• Sacramento Regional Transit District

3.3.2 Vatsal Shah — Cybersecurity Technical Lead/Assessor/Trainer

Key Responsibilities	Relevant Experience and Achievements	Client Names
Develop and implement cybersecurity training curricula	Developed and implemented cybersecurity awareness training for teams across various sectors, including practical and theoretical content on secure network architecture, application penetration, and vulnerability management.	• City of Sunnyvale • Lansing Board of Water and Light
Customize training modules for client-specific needs	Created custom training plans for cybersecurity risk mitigation, including penetration testing procedures and vulnerability assessments, tailored for different technical teams and operational environments.	• San Diego County Regional Airport Authority • Jacksonville Aviation Authority

Key Responsibilities	Relevant Experience and Achievements	Client Names
Design and deliver cybersecurity and privacy training	Delivered specialized training on compliance with NIST, CJIS, PCI, HIPAA, and SOX regulations, providing teams with the knowledge needed to ensure systems meet industry security and privacy standards.	• Kansas Dept. of Health & Environment • USDA
Integrate cybersecurity best practices into training	Led training sessions integrating best practices for managing security systems such as VPNs, SIEM, endpoint protection, and cloud security, focusing on enhancing practical security operations for teams.	• City of Roseville • Department of Treasury
Provide role-based security training	Conducted role-specific cybersecurity training for teams, ensuring that key personnel within different departments (e.g., security, IT, and compliance teams) received the targeted knowledge necessary to identify, mitigate, and report vulnerabilities.	• City of Sunnyvale • Oakland County, Michigan
Lead cybersecurity assessments and training on security incident response	Developed and conducted incident response exercises, including tabletop simulations, to prepare IT and security teams for potential cybersecurity events, ensuring readiness and awareness across departments.	• City of Roseville • Fort Wayne-Allen County Airport Authority
Ensure regulatory compliance through targeted cybersecurity training	Managed cybersecurity training aligned with compliance frameworks like PCI-DSS, NIST, and ISO 27001, ensuring that all employees were educated on the handling of sensitive data and secure system operations.	• San Diego County Regional Airport Authority • USDA
Evaluate and improve cybersecurity awareness and training programs	Conducted internal security assessments to evaluate the effectiveness of current cybersecurity training programs, identified gaps, and recommended improvements.	• Department of Treasury • Nevada Affordable Housing Assistance Corporation

3.3.3 Kumar Setty — Cybersecurity Assessor/Trainer

Key Responsibilities	Relevant Experience and Achievements	Client Names
Develop and implement cybersecurity training curricula	Developed and implemented comprehensive cybersecurity training programs focused on phishing, spear-phishing, USB handling, and security awareness using KnowBe4.	• Halo Investing • Client Confidential
Customize training modules for client-specific needs	Tailored training programs and policies for organizations to address their unique security requirements, including cloud security (AWS, Azure), HIPAA compliance, and PCI-DSS readiness.	• Client Confidential • Presence Health

Key Responsibilities	Relevant Experience and Achievements	Client Names
Design and deliver cybersecurity and privacy training	Delivered specialized cybersecurity training focused on risk assessments, threat modeling, and data security, ensuring staff are knowledgeable in both theoretical and practical aspects of cybersecurity.	• Halo Investing, • Presence Health
Integrate cybersecurity best practices into training	Integrated best practices for handling sensitive data, implementing secure file transfer protocols, and establishing incident management procedures across all training modules.	• Halo Investing, • Presence Health
Provide role-based security training	Delivered tailored training programs for different teams (e.g., IT staff, security personnel) focusing on their specific roles in safeguarding organizational systems and data.	• Halo Investing • Client Confidential
Lead cybersecurity assessments and training on security incident response	Led tabletop exercises for security teams to simulate real-world security events and improve incident response protocols, providing feedback and recommendations for improvement.	• Presence Health • Client Confidential
Ensure regulatory compliance through targeted cybersecurity training	Created training modules that emphasize compliance with HIPAA, NIST, FFIEC, and HITRUST, ensuring organizations meet industry standards.	• Client Confidential • Presence Health
Evaluate and improve cybersecurity awareness and training programs	Continuously assessed the effectiveness of cybersecurity training programs, providing insights and improvements based on real-world threats and vulnerabilities identified during assessments.	• Grant Thornton LLP • Pricewaterhous eCoopers

4. Approach to Scope of Work

GSG's approach to performing the Cybersecurity Consulting Services that are listed in the **Scope of Work** is explained in detail in the 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.

- **CMMC C3PAO Certification:** GSG is a CMMC C3PAO Candidate – ML3.
- **Top-Secret Facility Clearance:** GSG holds a DoD Top-Secret Facility Clearance, allowing work on highly sensitive projects.
- **Extensive Government Experience:** Over 1,000 completed cybersecurity projects, including major federal contracts.

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

3.1 Mandatory Contract Item Requirements: Contract Item must meet or exceed the mandatory requirements listed below.

3.1.1 Custom Privacy and Cybersecurity Training Solution

3.1.1.1 The Privacy and Cybersecurity Training Solution must be an adaptive curriculum for Cybersecurity (Information Security) and Privacy training. The State of West Virginia must be able to customize the training topics.

GSG's **Privacy and Cybersecurity Training Solution** is designed as a fully adaptive and customizable learning platform that ensures compliance with the State's requirements. Our approach integrates cutting-edge instructional design, automation, and real-time analytics to provide a tailored learning experience for diverse user groups.

Adaptive Curriculum and Customization

Our solution offers a **modular training framework** that allows the State to select, modify, and expand training topics based on evolving cybersecurity and privacy needs. The platform includes:

- **Role-Based Learning Paths:** Tailored courses for employees, executives, and IT staff.
- **AI-Driven Personalization:** Adjusts training difficulty based on user progress and assessment results.
- **Regulatory Compliance Modules:** Aligns with NIST, GDPR, HIPAA, and state-specific regulations.

Delivery and Engagement

- **Interactive E-Learning:** Gamified scenarios, phishing simulations, and real-world case studies enhance engagement.
- **Multi-Format Support:** Training is available via web-based portals, mobile apps, and LMS integration.
- **Real-Time Analytics Dashboard:** Provides compliance tracking, risk scoring, and progress reports.

Ongoing Updates and Support

GSG ensures continuous updates based on the latest cybersecurity threats and regulatory changes. We provide 24/7 technical support, expert consultation, and user feedback loops to enhance effectiveness.

By implementing this customizable, scalable, and adaptive training solution, GSG ensures the State maintains a proactive cybersecurity posture while meeting its unique privacy training needs.

3.1.1.2 The Privacy and Cybersecurity Training Solution must provide integration with the State's current Active Directory environment.

GSG's **Privacy and Cybersecurity Training Solution** seamlessly integrates with the State's **Active Directory (AD)** environment, ensuring efficient user management and secure access control.

Key Integration Features:

- **Single Sign-On (SSO):** Enables employees to access training using their existing AD credentials, reducing login friction, and enhancing security.
- **Automated User Provisioning:** Synchronizes user roles, departments, and access levels, ensuring tailored training assignments.
- **Real-Time Compliance Tracking:** Leverages AD data to generate customized reports on user participation and training completion.
- **Role-Based Access Control (RBAC):** Ensures only authorized users can access specific training modules based on their job functions.

By integrating with AD, GSG enhances security, streamlines user experience, and simplifies administrative management.

3.1.1.3 The Privacy and Cybersecurity Training Solution must have editable modules for the following topics, at a minimum:

3.1.1.3.1 Understanding Security Threats
3.1.1.3.2 Security Responsibilities
3.1.1.3.3 Physical Threats
3.1.1.3.4 Emergency Preparation
3.1.1.3.5 Securing Work Areas and Resources
3.1.1.3.6 Access Controls
3.1.1.3.7 Safe Computing and Electronic Threats
3.1.1.3.8 Social Engineering Threats
3.1.1.3.9 Password Guidelines
3.1.1.3.10 Safe Remote and Mobile Computing
3.1.1.3.11 Acceptable Use
3.1.1.3.12 Phishing Identification and Prevention
3.1.1.3.13 Physical Security and Emergency Preparation
3.1.1.3.14 Responsible Social Networking
3.1.1.3.15 Protecting and Handling Data
3.1.1.3.16 Records Management and Data Classification
3.1.1.3.17 Privacy Awareness and Privacy Principles (PII)
3.1.1.3.18 Complying with PCI-DSS
3.1.1.3.19 Complying with HIPAA
3.1.1.3.20 Understanding PII
3.1.1.3.21 Social Engineering
3.1.1.3.22 Identity Theft
3.1.1.3.23 Incident Reporting

GSG's **Privacy and Cybersecurity Training Solution** offers a fully **customizable, modular curriculum** that allows the State to edit and tailor training content for diverse user groups. Each module is designed to cover essential cybersecurity and privacy principles while ensuring engagement and compliance with state and federal regulations.

The **Understanding Security Threats** module educates users on common cyber risks, including malware, ransomware, and insider threats. **Security Responsibilities** define individual roles in safeguarding data and systems. **Physical Threats** addresses unauthorized access, theft, and sabotage of IT and physical assets. **Emergency Preparation** provides guidelines for responding to cybersecurity incidents, natural disasters, and security breaches.

Securing Work Areas and Resources emphasizes the importance of protecting sensitive materials, both digital and physical, within office spaces. **Access Controls** details authentication methods, least privilege principles, and Multi-Factor Authentication (MFA). **Safe Computing and Electronic Threats** covers best practices for internet use, malware protection, and software security. **Social Engineering Threats** teaches employees how to recognize and counter manipulation tactics used by cybercriminals.

Password Guidelines outlines the importance of strong passwords and secure credential management. **Safe Remote and Mobile Computing** provides security protocols for working remotely, including VPN use and secure device configurations. **Acceptable Use** ensures employees understand company policies for IT resource usage. **Phishing Identification and Prevention** trains users to detect and avoid email scams and deceptive links.

Physical Security and Emergency Preparation combines physical safety with cybersecurity protocols during incidents. **Responsible Social Networking** covers secure online behavior to prevent data leaks and reputational risks. **Protecting and Handling Data** ensures adherence to data protection policies, while **Records Management and Data Classification** explains proper data categorization and retention practices.

Privacy Awareness and Privacy Principles (PII) educates users on handling Personally Identifiable Information (PII) securely. **Complying with PCI-DSS** and **Complying with HIPAA** ensure compliance with financial and healthcare regulations. **Understanding PII** further emphasizes secure data handling. **Social Engineering** and **Identity Theft** focus on preventing manipulation tactics and fraudulent activities. Finally, **Incident Reporting** trains employees in recognizing and escalating security incidents efficiently.

By providing **editable modules**, GSG ensures that the State can adapt training content as cybersecurity threats evolve, fostering a culture of security awareness and regulatory compliance.

3.1.1.3.24 HIPAA Training, including:

- ***3.1.1.3.24.1 What is HIPAA?***
- ***3.1.1.3.24.2 Personal Health Identifying Information***
- ***3.1.1.3.24.3 Covered Entities***
- ***3.1.1.3.24.4 HIPAA Privacy Rule***
- ***3.1.1.3.24.5 HIPAA Security Rule?***
- ***3.1.1.3.24.6 HIPPA Enforcement Rule?***
- ***3.1.1.3.24.7 HIPAA Breach Notification Rule?***
- ***3.1.1.3.24.8 The Importance of confidentiality***
- ***3.1.1.3.24.9 The Minimum Necessary Standard***
- ***3.1.1.3.24.10Business Associate Agreements***
- ***3.1.1.3.24.11Patient Rights***

GSG's **HIPAA Training Module** provides comprehensive education on **Health Insurance Portability and Accountability Act (HIPAA)** compliance, ensuring that employees understand their roles in protecting sensitive health information.

The **What is HIPAA?** section introduces the purpose and significance of HIPAA, highlighting its role in securing patient health information. **Personal Health Identifying Information (PHI)** defines what constitutes PHI, including names, addresses, Social Security numbers, and medical records, emphasizing the need for strict handling protocols. **Covered Entities** identifies organizations subject to HIPAA regulations, such as healthcare providers, insurers, and clearinghouses.

The **HIPAA Privacy Rule** explains individuals' rights over their health data, limiting access and disclosure of PHI. The **HIPAA Security Rule** details required safeguards, including administrative, physical, and technical measures to protect electronic PHI (ePHI). The **HIPAA Enforcement Rule** outlines penalties for non-compliance, explaining how violations are investigated and addressed by the Department of Health and Human Services (HHS).

The **HIPAA Breach Notification Rule** provides guidance on reporting breaches, specifying timelines and notification requirements to affected individuals and regulatory bodies. **The Importance of Confidentiality** reinforces the ethical and legal duty to protect patient information from unauthorized access or disclosure. **The Minimum Necessary Standard** ensures that only the least amount of PHI required for a task is accessed, reducing data exposure risks.

Business Associate Agreements (BAAs) explain contractual requirements for third-party vendors handling PHI, ensuring they comply with HIPAA regulations. Finally, **Patient Rights** educates employees on individuals' rights, including access to their medical records, request for amendments, and the ability to file complaints regarding privacy violations.

By offering **customizable HIPAA training**, GSG ensures the State meets compliance requirements while fostering a culture of **privacy, security,** and **patient trust** within healthcare-related operations.

3.1.1.4 The Privacy and Cybersecurity Training Solution must have the option to include Role Based Training.

GSG's **Privacy and Cybersecurity Training Solution** includes a **Role-Based Training** feature, ensuring that employees receive targeted education based on their job functions and security responsibilities. This approach tailors training content for **executives, IT administrators, healthcare professionals, finance staff,** and **general employees**, providing relevant scenarios and compliance requirements specific to their roles.

The system **automatically assigns training modules** based on Active Directory roles, ensuring that users only receive information applicable to their access level and responsibilities. IT staff receive **advanced security protocols**, while general employees focus on **basic cybersecurity hygiene**. Real-time tracking and **customizable learning paths** enhance engagement and compliance.

By implementing **role-based training**, GSG ensures the State maximizes cybersecurity awareness while optimizing training efficiency.

3.1.1.5 The Privacy and Cybersecurity Training Solution must support 25,000 active employees and on-site contractors.

GSG's Privacy and Cybersecurity Training Solution is built to support 25,000 active employees and on-site contractors, ensuring seamless scalability and performance. The platform is hosted on a highly available cloud-based infrastructure with load-balancing and auto-scaling capabilities to accommodate concurrent users without performance degradation.

To manage large-scale training efficiently, the system includes automated user provisioning through Active Directory integration, real-time progress tracking, and detailed compliance reporting. Employees and contractors can access the training via web-based portals and mobile applications, ensuring flexibility and accessibility.

GSG's solution also supports role-based access and customized learning paths, allowing tailored training for different employee groups. With 24/7 technical support and continuous updates, the platform guarantees reliable, secure, and future-proof training experience that meets the State's workforce requirements.

3.1.1.6 The Privacy and Cybersecurity Training Solution must be hosted in an LMS that is compatible with a SCORM 2.0 or higher.

GSG's Privacy and Cybersecurity Training Solution is hosted on a Learning Management System (LMS) that is fully compatible with SCORM 2.0 or higher, ensuring seamless integration with industry-standard e-learning platforms. The SCORM-compliant system allows for interoperability, content reusability, and tracking of learner progress across multiple sessions and devices.

The LMS provides comprehensive analytics, allowing administrators to monitor user engagement, completion rates, and assessment scores in real time. It also includes automated certification tracking, ensuring compliance with regulatory training requirements.

To enhance user experience, the LMS features intuitive navigation, mobile accessibility, and interactive training modules, such as gamification, quizzes, and scenario-based learning. Additionally, it supports integration with third-party applications and customized reporting dashboards to meet the State's training objectives.

By leveraging a SCORM 2.0+ compatible LMS, GSG ensures flexible, scalable, and standards-compliant training experience for all employees and contractors.

3.1.1.7 LMS must allow for additional 3" party SCORM compliant courses to be uploaded.

GSG's **Privacy and Cybersecurity Training Solution** is hosted on an **LMS that supports additional 3" party SCORM compliant.**

3.1.1.8 LMS must be able to integrate with Microsoft Lightweight Directory Access Protocol (LDAP).

GSG's LMS integrates with Microsoft Lightweight Directory Access Protocol (LDAP), ensuring secure authentication, user provisioning, and role-based access management. This integration allows employees and contractors to use their existing Microsoft credentials for Single Sign-On (SSO), enhancing security and streamlining user access.

Through LDAP synchronization, employee roles, departments, and permissions are automatically updated, ensuring that training content is assigned based on job functions. The integration also supports automated deactivation of accounts when employees leave, ensuring data security. With real-time directory updates, organizations maintain compliance while reducing administrative overhead.

3.1.1.9 The Privacy and Cybersecurity Training Solution must be branded with the West Virginia State Seal and Office of Technology Logos.

GSG ensures that the Privacy and Cybersecurity Training Solution is fully branded with the West Virginia State Seal and Office of Technology logos, maintaining a professional and official appearance. Custom branding ensures that employees recognize the training as an official state initiative, reinforcing the importance of cybersecurity education.

All training modules, login portals, dashboards, and certificates will display the official logos, ensuring consistency across the platform. The design also follows state-approved branding guidelines, including color schemes and typography, providing a cohesive and recognizable user experience.

3.1.1.10 The Privacy and Cybersecurity Training Solution must contain appropriate images to the training content and contain West Virginia-specific graphics.

GSG's training solution includes appropriate images, infographics, and West Virginia-specific graphics to enhance engagement and contextual relevance. The platform features customized visuals, including state government buildings, local infrastructure, and region-specific cyber threats, making the training content relatable and impactful for employees.

Interactive elements such as infographics, maps, and real-world cybersecurity case studies tailored to West Virginia's government sector ensure high engagement and knowledge retention. By incorporating state-specific scenarios, employees gain a practical understanding of how cybersecurity threats impact their local environment.

3.1.1.11 The Privacy and Cybersecurity Training Solution must contain a customer customizable "Resources™ section.

GSG's LMS includes a customizable "Resources" section, allowing the State to provide employees with important cybersecurity references, state policies, regulatory guidelines, and training materials. Administrators can upload documents, videos, FAQs, and external links to keep employees informed about emerging cyber threats, compliance updates, and security best practices.

This section can be customized by department or role, ensuring users access relevant and up-to-date cybersecurity resources. With searchable content, bookmarks, and real-time updates, employees can easily reference materials anytime, supporting continuous learning.

3.1.1.12 The Privacy and Cybersecurity Training Solution must generate optional Certificates of Completion

GSG's training solution generates optional Certificates of Completion, allowing employees to demonstrate compliance with cybersecurity and privacy training. Certificates include the West Virginia State Seal, employee name, course title, completion date, and administrator signature for verification.

Employees can download, print, or share their certificates for compliance tracking and professional development. Administrators can automate certificate issuance based on completion criteria and track certification status through LMS analytics, ensuring compliance across the workforce.

3.1.1.13 The Privacy and Cybersecurity Training Solution must provide options for course rollout assistance, specifically:

3.1.1.13.1 Launching an entire course
3.1.1.13.2 Launching sections of a course
3.1.1.13.3 Noting students as "passed" or "failed"
3.1.1.13.4 Pass or failed percentage or score must be customizable.

GSG's **Privacy and Cybersecurity Training Solution** provides **comprehensive course rollout assistance**, ensuring a **flexible and structured training implementation** for the State. The system includes **customizable deployment options** that allow administrators to launch courses efficiently while tracking progress and performance.

The **Launching an Entire Course** feature enables organizations to **deploy full training programs to employees and contractors simultaneously**. This approach ensures **consistent learning outcomes**, compliance tracking, and easy progress monitoring. Administrators can schedule course launches, send automated notifications, and enforce completion deadlines.

For a more phased approach, the **Launching Sections of a Course** feature allows training content to be **delivered in stages**, ensuring that employees absorb information **at a manageable pace**. This functionality supports **progressive learning**, allowing users to complete modules sequentially while retaining key cybersecurity concepts before moving to advanced topics.

To track learner performance, the **Noting Students as "Passed" or "Failed"** feature provides **real-time assessment tracking** based on quizzes, final exams, and completion status. Administrators can **automatically or manually assign pass/fail status**, ensuring flexibility in grading.

Additionally, the **Pass or Fail Percentage or Score Must Be Customizable** feature allows organizations to set **customized scoring thresholds** to align with their training policies. Whether using **a standard pass mark (e.g., 70%) or role-specific criteria**, administrators can adjust scoring rules based on job function, risk level, or compliance requirements.

By integrating **customizable course rollout options**, GSG ensures that the State can **effectively deploy, manage, and track** cybersecurity training, ensuring a **well-trained, security-aware workforce**.

3.1.1.14 The Privacy and Cybersecurity Training Solution must allow knowledge checks and graded assessments

GSG's **Privacy and Cybersecurity Training Solution** includes **built-in knowledge checks and graded assessments** to ensure **effective learning, retention, and compliance tracking** for the State. These assessments help **reinforce key cybersecurity and privacy concepts**, allowing employees to demonstrate their understanding before progressing through the course.

The **knowledge checks** feature provides **interactive quizzes, scenario-based questions, and real-time feedback** throughout the training modules. These checks help users assess their comprehension and identify areas requiring further review.

The **graded assessments** are fully **customizable**, allowing administrators to set **passing scores, question formats (multiple-choice, true/false, short answers), and assessment difficulty levels**. The system supports **automated grading, manual review options, and retake settings**, ensuring flexible evaluation methods.

With **detailed reporting and analytics**, administrators can track **assessment scores, completion rates, and knowledge gaps**, ensuring compliance with cybersecurity training requirements. By integrating **knowledge checks and graded assessments**, GSG's solution enhances **engagement, accountability, and overall cybersecurity awareness** across the workforce.

3.1.1.15 The Privacy and Cybersecurity Training Solution must have a targeted length of at least 30 minutes, and no more than 45 minutes, of education content.

GSG's Privacy and Cybersecurity Training Solution ensures that educational content is comprehensive yet concise, lasting between thirty and forty-five minutes. This duration balances thorough training coverage with user engagement, ensuring employees receive critical cybersecurity knowledge without overwhelming them. The content includes interactive modules, real-world case studies, and quizzes to reinforce learning. By maintaining an optimal training length, employees remain focused and retain information more effectively. The course structure is modular, allowing organizations to adapt content based on user roles and needs, ensuring flexibility and relevance while meeting compliance requirements

3.1.1.16 The Privacy and Cybersecurity Training Solution must provide a phishing simulator along with training if an end user fails the phishing simulation.

GSG's Phishing Simulator provides a real-world phishing attack experience, allowing organizations to test, train, and enhance employee awareness. If an end user fails the phishing simulation, the system automatically enrolls them in targeted training. This training includes interactive lessons on identifying phishing attempts, real-world phishing case studies, and tips for avoiding common threats.

The system tracks repeat failures and adapts training modules, accordingly, ensuring progressive learning. Administrators can analyze user performance, measure improvements, and adjust training content based on phishing campaign results. With real-time feedback and interactive learning, employees gain practical cybersecurity skills, reducing the risk of successful phishing attacks. GSG's adaptive approach ensures users learn from mistakes while reinforcing best practices for email security.

3.1.1.17 The Phishing Simulator must have predesigned and editable phishing templates for users conducting the simulation.

3.1.1.17.1 Customization must be included for the email message itself along with attachments and web address the end user will click on.

3.1.1.17.2 Predesigned templates must mimic current real-world phishing attacks.

GSG's Phishing Simulator includes a library of predesigned phishing templates based on real-world phishing tactics, such as credential harvesting, fake invoices, and social engineering scams. These templates are fully customizable, allowing administrators to edit email content, subject lines, sender details, and embedded links to mimic emerging threats.

Organizations can modify templates to align with industry-specific threats, regulatory requirements, or past security incidents. The system also supports A/B testing, enabling cybersecurity teams to evaluate which phishing tactics are most effective against employees. By offering both standardized and customizable templates, GSG's solution enhances phishing awareness training, making it relevant, practical, and adaptable to an evolving threat landscape.

3.1.1.18 The phishing simulator must support multi-factor authentication for log-in.

GSG's Phishing Simulator enforces Multi-Factor Authentication (MFA) to enhance security and prevent unauthorized access. Users must authenticate using at least two verification methods, such as passwords, One-Time Passcodes (OTP), biometric authentication, or push notifications.

The MFA system integrates with existing authentication platforms, including Microsoft Authenticator, Google Authenticator, and hardware-based security keys. Administrators can enforce MFA policies at different levels, ensuring that privileged users, administrators, and cybersecurity teams follow strict authentication measures.

By implementing MFA, GSG ensures that the phishing simulation platform remains secure, protecting sensitive data, user reports, and analytics dashboards from unauthorized access. The system also supports adaptive MFA, requiring stronger authentication based on user behavior and risk level.

3.1.1.19 The phishing simulator must integrate with Microsoft Lightweight Directory Access Protocol (LDAP).

GSG's Phishing Simulator integrates seamlessly with Microsoft Lightweight Directory Access Protocol (LDAP), allowing for centralized authentication and RBAC. This integration enables automated user provisioning, ensuring that employees and contractors are automatically enrolled in training based on their job roles and security requirements.

With LDAP integration, administrators can track employee participation, enforce security policies, and streamline user access management. The system also supports Single Sign-On (SSO), reducing login friction while maintaining secure authentication practices. By leveraging LDAP, GSG ensures seamless user experience, enhanced security, and simplified administration for phishing simulation and cybersecurity training programs.

3.1.1.20 Provide reports, visualizations and graphs showing user interactions.

3.1.1.20.1 Reports must be able to be exported to popular file formats for distribution such as .pdf, .csv, .xlsx, etc.

3.1.1.20.2 Reports must be able to generate reports for specific end-users or specific state.

GSG's Phishing Simulator provides detailed reports, visualizations, and analytics dashboards to track user performance, phishing test outcomes, and training progress. Administrators can generate customized reports showing click-through rates, phishing email interactions, and employee pass/fail statistics.

The platform supports exportable reports in popular formats, including .pdf, .csv, and .xlsx, ensuring compatibility with compliance audits, executive summaries, and cybersecurity policy reviews. The system also allows filtering reports by individual users, departments, or entire state-level organizations, providing granular visibility into security awareness trends.

Visual dashboards include interactive graphs, heat maps of phishing attempts, and performance comparisons over time, allowing security teams to identify high-risk users and departments. With automated reporting schedules, administrators can receive periodic updates on phishing campaign effectiveness and training completion rates, ensuring continuous monitoring and improvement.

3.1.1.21 The phishing simulator must support automation for creating future tests and automatically launching them on the specified date.

GSG's Phishing Simulator supports automation for scheduling and launching future phishing tests, ensuring that employees receive ongoing training without manual intervention. Administrators can preconfigure phishing campaigns, setting specific dates, target groups, and attack types to be launched automatically.

The automation feature allows for progressive difficulty adjustments, gradually increasing phishing sophistication based on employee performance trends. Security teams can schedule recurring tests at intervals, ensuring that phishing awareness remains top-of-mind for employees.

With AI-driven analytics, the system adjusts future phishing tests based on previous results, targeting users who have failed prior simulations with more sophisticated phishing tactics. By automating phishing test deployment, GSG's solution ensures that the State maintains an ongoing, proactive defense against social engineering attacks.

3.1.1.22 The phishing simulator must also include a reporting option for the end users to report phishing emails and track the reporting statistics for testing campaigns.

3.1.1.22.1 The reporting option must be able to be utilized for all phishing emails reported to the Office of Technology.
3.1.1.22.2 Be sure to describe and list all tools or processes that can be used to analyze malicious email with the reporting tool.

GSG's Phishing Simulator includes a phishing email reporting feature, allowing users to report suspicious emails directly to the Office of Technology. Employees can use a one-click "Report Phishing" button within their email client, triggering immediate analysis and tracking.

All reported emails are logged, categorized, and analyzed using advanced threat intelligence tools such as:

- AI-based threat detection to identify phishing patterns.
- URL sandboxing to safely inspect embedded links.
- Attachment scanning for malware or malicious scripts.
- Behavioral analysis to detect social engineering tactics.

The reporting tool provides real-time statistics on employee-reported phishing attempts, enabling cybersecurity teams to track reporting trends and user vigilance. The system also compares reported phishing emails with ongoing phishing simulation campaigns, helping to evaluate employee awareness and responsiveness.

By integrating phishing reporting and advanced email analysis, GSG ensures continuous improvement in the State's cybersecurity resilience while providing actionable intelligence for security teams.

3.1.1.23 The phishing simulator must have the ability to test for user input (i.e., the user clicks on a link and provides requested information to "scammers")

GSG's Phishing Simulator includes advanced testing capabilities to evaluate user interaction beyond link clicks, specifically assessing whether users input credentials or sensitive information on simulated phishing pages. The simulator mimics real-world phishing tactics, presenting login pages, fake surveys, or malicious forms to analyze user responses.

If a user enters credentials or other requested data, the system logs the interaction, providing detailed analytics to administrators. The captured data remains encrypted and is used only for security awareness training, ensuring privacy and compliance. The simulator can be configured to send immediate educational feedback when a user inputs sensitive data, guiding them on identifying phishing threats.

Reports highlight which users provided input, the type of information entered, and behavioral patterns, helping security teams identify high-risk individuals. By simulating credential harvesting techniques, the training solution reinforces secure browsing habits and strengthens organizational cybersecurity awareness.

3.1.1.24 The phishing simulator must support attachments.

GSG's Phishing Simulator supports the inclusion of attachments to mimic phishing emails that use malicious file delivery tactics. Administrators can configure simulated attacks using various file types, including PDFs, Word documents, and Excel spreadsheets, to train users on recognizing malicious attachments.

The system can generate realistic phishing scenarios where opening an attachment prompts user with a fake login request or enables simulated malware execution, measuring their response. If a user opens or interacts with an attachment, the simulator records the action and provides immediate feedback on how to verify email attachments safely.

Additionally, the simulator tracks email forwarding behaviors, identifying employees who inadvertently spread potentially harmful content. Reports include who opened attachments, what actions they took, and timestamps, helping security teams' pinpoint vulnerabilities. By incorporating attachment-based phishing simulations, GSG ensures employees are well-prepared to identify and avoid real-world malware threats.

3.1.1.25 The phishing simulator must be able to provide, at a minimum, statistics on: users that clicked links and/or visited sites, provided credentials, opened or forwarded the email, time stamps for interactions, phishing training and test results.

GSG's Phishing Simulator offers comprehensive data tracking and reporting to analyze user behavior and test results. The system records statistics on:

- **Users who clicked phishing links and visited fake sites.**
- **Users who provided credentials** on fraudulent login pages.
- **Users who opened or forwarded phishing emails.**
- **Time stamps of each interaction.**
- **Phishing training completion rates and test scores.**

Administrators can access real-time dashboards displaying graphical insights, heat maps, and trend analysis. Reports can be filtered by department, individual users, or risk level, allowing security teams to identify high-risk employees and tailor training accordingly.

All reports are exportable in multiple formats (.pdf, .csv, .xlsx) for compliance documentation and executive reviews. The simulator also supports automated reporting schedules, ensuring regular updates on phishing campaign effectiveness. With these detailed analytics, GSG's solution enhances proactive threat detection and security awareness improvements.

3.1.1.26 The phishing simulator must support phishing campaigns up to 5,000 users/email addresses.

GSG's Phishing Simulator is built for large-scale deployment, supporting phishing campaigns for up to 5,000 users per simulation. The system efficiently manages bulk email distribution, ensuring secure and targeted phishing tests across the organization.

To prevent email filtering issues, the simulator integrates email whitelisting options, allowing phishing simulations to bypass spam filters while maintaining security best practices. Campaigns can be scheduled in waves or distributed to segmented user groups based on departments, job roles, or security levels.

The platform includes automated scheduling, allowing administrators to launch and monitor multiple concurrent phishing campaigns. User progress tracking and risk scoring help security teams evaluate employee responses, ensuring continuous security improvement.

By supporting large-scale, real-world phishing tests, GSG's solution provides actionable insights into the State's cybersecurity resilience, helping the State reduce phishing attack risks effectively.

3.1.1.27 The phishing simulator must have end-user education options in the form of an educational landing page, reply email, or training module.

GSG's Phishing Simulator includes three distinct educational response mechanisms to train users:

- Educational Landing Pages – Users who click on phishing links are redirected to a customized landing page explaining the phishing attempt and providing security tips.
- Reply Email Training – If users respond to phishing emails, they receive automated email feedback outlining the risks and best practices for verifying emails.
- Interactive Training Modules – Users failing phishing simulations are automatically enrolled in an interactive training course, covering phishing identification, social engineering tactics, and prevention strategies.

Administrators can customize training content based on specific phishing scenarios. The system tracks training completion rates, ensuring accountability and improvement. By providing immediate, interactive education, GSG reinforces security awareness and behavioral changes, reducing the likelihood of future phishing attacks.

3.1.2 Vendor should provide documentation with its bid showing how its product meets the specifications contained in this solicitation. This information must be provided prior to award.

GSG is committed to full transparency and compliance with procurement requirements. With its bid, GSG provides:

- A detailed technical whitepaper outlining how the solution meets all functional and security specifications.
- Product documentation, including user guides, training manuals, and integration instructions.
- Security certifications and compliance documentation, demonstrating adherence to SCORM, LDAP, MFA, and phishing simulation best practices.
- Case studies and client references showcasing successful implementations of the solution in similar government environments.
- A test environment demonstration, allowing stakeholders to evaluate the phishing simulator's features before deployment.

This documentation ensures the State receives a fully vetted, compliant, and effective phishing awareness solution before the contract award.

3.1.3 Vendor should include Optional Annual Renewal Years pricing for Years 2, 3, and 4. Optional Annual Renewals will be initiated by the Agency, agreed to by the Vendor, and executed via formal Change Order processed by the WV Purchasing Division.

GSG provides flexible and transparent pricing for optional annual renewals for Years 2, 3, and 4, ensuring long-term support and continuity. The renewal pricing includes:

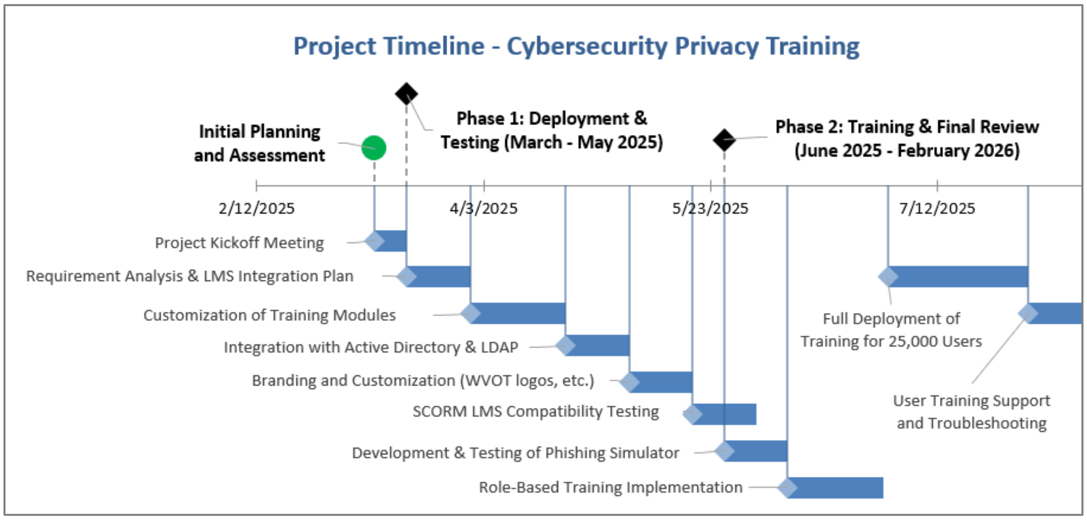
- Full access to phishing simulator updates and feature enhancements.
- Ongoing technical support and maintenance for system stability and performance.
- Continuous content updates, including new phishing scenarios, emerging cyber threats, and compliance regulation changes.
- Scalability options, allowing for additional users and expanded phishing campaigns as needed.

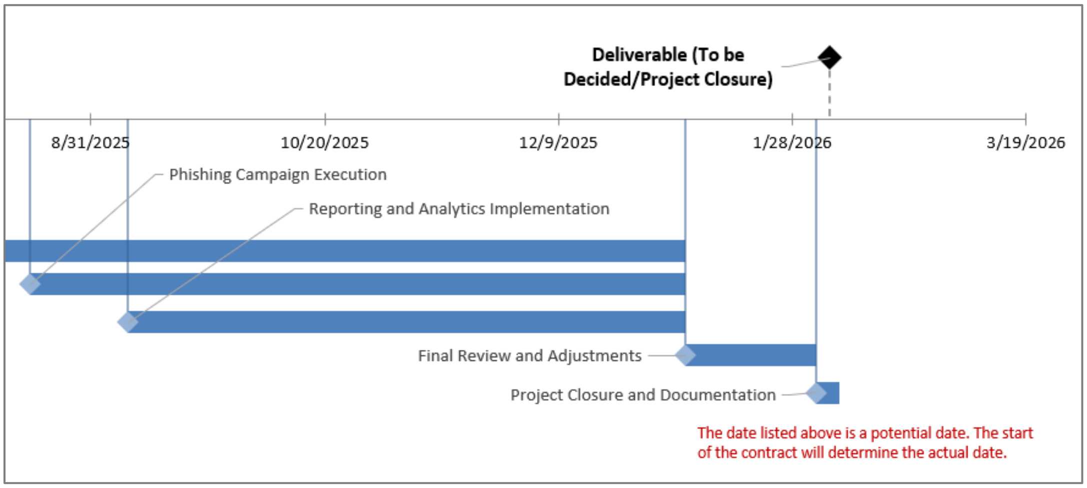
The renewal process is streamlined through a formal Change Order, ensuring that both the Agency and GSG mutually agree on extensions. Pricing remains competitive and predictable, preventing unexpected budget increases.

GSG's renewal structure ensures long-term effectiveness, cost-efficiency, and adaptability for the State's cybersecurity training needs.

4.1 Timeline and Workplan

The following is a sample project timeline for carrying out scope requirements:





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

Task ID	Task Name	Start Date	Duration	Milestone/Deliverable	Responsible Party
Phase 1: Deployment and Testing (March - May 2025)					
1	Project Kickoff Meeting	3/10/2025	1 week	Kickoff Meeting with WVOT	Vendor, WVOT
2	Requirement Analysis & LMS Integration Plan	3/17/2025	2 weeks	Finalized Training & LMS Integration Plan	Vendor
3	Customization of Training Modules	3/31/2025	3 weeks	Customized Training Modules Ready	Vendor
4	Integration with Active Directory & LDAP	4/21/2025	2 weeks	AD & LDAP Integration Completed	Vendor, WVOT IT
5	Branding and Customization (WVOT logos, etc.)	5/5/2025	2 weeks	Training Platform with WVOT Branding	Vendor
6	SCORM LMS Compatibility Testing	5/19/2025	2 weeks	SCORM Compliance Confirmed	Vendor, WVOT
7	Development & Testing of Phishing Simulator	5/26/2025	2 weeks	Phishing Simulator Fully Functional	Vendor
Phase 2: Training and Final Review (June 2025 - February 2026)					
8	Role-Based Training Implementation	6/9/2025	3 weeks	Role-Based Modules Deployed	Vendor
9	Full Deployment of Training for 25,000 Users	7/1/2025	4 weeks	Full Training Rollout	Vendor, WVOT
10	User Training Support and Troubleshooting	8/1/2025	Ongoing (7 months)	Continuous Training Assistance & Issue Resolution	Vendor
11	Phishing Campaign Execution	8/18/2025	Every 3 months	Periodic Phishing Campaign Reports	Vendor, WVOT
12	Reporting and Analytics Implementation	9/8/2025	3 weeks	Reporting Dashboard Ready	Vendor
13	Final Review and Adjustments	1/5/2026	4 weeks	Final Adjustments Completed	Vendor, WVOT
14	Project Closure and Documentation	2/2/2026	4 weeks	Final Project Report Submitted	Vendor

5. References

GSG has considerable experience in providing cybersecurity services to a broad variety of private and public sector clients. GSG provides top-notch, proven components of success, experience and expertise for information security, the use of the latest technologies and methods, the ability to deliver service that exceeds expectations, and a proven commitment to serving information security needs of all kinds. GSG is experienced in providing a wide range of IT services throughout the United States and worldwide to local, state, and federal agencies and corporations. We have earned a national reputation as a valuable partner that consistently exceeds customer expectations.

The following are the references for which we have performed similar services:

5.1.1 Reference #1 Cyber Security Services: City of New Orleans

Reference #1 Cyber Security Services	
Company Name	**City of New Orleans**
Address	1300 Perdido Street, Suite 4W07, New Orleans, Louisiana 70112
Point of Contact	LaShonda Hunter-Mendy, ITI Data Center Manager (504) 658-7624 || LaShonda.Hunter@nola.gov
Dates	September 2022 – September 2024
Description of Services	GSG has been selected as a strategic partner by the City of New Orleans – New Orleans Police Department (NOPD) to purchase multiple, specific technology and cyber security services and products that are core components of their enterprise infrastructure. We are providing: • Data Management • Data Security • Network Detection Response (NDR) • Endpoint Detection Response (EDR) • Managed Defense and Response (MDR) • Endpoint Protection • Email Security Firewall • Incident Response Services • Security Awareness Training • Vulnerability Assessments • Penetration Testing • Security Information Event Manager (SIEM) • Threat Remediation • Forensic Analysis • Web Application Vulnerability Scanner • Multifactor Authentication and Recovery Services
	Relevancy in Size: GSG's work with the New Orleans Police Department (NOPD), which involves comprehensive cybersecurity services, aligns with the RFP's scale of supporting large organizations. The scope of services, including security awareness for a large workforce and integration with existing systems, demonstrates GSG's capability to manage projects for entities with extensive operational requirements. **Relevancy in Scope:** GSG's involvement in network detection, endpoint protection, vulnerability assessments, penetration testing, and incident response aligns directly with the RFP's need for a comprehensive and customizable cybersecurity training solution. Our services encompass a wide range of technology areas, ensuring alignment with the RFP's broad and diverse security needs. **Relevancy in Complexity:** GSG's deployment of advanced cybersecurity technologies like NDR, EDR, and SIEM, along with incident response and threat remediation, showcases our ability to manage complex security environments. This mirrors the RFP's complexity in delivering an adaptive, scalable, and secure training solution that integrates with large-scale infrastructure and multiple cybersecurity domains.

5.1.2 Reference #2 Cybersecurity Risk Assessment: Boston Public Health Commission

Reference #2 Cybersecurity Risk Assessment	
Company Name	**Boston Public Health Commission (BPHC)**
Address	1010 Massachusetts Ave, 2nd Floor,

	Boston, MA 02118
Point of Contact	Jeffrey Beers, Director of Technical Services/BPHC and Boston EMS 617-534-2368 || JBeers@bphc.org
Dates	June 2023 - October 2023
Description of Services	GSG provided a comprehensive cybersecurity vulnerability assessment of the BPHC's network. Additionally, GSG offered assessments through information security guidance aligned with industry standards and best practices, including methodologies outlined in the National Institute for Standards and Technology (NIST), Cyber Security Framework (CSF), HIPAA, ISO/IEC, etc. GSG developed an information security roadmap to prepare a plan for remediating any identified items. GSG conducted penetration testing and perimeter testing, which included internal network assessments, external network assessments, user privilege escalation, segmentation testing, wireless scanning (both private and guest), applications, database assessments, brute force attacks, social engineering (via phone and email), phishing/spear phishing attacks, employee impersonation, and pretexting.
	Relevancy in Size: GSG's comprehensive cybersecurity services, including vulnerability assessments, penetration testing, and information security guidance, demonstrate our capability to handle large-scale cybersecurity needs, similar to the requirements of supporting 25,000 employees and contractors as outlined in the RFP. **Relevancy in Scope:** GSG's work covering a broad range of cybersecurity areas—such as internal/external network assessments, social engineering, and database security—directly aligns with the RFP's need for an adaptive and customizable cybersecurity training solution across various critical topics. **Relevancy in Complexity:** GSG's use of advanced testing methods, including social engineering attacks and segmentation testing, highlights our expertise in handling complex environments, mirroring the RFP's focus on delivering a multifaceted and role-based training solution for diverse cybersecurity challenges.

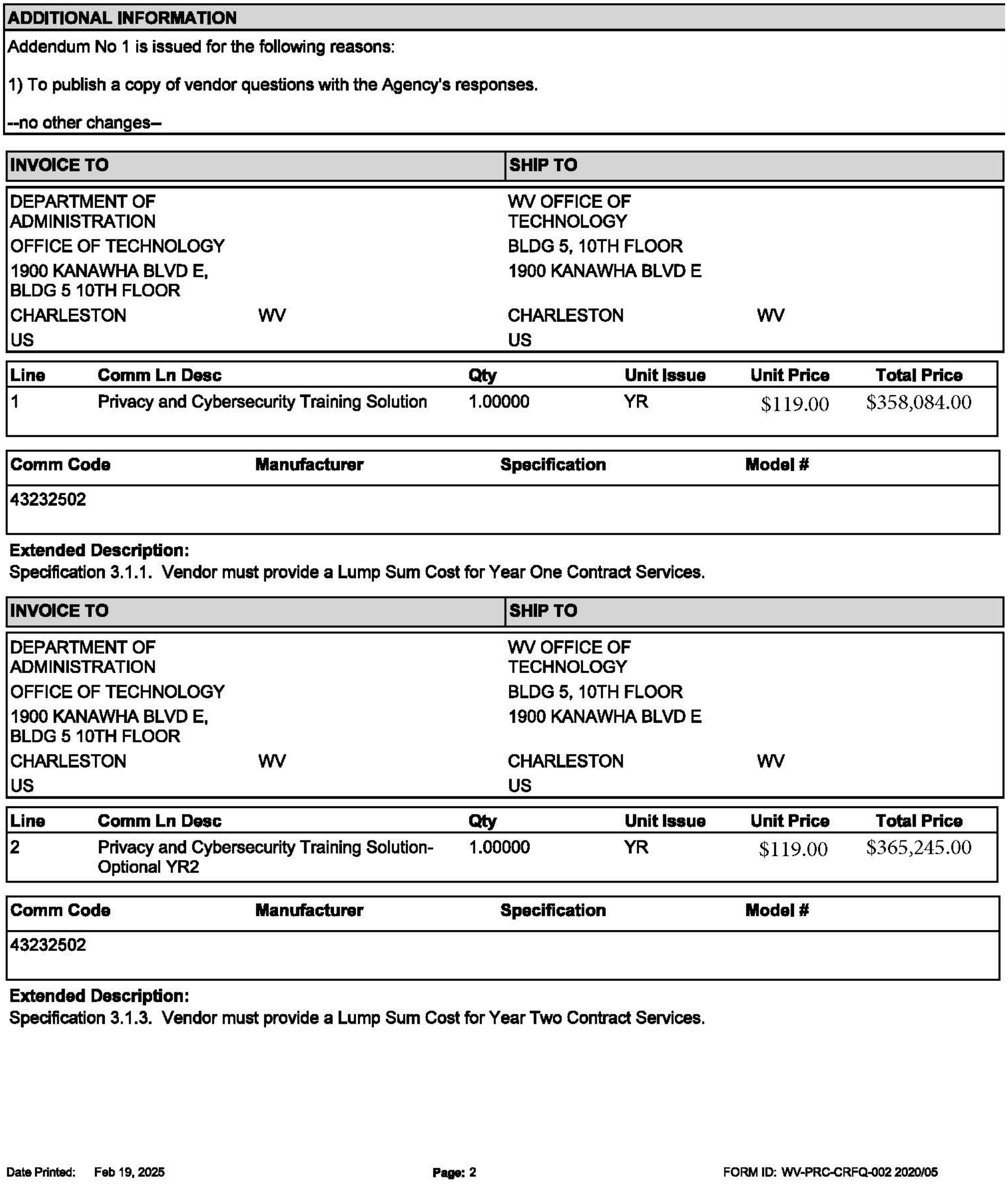
5.1.3 Reference #3 Penetration Testing and Digital Forensics: Lansing Board of Water and Light

Reference #3 Penetration Testing and Digital Forensics	
Company Name	**Lansing Board of Water and Light (LBWL)**
Address	1110 S. Pennsylvania Building E Lansing, Michigan 48912
Point of Contact	Vernon Myers, Security Lead and Engineer, Information Technology (517) 702 -6569 || Vernon.Myers@lbwl.com
Dates	January 2020 – January 2023
Description of Services	GSG is providing penetrating testing and digital forensic examination of the computing environment to: • Assist in the identification of any indicators of compromise not otherwise detected by existing deployed cybersecurity tools. • Perform remediation of all detected malware and inoculating the environment against reinfection where possible. • Tasks for this project include:

	○ Testing for weaknesses in web and mobile application interfaces. ○ Vulnerability testing for SCADA systems. ○ Testing for misconfigurations of application servers, databases, and middleware impacting cybersecurity. ○ Assessing susceptibility to known and common exploits and social engineering attacks. ○ Malware identification and remediation. ○ System hardening recommendations (hardware and software). ○ Tailored cybersecurity training.
	Relevancy in Size: GSG's extensive cybersecurity services, including penetration testing and malware remediation, are suitable for large-scale environments, similar to the requirement of supporting 25,000 active employees and contractors outlined in the RFP. **Relevancy in Scope:** The wide-ranging tasks GSG performs—such as vulnerability testing, SCADA assessments, social engineering, and malware remediation—align with the RFP's need for a comprehensive, customizable, and adaptable cybersecurity training solution covering diverse topics. **Relevancy in Complexity:** GSG's handling of complex cybersecurity elements like system hardening, vulnerability testing, and incident remediation demonstrates our ability to manage sophisticated environments, mirroring the RFP's need for a robust and advanced training solution across a range of cybersecurity threats.

6. Pricing

The following is our price for this requirement:



ADDITIONAL INFORMATION
Addendum No 1 is issued for the following reasons: 1) To publish a copy of vendor questions with the Agency's responses. --no other changes--

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Privacy and Cybersecurity Training Solution	1.00000	YR	$119.00	$358,084.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

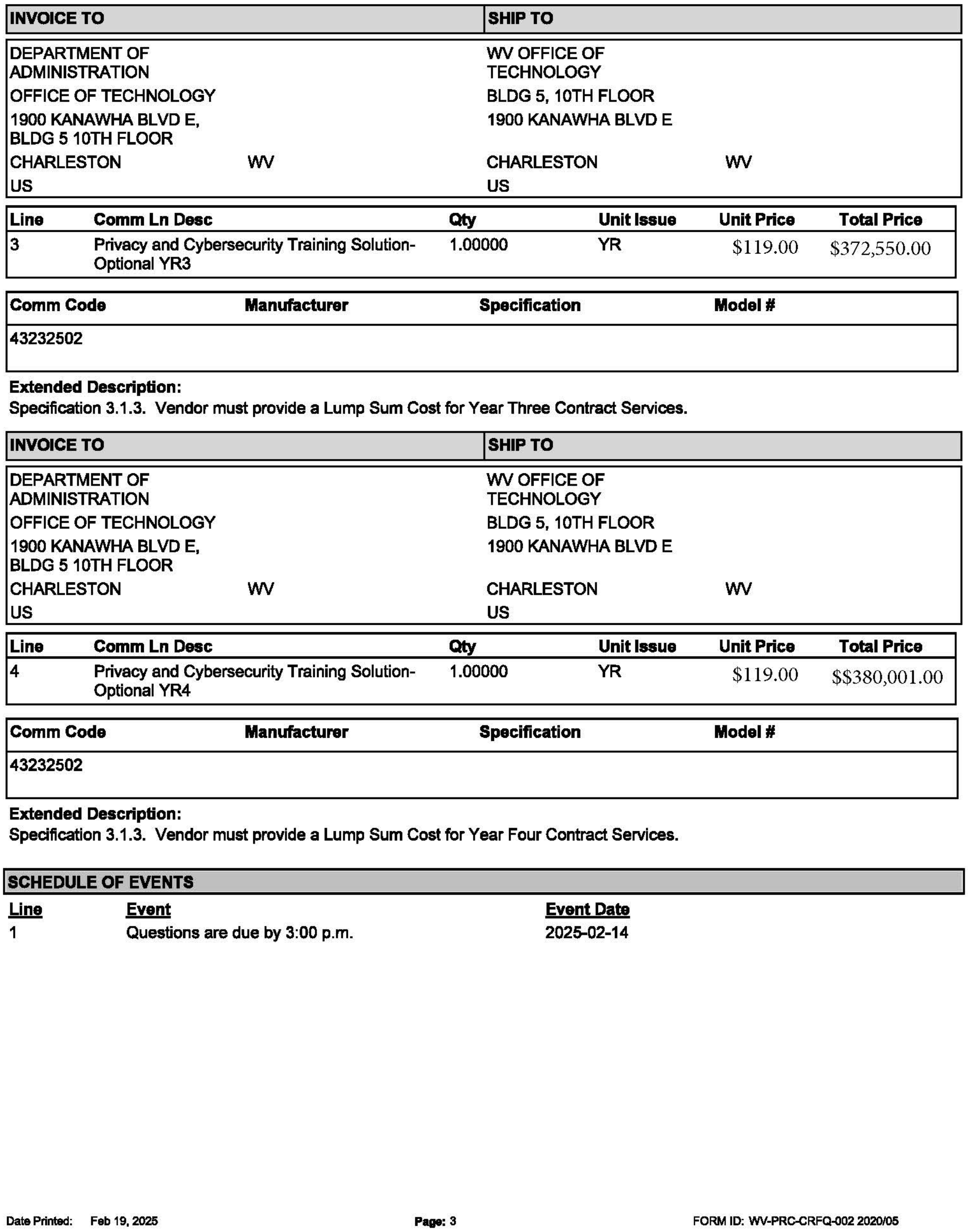
INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV US	WV OFFICE OF TECHNOLOGY BLDG 5, 10TH FLOOR 1900 KANAWHA BLVD E CHARLESTON WV US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Privacy and Cybersecurity Training Solution-Optional YR2	1.00000	YR	$119.00	$365,245.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.

Date Printed: Feb 19, 2025 Page: 2 FORM ID: WV-PRC-CRFQ-002 2020/05



INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Privacy and Cybersecurity Training Solution-Optional YR3	1.00000	YR	$119.00	$372,550.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

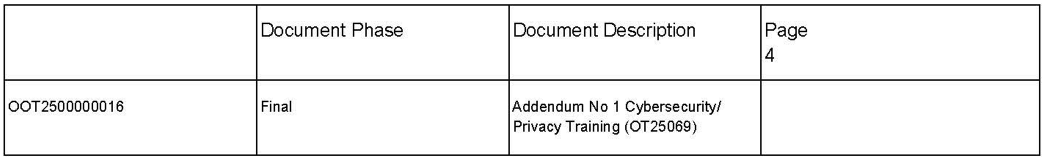
Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Privacy and Cybersecurity Training Solution-Optional YR4	1.00000	YR	$119.00	$$380,001.00

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2025-02-14



	Document Phase	Document Description	Page 4
OOT2500000016	Final	Addendum No 1 Cybersecurity/ Privacy Training (OT25069)	

Payment Schedule:

GSG will accept a 100% services fee invoice upon acceptance of all final deliverables and/or tasks/sub-tasks.

Assumptions:

The above Fixed Cost is based upon the scope and clarification response provided in the RFP and Q&A document. If any of the scope and/or quantities of devices or locations increases, then our effort will be increased appropriately.

GSG proposes a 2% annual escalation for the proposed total cost from the second year to provide the most competitive pricing for the entire contract duration.

Creating Training Material:

1. Content Planning and Structure
    - Break the approximate 200 slides into logical sections or modules (e.g., 10 modules with 20 slides each).
    - Each module should have a clear focus, with concise content and supporting visuals.
    - Organize the content hierarchy: main topics, subtopics, and supporting details.
    - Quiz questions to be designed
2. Slide Design & Formatting
    - Create a consistent template for all slides, including colour schemes, fonts, and layout to maintain uniformity.
    - Consider using PowerPoint, Google Slides, or other professional tools to streamline the design.
    - Include placeholder images links initially and later replace them with finalized visuals.
3. Adding Images & Graphics
    - Create or source images, infographics, or diagrams that complement the content.
    - Place images thoughtfully to illustrate key points without overcrowding the slide.
    - If you're creating custom graphics (e.g., flowcharts, diagrams), use design tools like Canva or Adobe Illustrator.
4. Finalizing and Review
    - Review the entire presentation for consistency, clarity, and accuracy.
    - Double-check slide transitions, animations, and timing.
    - Mock run

- Get feedback from others (colleagues or peers) to ensure the training content is clear and engaging.

KnowBe4 - Security Awareness Training (Platinum Support): GSG's pricing for third-party software such as KnowBe4 is based on the total number of users.

Unlimited Phishing Security Tests, Automated Security Awareness Program (ASAP), Security 'Hints & Tips', KnowBe4 Learner App, Training Access Level I, Automated Training Campaigns, Brandable Content, Assessments, AI-recommended training, Phish Alert Button, Phishing Reply Tracking, User Provisioning via Active Directory or SCIM Integration, SSO/SAML Integration, Industry Benchmarking, Virtual Risk Officer™, Advanced Reporting, Global Technical Support, Training Access Level II, Monthly Email Exposure Check, Smart Groups, Reporting, User Event and Webhook APIs, Security Roles, Social Engineering Indicators (SEI), USB Drive Test, SecurityCoach™ (Optional add-on), Compliance Plus (Optional add-on), KnowBe4 Student Edition (Optional add-on), PhishER™ Plus (Stand-alone product or optional add-on).

For effective project scheduling, the State 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 State stakeholders should be available as needed to ensure the timeliness and success of this project.

Depending upon internal security testing requirement, either the State or GSG will provide the laptop to accomplish internal security testing.

The GSG cyber team believes that the entire scope of work can be successfully accomplished remotely utilizing virtual meetings/conferences. If any onsite work is required, then we will determine the specific need for onsite work and the corresponding accurate travel cost. We will charge for actual travel cost as per IRS / Federal Travel Regulation. For understanding purpose, 1 trip of 3 to 5 days per person travel costs around $1500 including flight, lodging, meals, etc.

The State will provide access to all proprietary information, applications, and systems including third parties necessary for the success of this project.

During this engagement, any vulnerabilities, sensitive information, or configuration data discovered during this engagement won't be shared with anybody but the designated State employees.

Some tasks may be accomplished in parallel depending upon the information, systems, and stakeholders' availability.

During this effort, GSG will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between the State and third parties.

The State 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 State's inability to meet stated prerequisites prior to an engagement, nor when delays result from the State personnel not being available to provide the required support for the success of this project.

Servers' OS installation is not part of this scope.

The proposal will be valid for 90 days.

KnowBe4 Assumptions:

1. GSG includes a 5% discount on the MSRP Price.

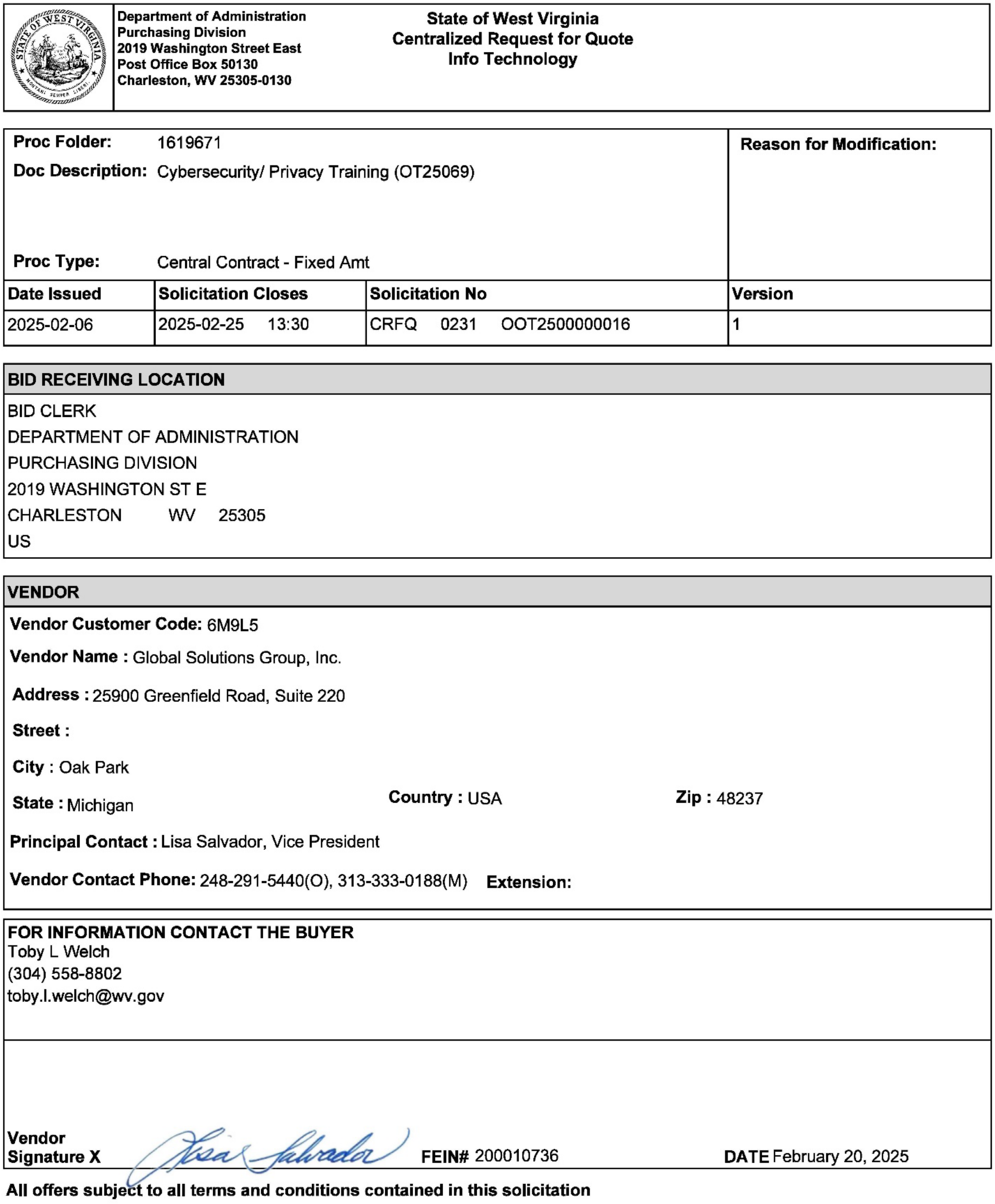
2. KnowBe4 offers SaaS subscription is priced per seat, per year. It offers Silver, Gold, Platinum or Diamond levels to meet organization's needs, comprised of three levels of training access and increasingly powerful features.

3. KnowBe4 offers attractive discounts for a 3-year contract.

4. Pricing in US dollars as per January 2025 list pricing for North America. List pricing may be modified at any time.

7. Required Forms

7.1 Cover Page Version 1



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder: 1619671			**Reason for Modification:**
Doc Description: Cybersecurity/ Privacy Training (OT25069)			
Proc Type: Central Contract - Fixed Amt			
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2025-02-06	2025-02-25 13:30	CRFQ 0231 OOT2500000016	1

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 6M9L5

Vendor Name : Global Solutions Group, Inc.

Address : 25900 Greenfield Road, Suite 220

Street :

City : Oak Park

State : Michigan **Country :** USA **Zip :** 48237

Principal Contact : Lisa Salvador, Vice President

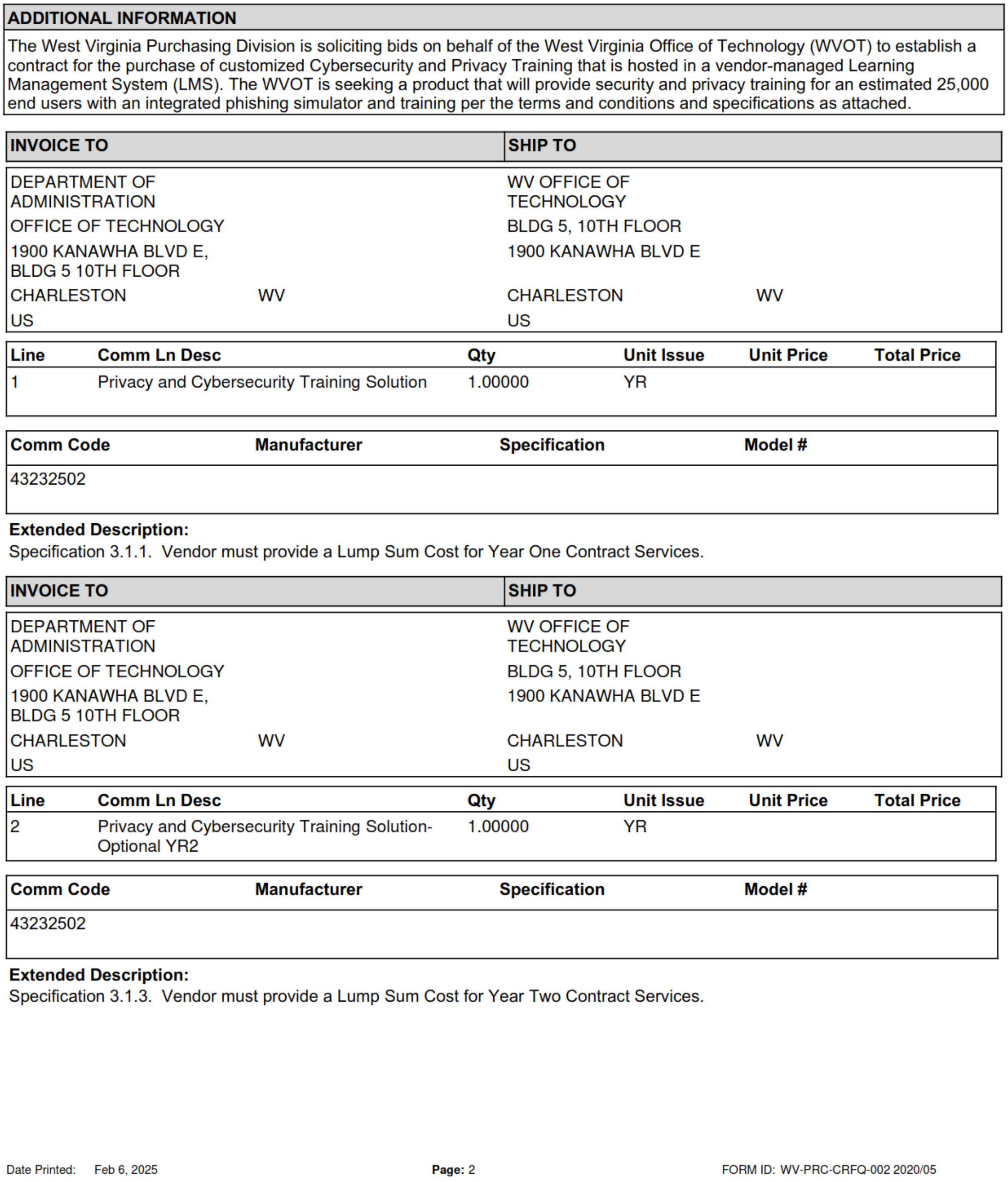
Vendor Contact Phone: 248-291-5440(O), 313-333-0188(M) **Extension:**

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X Lisa Salvador **FEIN#** 200010736 **DATE** February 20, 2025

All offers subject to all terms and conditions contained in this solicitation

Date Printed: Feb 6, 2025 **Page:** 1 FORM ID: WV-PRC-CRFQ-002 2020/05



ADDITIONAL INFORMATION
The West Virginia Purchasing Division is soliciting bids on behalf of the West Virginia Office of Technology (WVOT) to establish a contract for the purchase of customized Cybersecurity and Privacy Training that is hosted in a vendor-managed Learning Management System (LMS). The WVOT is seeking a product that will provide security and privacy training for an estimated 25,000 end users with an integrated phishing simulator and training per the terms and conditions and specifications as attached.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Privacy and Cybersecurity Training Solution	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

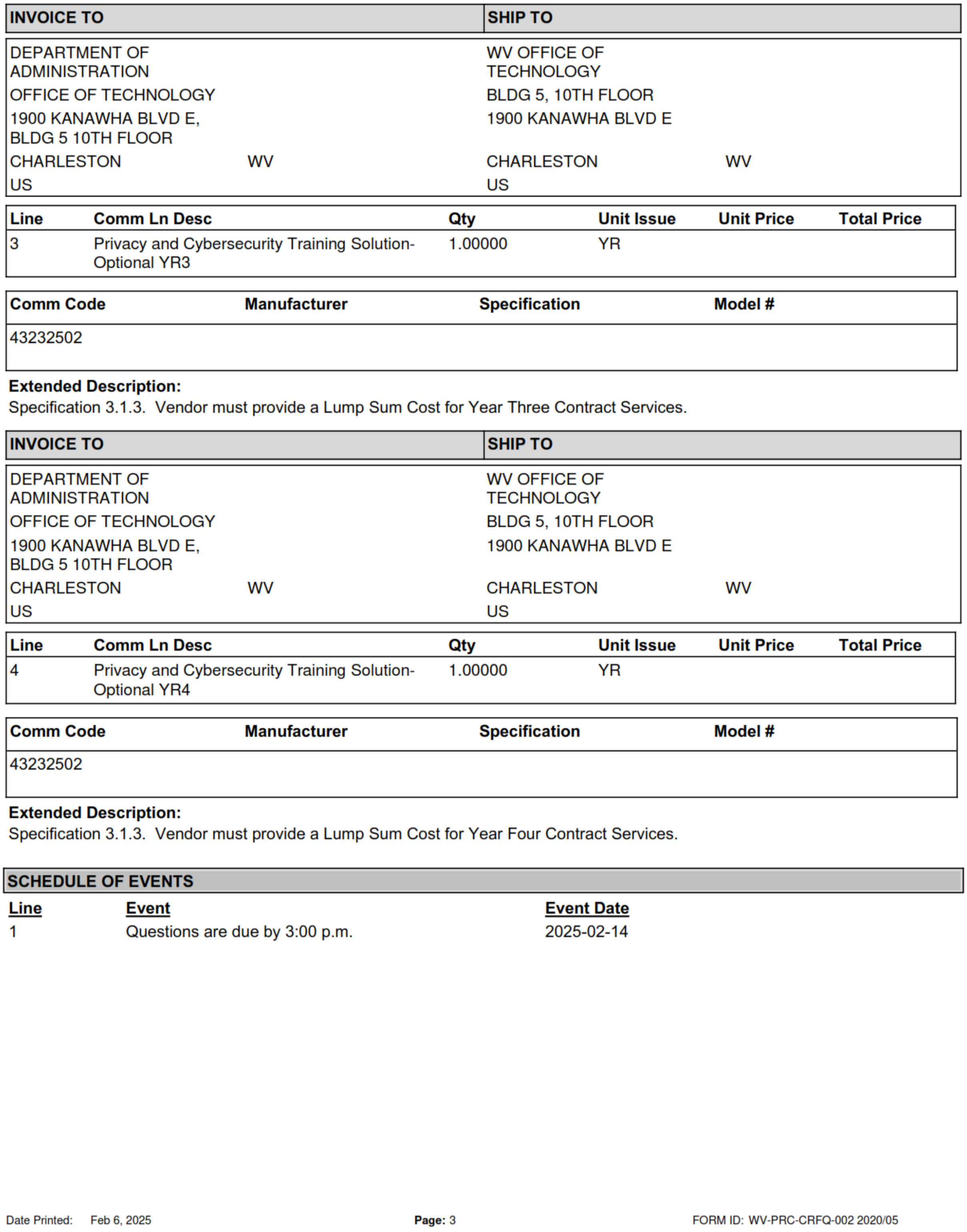
Extended Description:
Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Privacy and Cybersecurity Training Solution-Optional YR2	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.



INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Privacy and Cybersecurity Training Solution-Optional YR3	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

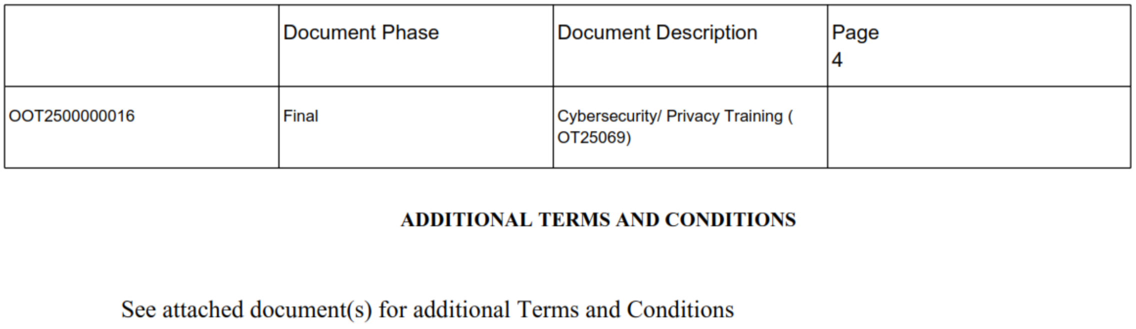
Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Privacy and Cybersecurity Training Solution-Optional YR4	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2025-02-14

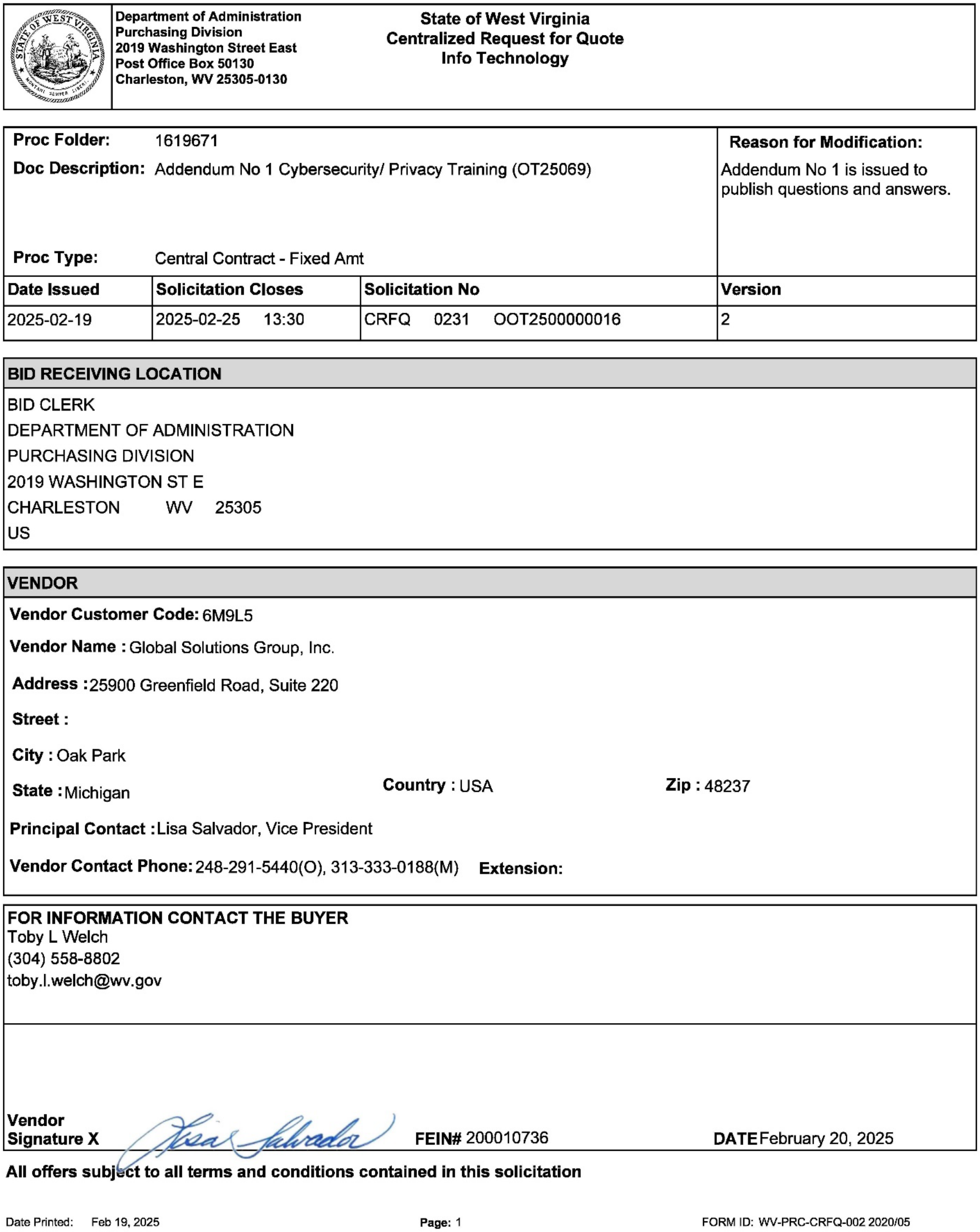


	Document Phase	Document Description	Page 4
OOT2500000016	Final	Cybersecurity/ Privacy Training (OT25069)	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

7.2 Addendum 1



Department of Administration Purchasing Division 2019 Washington Street East Post Office Box 50130 Charleston, WV 25305-0130	**State of West Virginia** **Centralized Request for Quote** **Info Technology**

Proc Folder:	1619671	**Reason for Modification:**
Doc Description:	Addendum No 1 Cybersecurity/ Privacy Training (OT25069)	Addendum No 1 is issued to publish questions and answers.
Proc Type:	Central Contract - Fixed Amt	

Date Issued	Solicitation Closes	Solicitation No	Version
2025-02-19	2025-02-25 13:30	CRFQ 0231 OOT2500000016	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 6M9L5

Vendor Name : Global Solutions Group, Inc.

Address : 25900 Greenfield Road, Suite 220

Street :

City : Oak Park

State : Michigan **Country :** USA **Zip :** 48237

Principal Contact : Lisa Salvador, Vice President

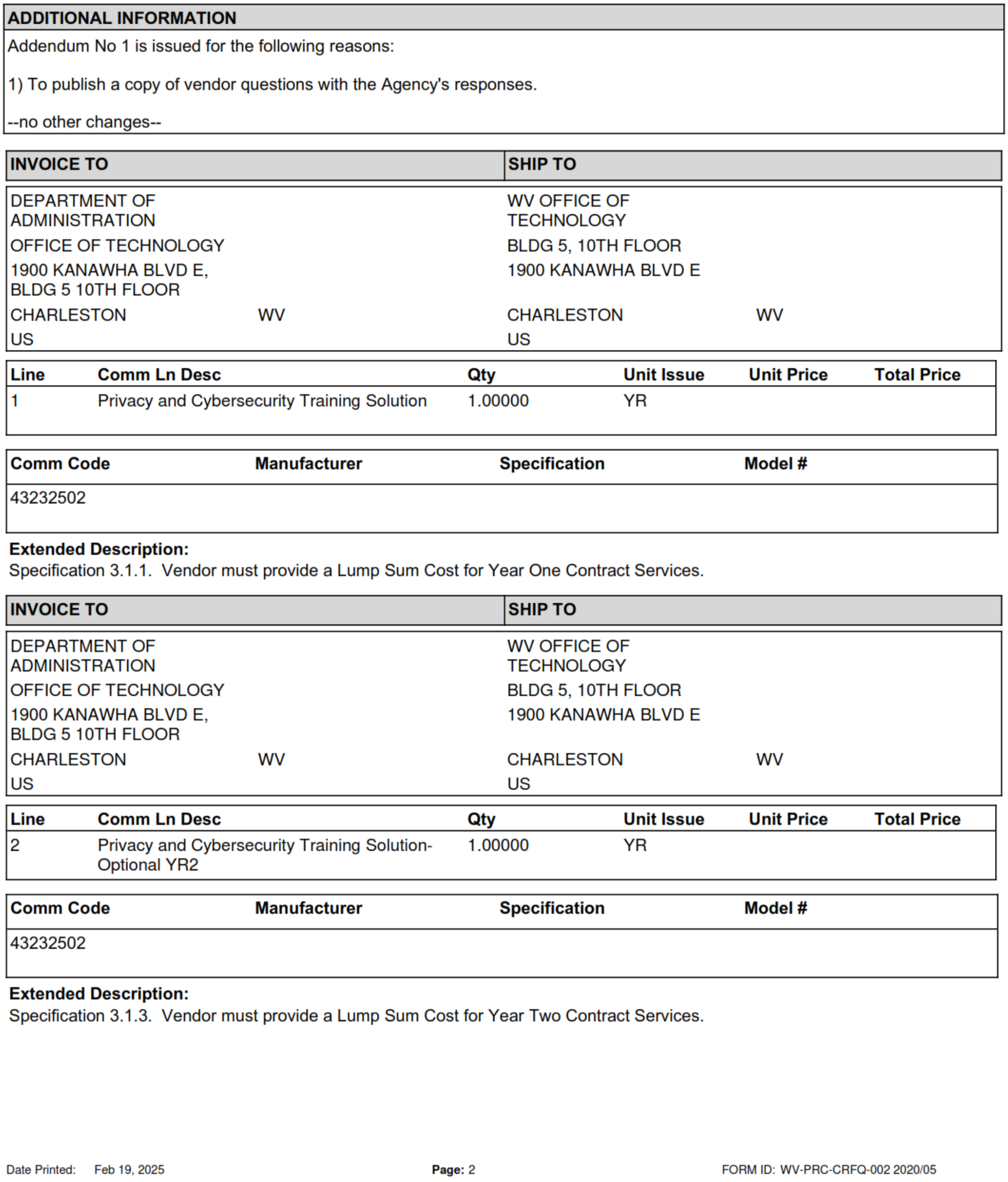
Vendor Contact Phone: 248-291-5440(O), 313-333-0188(M) **Extension:**

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X Lisa Salvador **FEIN#** 200010736 **DATE** February 20, 2025

All offers subject to all terms and conditions contained in this solicitation

Date Printed: Feb 19, 2025 **Page:** 1 FORM ID: WV-PRC-CRFQ-002 2020/05



ADDITIONAL INFORMATION
Addendum No 1 is issued for the following reasons: 1) To publish a copy of vendor questions with the Agency's responses. --no other changes--

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Privacy and Cybersecurity Training Solution	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

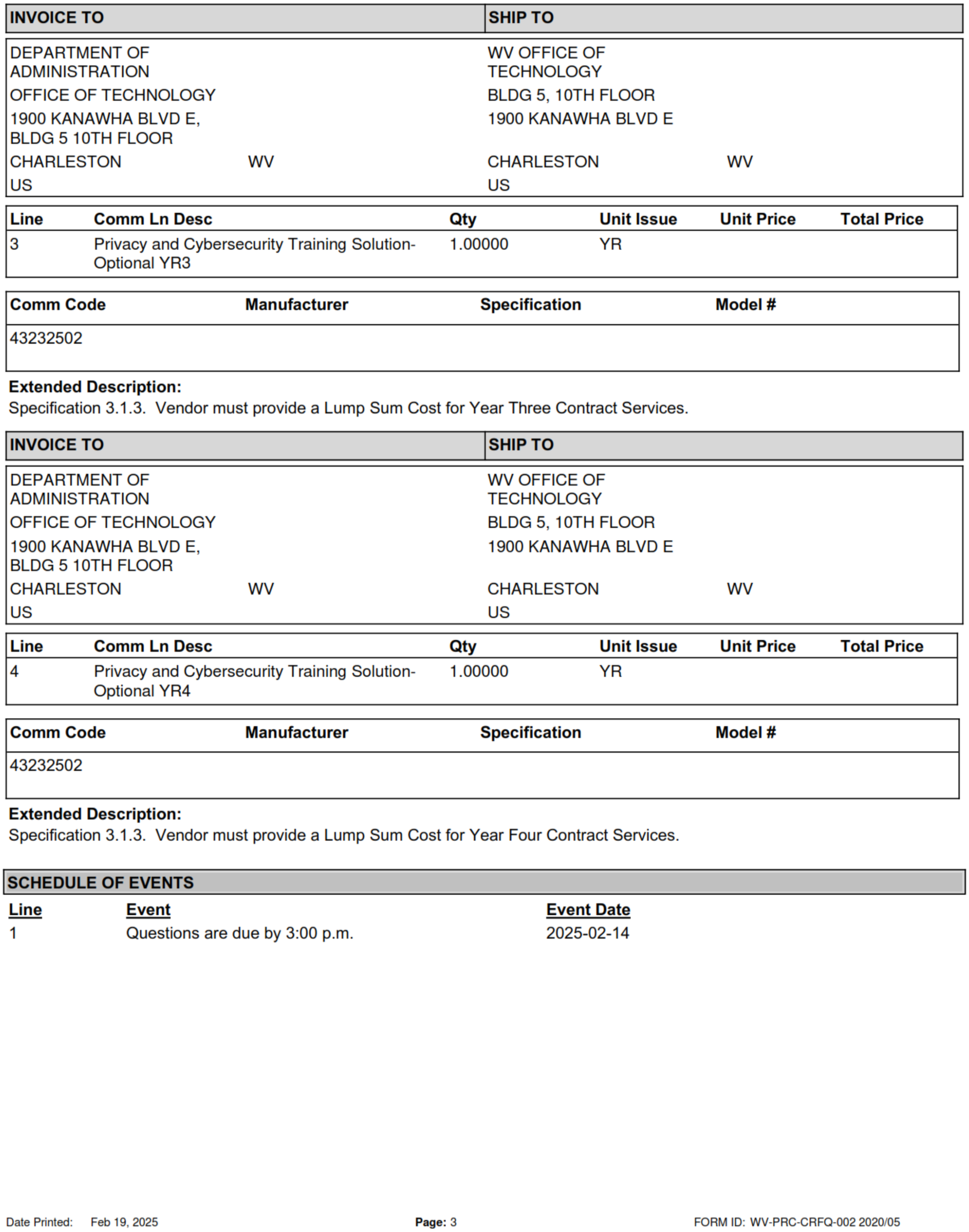
Extended Description:
Specification 3.1.1. Vendor must provide a Lump Sum Cost for Year One Contract Services.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Privacy and Cybersecurity Training Solution-Optional YR2	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Two Contract Services.



INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Privacy and Cybersecurity Training Solution-Optional YR3	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Three Contract Services.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

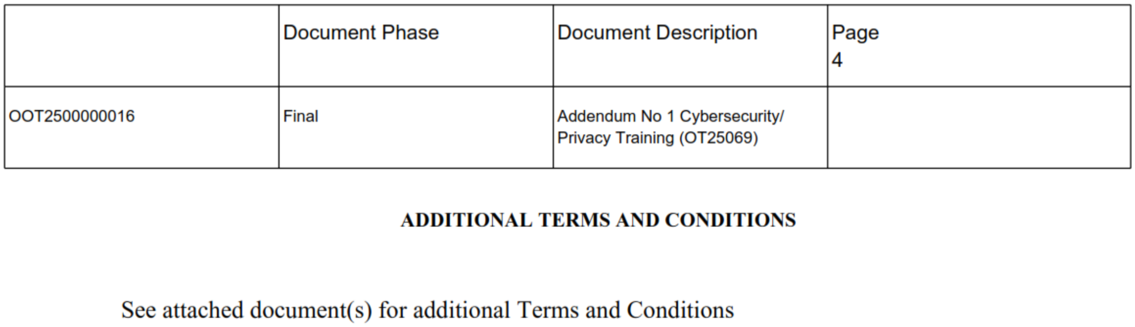
Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Privacy and Cybersecurity Training Solution-Optional YR4	1.00000	YR		

Comm Code	Manufacturer	Specification	Model #
43232502			

Extended Description:
Specification 3.1.3. Vendor must provide a Lump Sum Cost for Year Four Contract Services.

SCHEDULE OF EVENTS

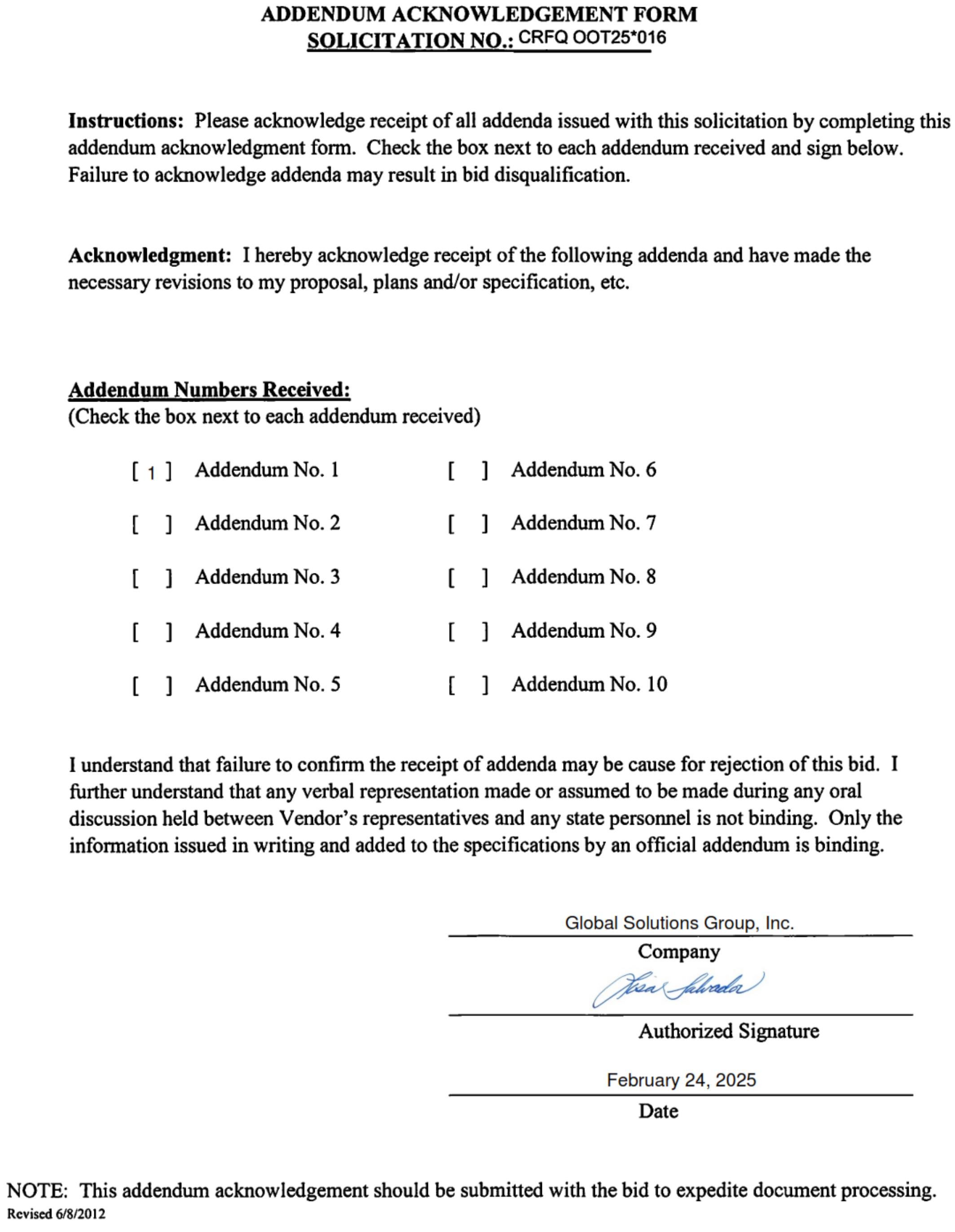
Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2025-02-14



	Document Phase	Document Description	Page 4
OOT2500000016	Final	Addendum No 1 Cybersecurity/ Privacy Training (OT25069)	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions



ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ OOT25*016

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:
(Check the box next to each addendum received)

[1] Addendum No. 1
[ ] Addendum No. 2
[ ] Addendum No. 3
[ ] Addendum No. 4
[ ] Addendum No. 5
[ ] Addendum No. 6
[ ] Addendum No. 7
[ ] Addendum No. 8
[ ] Addendum No. 9
[ ] Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

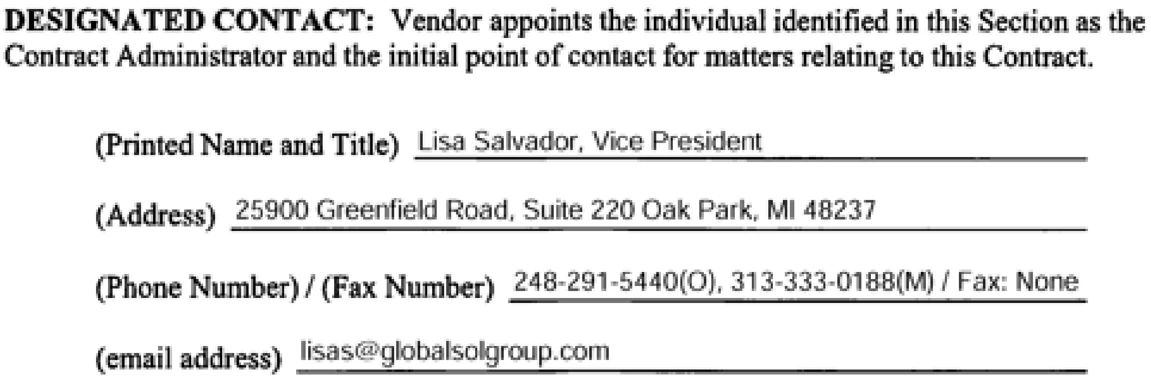
Global Solutions Group, Inc.
Company

Authorized Signature

February 24, 2025
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

7.3 Designated Contact



DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

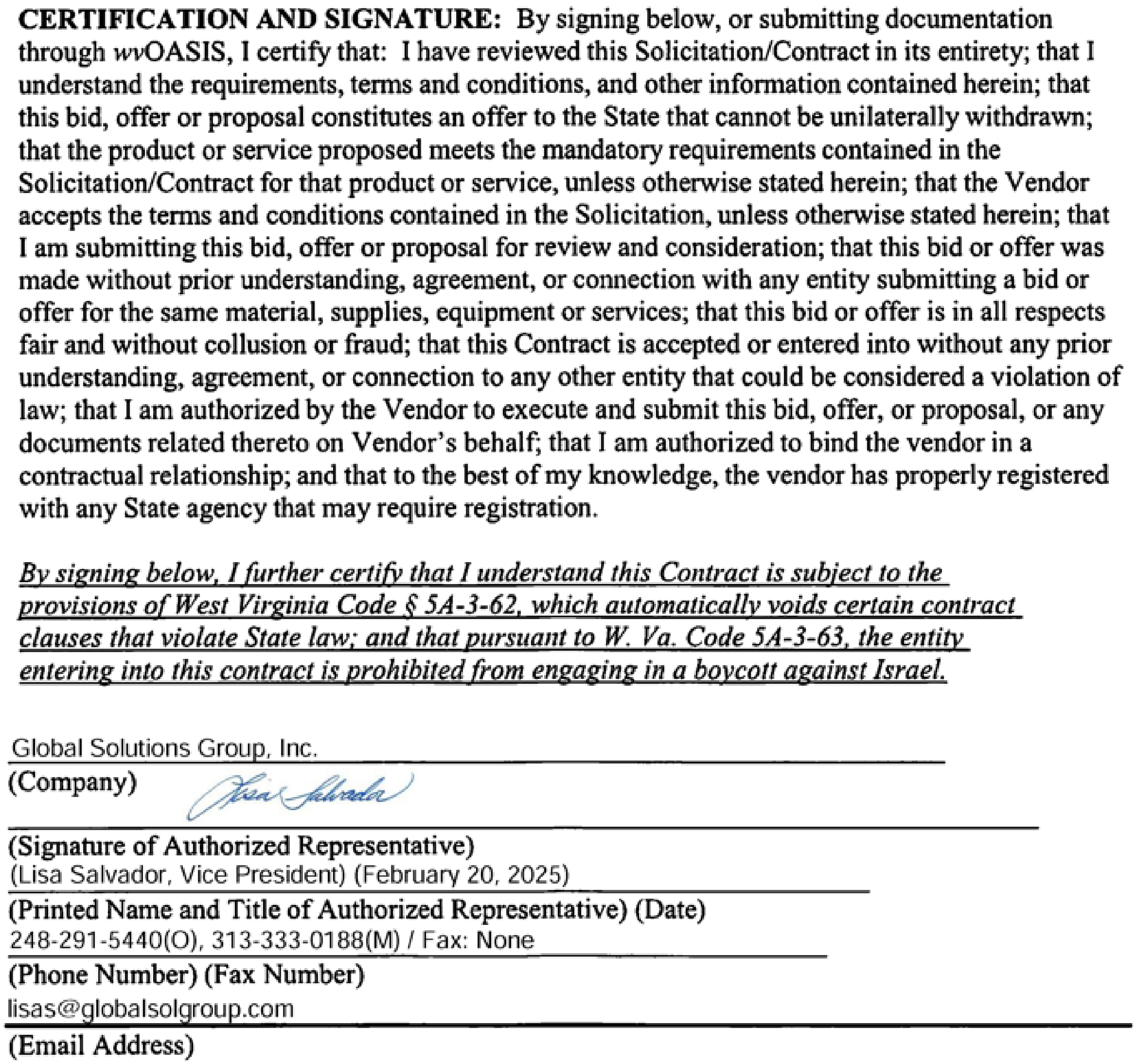
(Printed Name and Title) Lisa Salvador, Vice President

(Address) 25900 Greenfield Road, Suite 220 Oak Park, MI 48237

(Phone Number) / (Fax Number) 248-291-5440(O), 313-333-0188(M) / Fax: None

(email address) lisas@globalsolgroup.com

7.4 Certification and Signature



CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; that I am authorized by the Vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on Vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Global Solutions Group, Inc.
(Company)

Lisa Salvador
(Signature of Authorized Representative)

(Lisa Salvador, Vice President) (February 20, 2025)
(Printed Name and Title of Authorized Representative) (Date)

248-291-5440(O), 313-333-0188(M) / Fax: None
(Phone Number) (Fax Number)

lisas@globalsolgroup.com
(Email Address)

8. Performance Reviews

GSG has amassed a significant amount of "Exceptional" performance ratings and kudos from our customers. Section 8.1-8.4 are copies of the original documents.

Our continued stellar performance on contracts is recognized by customers and acknowledge our outstanding contract performance in the following written customer reviews.

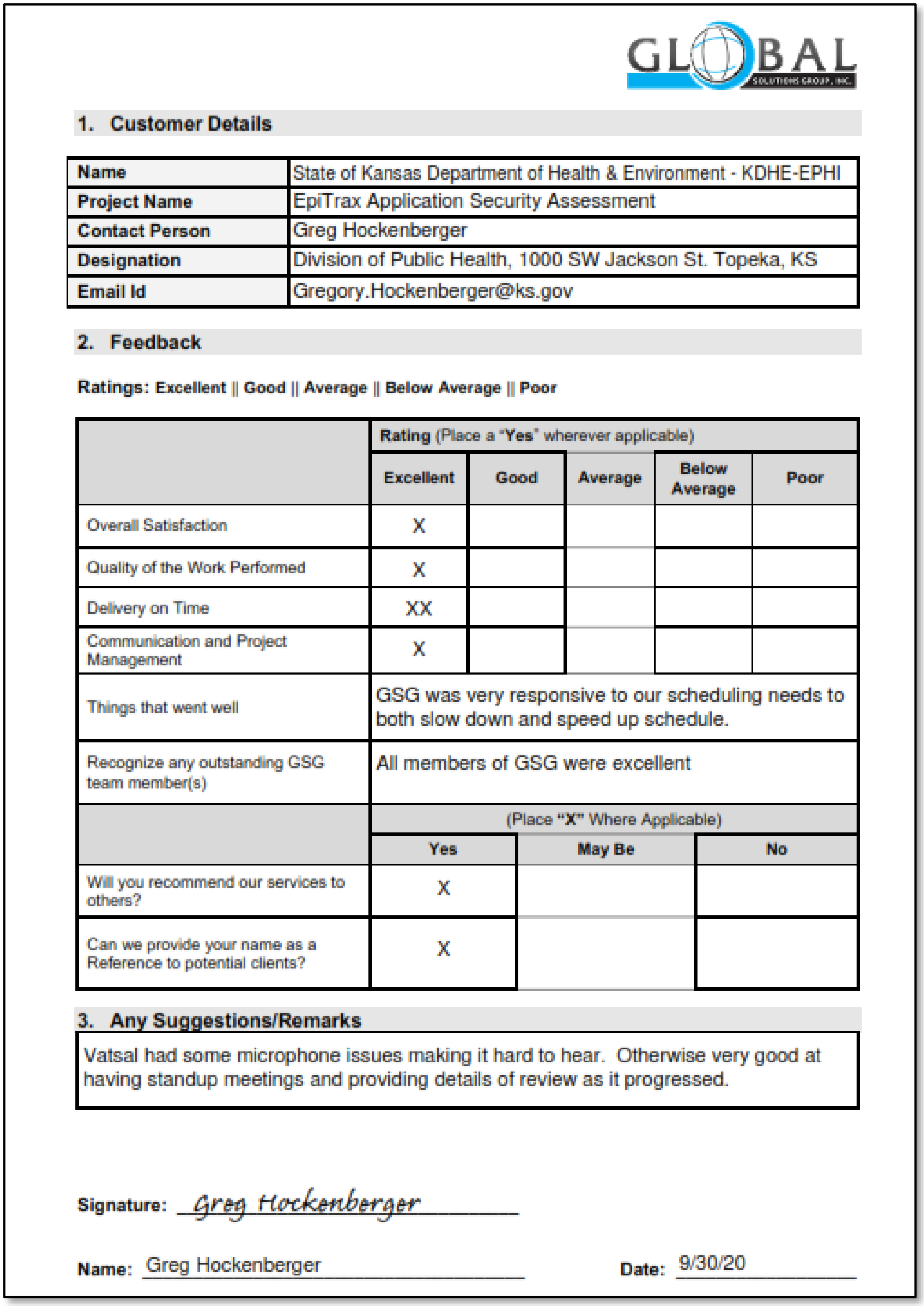
Below is a summary of cyber services performed for customers over the past five years with summaries on the subsequent pages.

State and Local Performance Assessments	State of Kansas Department of Health & Environment	**Excellent** in Overall Satisfaction, Work Performed, Delivery, Communication
	Fort Wayne–Allen County Airport Authority	**Excellent** in Overall Satisfaction, Work Performed, Delivery, Communication
	State of Kansas	**Excellent** Performance, first-class support
Past Performance Rating Form	U.S. Department of Interior	**Very Good** in Quality, Schedule, Cost Control and Management
Contract Performance Assessment Report System (CPARS)	2023 Security Assessment Support for Department of State x0872	**Very Good** in Quality, Schedule, Cost Control, and Management
	2023 Privacy and Information Security Services for AmeriCorps x0918	**Very Good** in Quality, Schedule, Cost Control, and Management
	Operational Security Assessments, Penetration Testing, and Web Security Assessments x0556	**Exceptional** Quality and Cost Control
	Operational Security Assessment, Penetration Testing, and Web Security Assessment x0604	**Exceptional** Quality
	Penetration Testing for USDA Agencies x0265	**Exceptional** Schedule and Quality
	Operational Security Assessment x0567	**Very Good** Quality
	Penetration Testing x0604	**Exceptional** Quality
	Albuquerque Service Center x0004	**Very Good** Quality, Schedule, Cost Control and Regulatory Compliance
Exit Surveys	Food and Nutrition Service, Information Security Center, Security Assessment Team, Penetration Testing	**Very Satisfied** (maximum rating) in all categories
	APHIS - Information Security Center – Animal and Plant Health Inspection Service	**Very Satisfied** (maximum rating) in all categories
	AMS - Exit Survey Questionnaire for Agriculture Marketing Services	**Very Satisfied** (maximum rating) in all categories

8.1 State and Local Performance Assessments

8.1.1 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

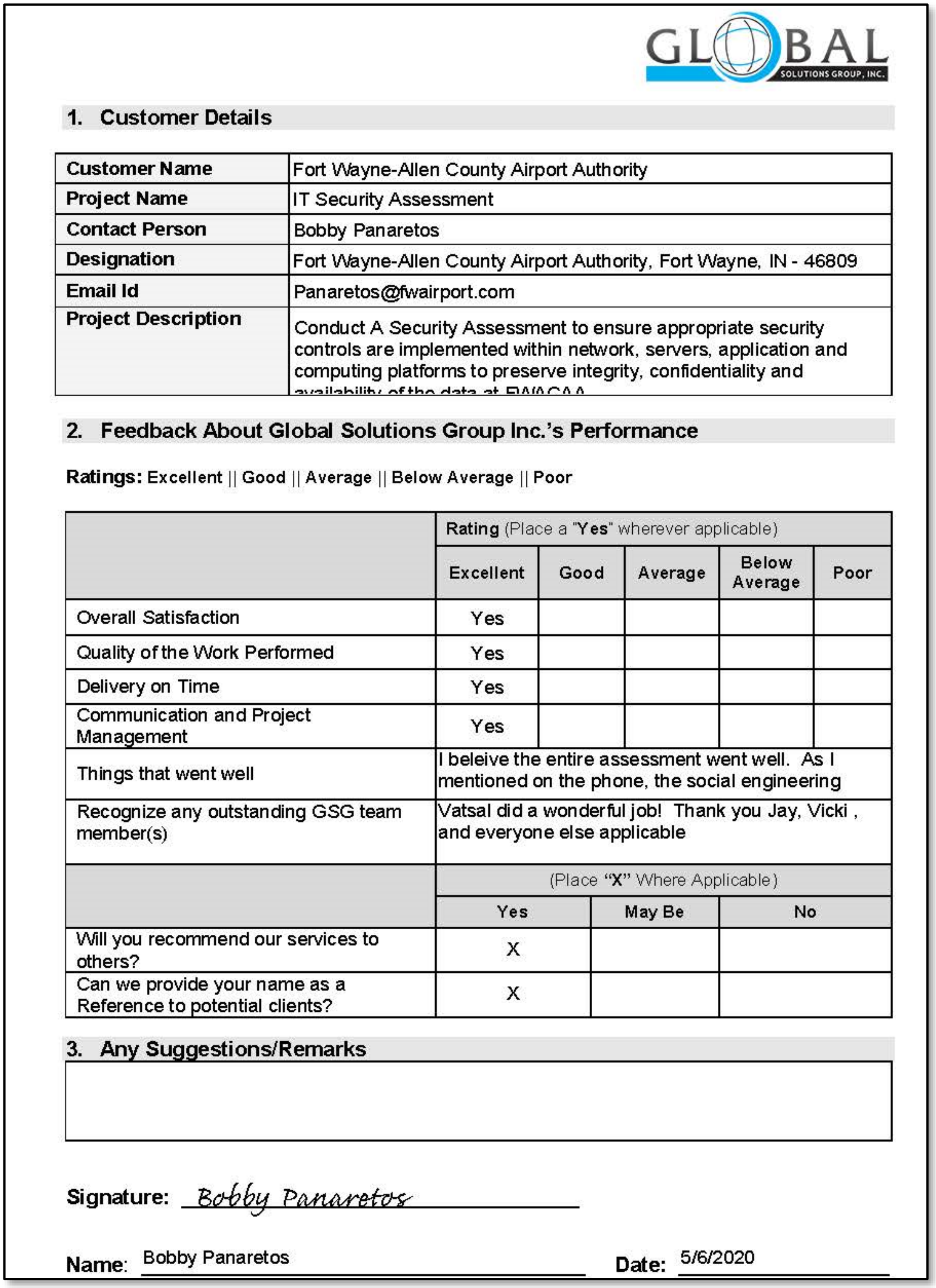
Vatsal had some microphone issues making it hard to hear. Otherwise very good at having standup meetings and providing details of review as it progressed.

Signature: Greg Hockenberger

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

8.1.2 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

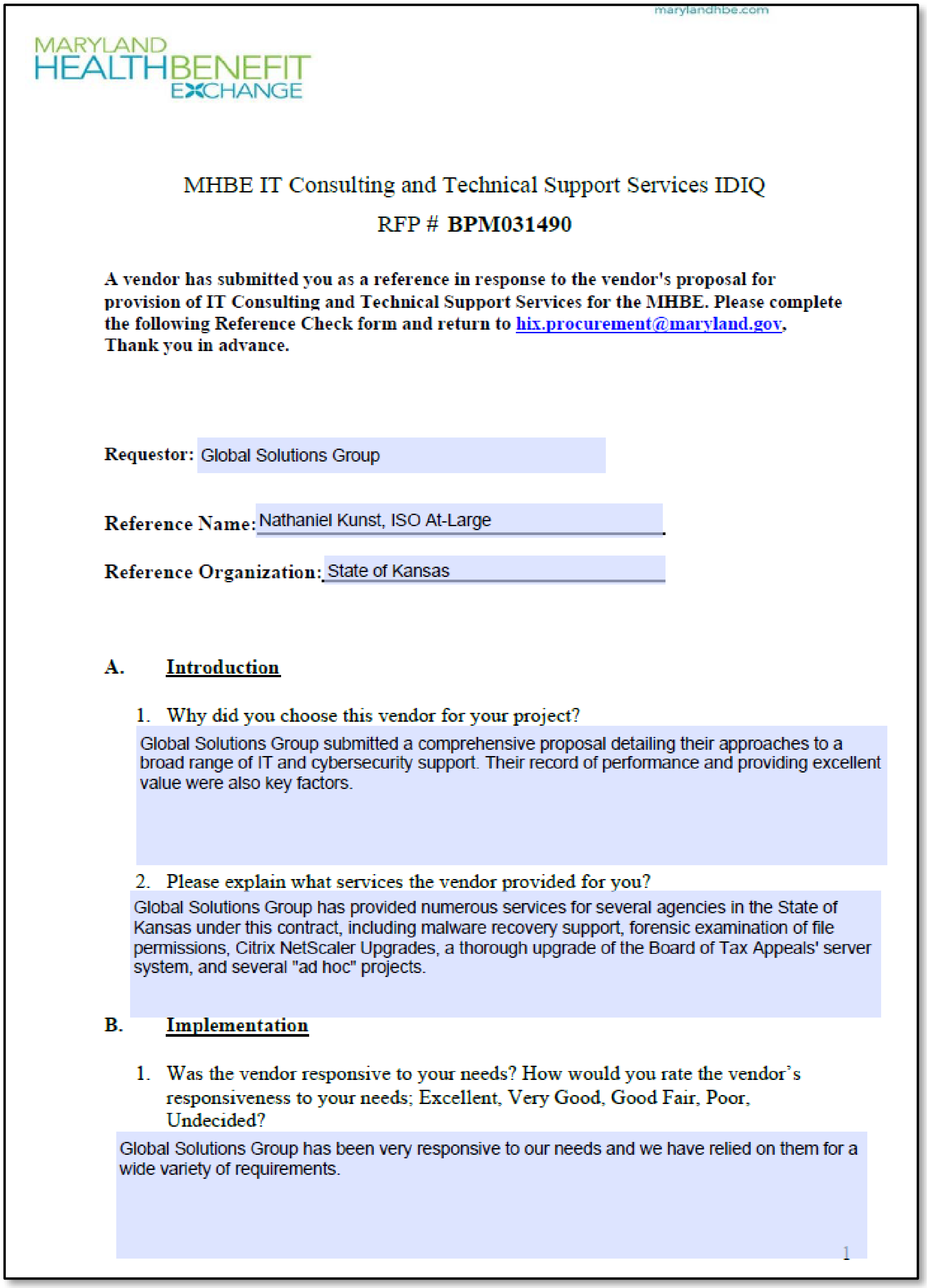
Signature: Bobby Panaretos

Name: Bobby Panaretos

Date: 5/6/2020

8.1.3 State of Kansas

Synopsis: Vendor Overall Performance Excellent, First-Class



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?

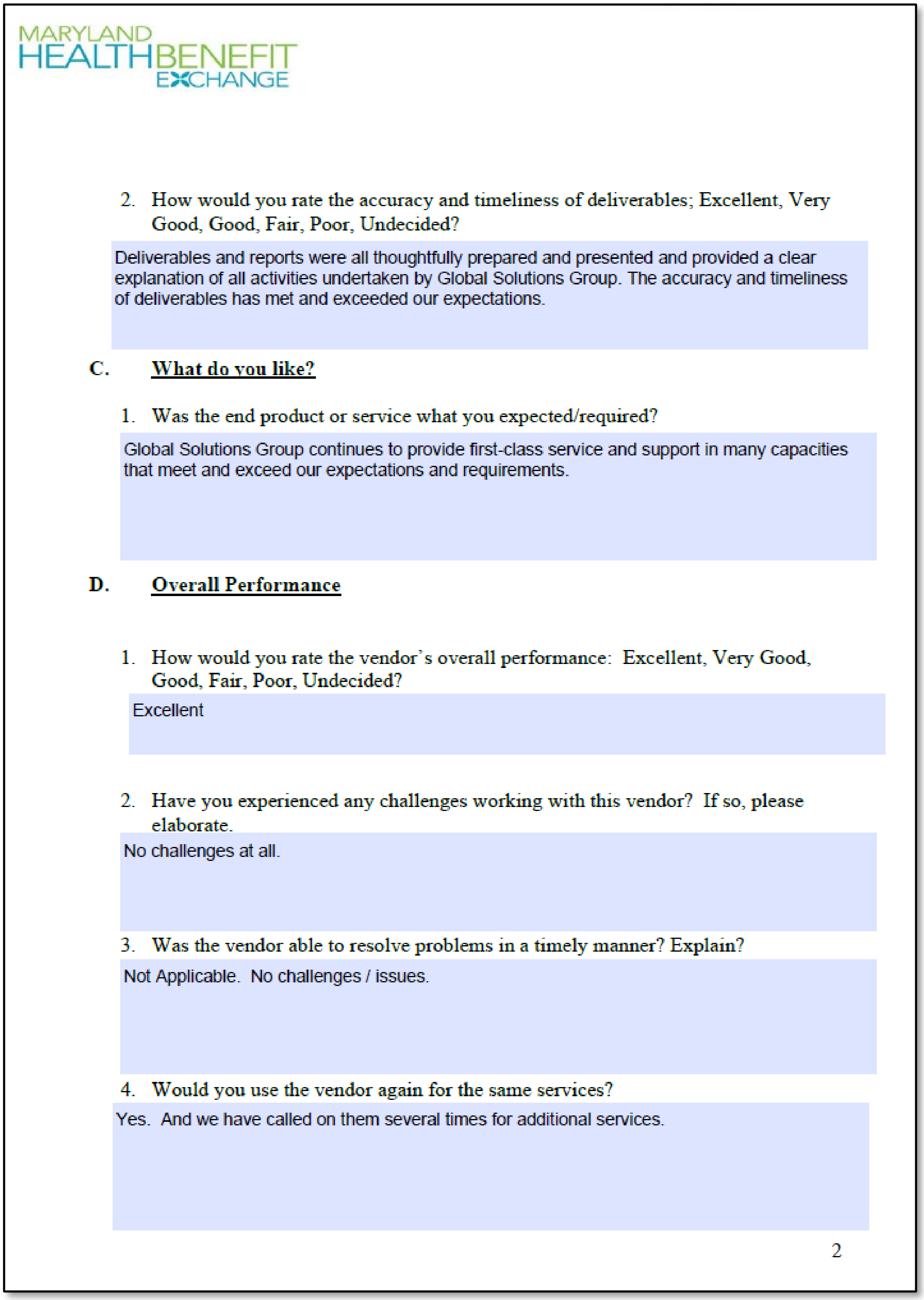
Global Solutions Group has provided numerous services for several agencies in the State of Kansas under this contract, including malware recovery support, forensic examination of file permissions, Citrix NetScaler Upgrades, a thorough upgrade of the Board of Tax Appeals' server system, and several "ad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

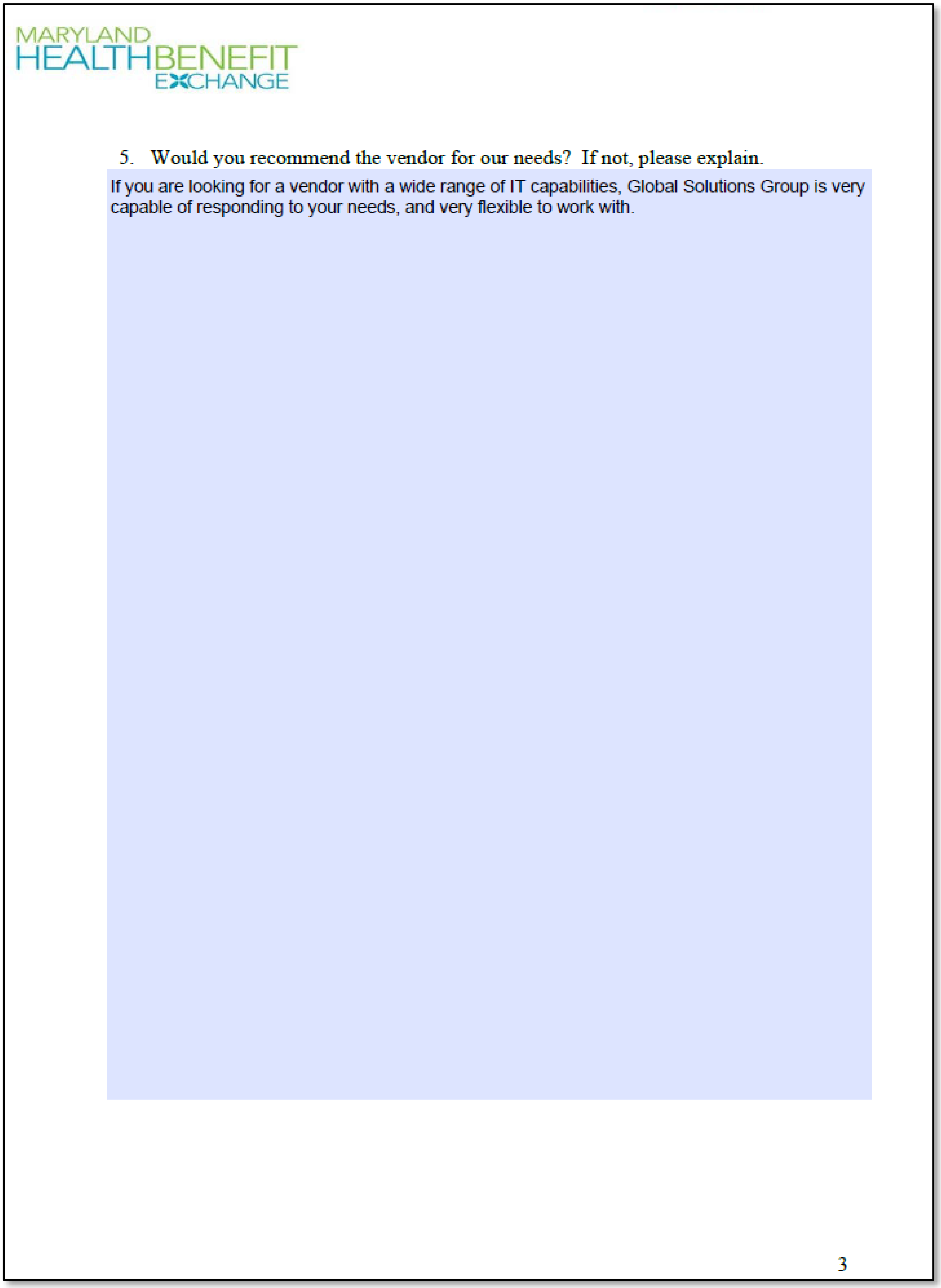
3. Was the vendor able to resolve problems in a timely manner? Explain?

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 HEALTHBENEFIT EXCHANGE

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

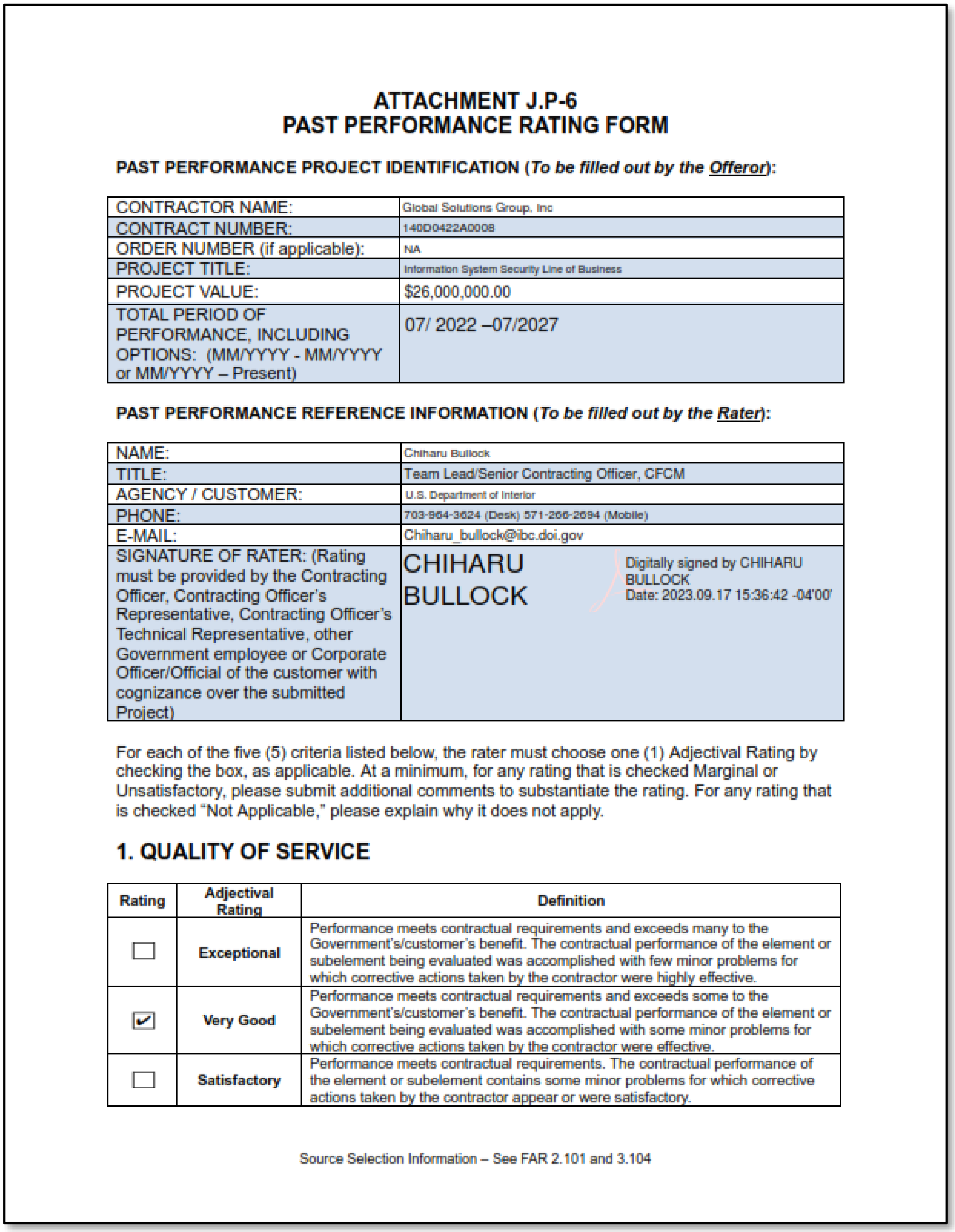
If you are looking for a vendor with a wide range of IT capabilities, Global Solutions Group is very capable of responding to your needs, and very flexible to work with.

8.2 Past Performance Rating Form

The following is past performance project identification.

8.2.1 U.S. Department of Interior

Synopsis: Quality, Schedule, Cost Control, and Management is Very Good



ATTACHMENT J.P-6
PAST PERFORMANCE RATING FORM

PAST PERFORMANCE PROJECT IDENTIFICATION (*To be filled out by the Offeror*):

CONTRACTOR NAME:	Global Solutions Group, Inc
CONTRACT NUMBER:	140D0422A0008
ORDER NUMBER (if applicable):	NA
PROJECT TITLE:	Information System Security Line of Business
PROJECT VALUE:	$26,000,000.00
TOTAL PERIOD OF PERFORMANCE, INCLUDING OPTIONS: (MM/YYYY - MM/YYYY or MM/YYYY – Present)	07/ 2022 –07/2027

PAST PERFORMANCE REFERENCE INFORMATION (*To be filled out by the Rater*):

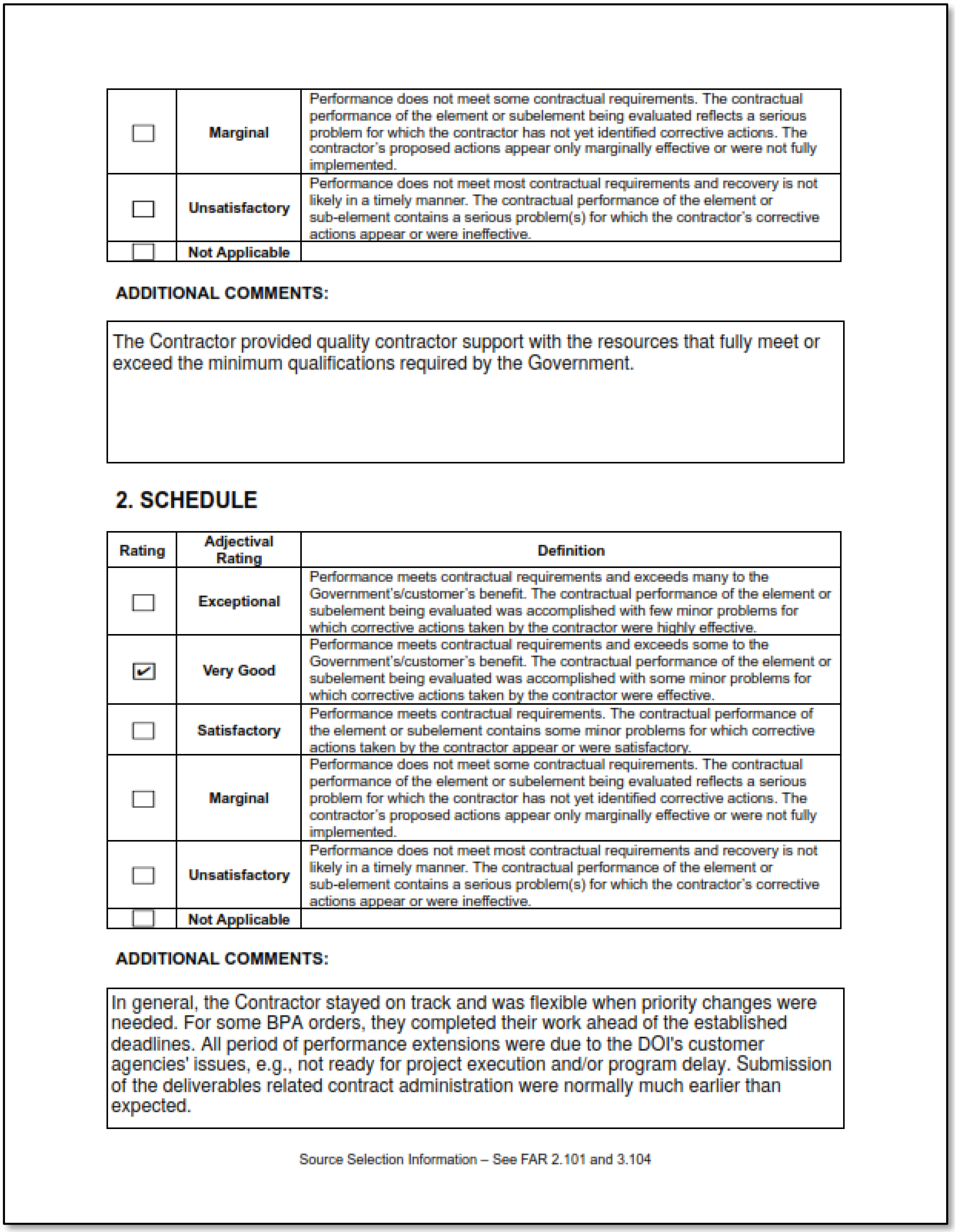
NAME:	Chiharu Bullock
TITLE:	Team Lead/Senior Contracting Officer, CFCM
AGENCY / CUSTOMER:	U.S. Department of Interior
PHONE:	703-964-3624 (Desk) 571-266-2694 (Mobile)
E-MAIL:	Chiharu_bullock@ibc.doi.gov
SIGNATURE OF RATER: (Rating must be provided by the Contracting Officer, Contracting Officer's Representative, Contracting Officer's Technical Representative, other Government employee or Corporate Officer/Official of the customer with cognizance over the submitted Project)	CHIHARU BULLOCK Digitally signed by CHIHARU BULLOCK Date: 2023.09.17 15:36:42 -04'00'

For each of the five (5) criteria listed below, the rater must choose one (1) Adjectival Rating by checking the box, as applicable. At a minimum, for any rating that is checked Marginal or Unsatisfactory, please submit additional comments to substantiate the rating. For any rating that is checked "Not Applicable," please explain why it does not apply.

1. QUALITY OF SERVICE

Rating	Adjectival Rating	Definition
□	**Exceptional**	Performance meets contractual requirements and exceeds many to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
☑	**Very Good**	Performance meets contractual requirements and exceeds some to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
□	**Satisfactory**	Performance meets contractual requirements. The contractual performance of the element or subelement contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.

Source Selection Information – See FAR 2.101 and 3.104



□	**Marginal**	Performance does not meet some contractual requirements. The contractual performance of the element or subelement being evaluated reflects a serious problem for which the contractor has not yet identified corrective actions. The contractor's proposed actions appear only marginally effective or were not fully implemented.
□	**Unsatisfactory**	Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains a serious problem(s) for which the contractor's corrective actions appear or were ineffective.
□	**Not Applicable**	

ADDITIONAL COMMENTS:

The Contractor provided quality contractor support with the resources that fully meet or exceed the minimum qualifications required by the Government.

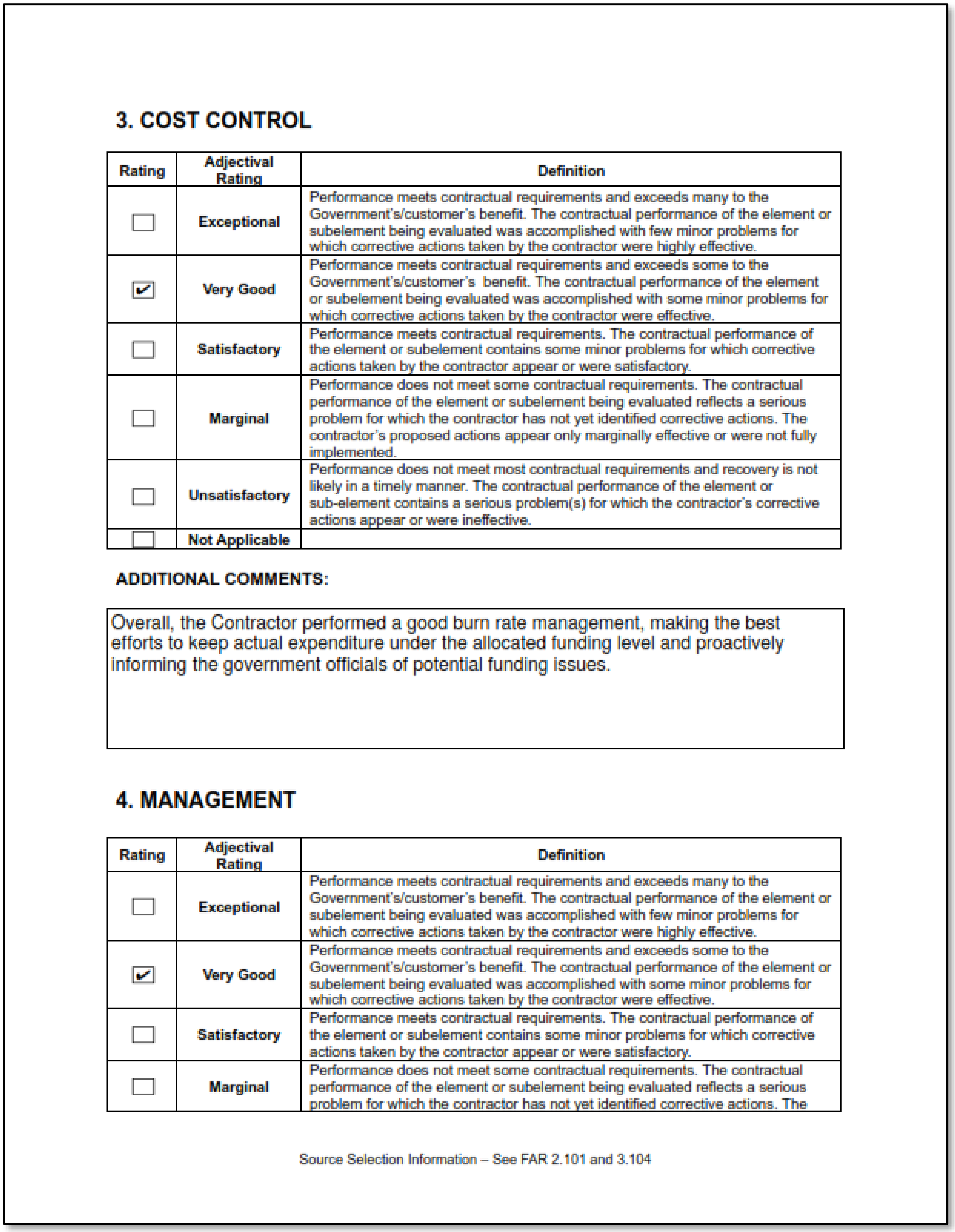
2. SCHEDULE

Rating	Adjectival Rating	Definition
□	**Exceptional**	Performance meets contractual requirements and exceeds many to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
☑	**Very Good**	Performance meets contractual requirements and exceeds some to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
□	**Satisfactory**	Performance meets contractual requirements. The contractual performance of the element or subelement contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.
□	**Marginal**	Performance does not meet some contractual requirements. The contractual performance of the element or subelement being evaluated reflects a serious problem for which the contractor has not yet identified corrective actions. The contractor's proposed actions appear only marginally effective or were not fully implemented.
□	**Unsatisfactory**	Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains a serious problem(s) for which the contractor's corrective actions appear or were ineffective.
□	**Not Applicable**	

ADDITIONAL COMMENTS:

In general, the Contractor stayed on track and was flexible when priority changes were needed. For some BPA orders, they completed their work ahead of the established deadlines. All period of performance extensions were due to the DOI's customer agencies' issues, e.g., not ready for project execution and/or program delay. Submission of the deliverables related contract administration were normally much earlier than expected.

Source Selection Information – See FAR 2.101 and 3.104



3. COST CONTROL

Rating	Adjectival Rating	Definition
□	Exceptional	Performance meets contractual requirements and exceeds many to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
☑	Very Good	Performance meets contractual requirements and exceeds some to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
□	Satisfactory	Performance meets contractual requirements. The contractual performance of the element or subelement contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.
□	Marginal	Performance does not meet some contractual requirements. The contractual performance of the element or subelement being evaluated reflects a serious problem for which the contractor has not yet identified corrective actions. The contractor's proposed actions appear only marginally effective or were not fully implemented.
□	Unsatisfactory	Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains a serious problem(s) for which the contractor's corrective actions appear or were ineffective.
□	Not Applicable	

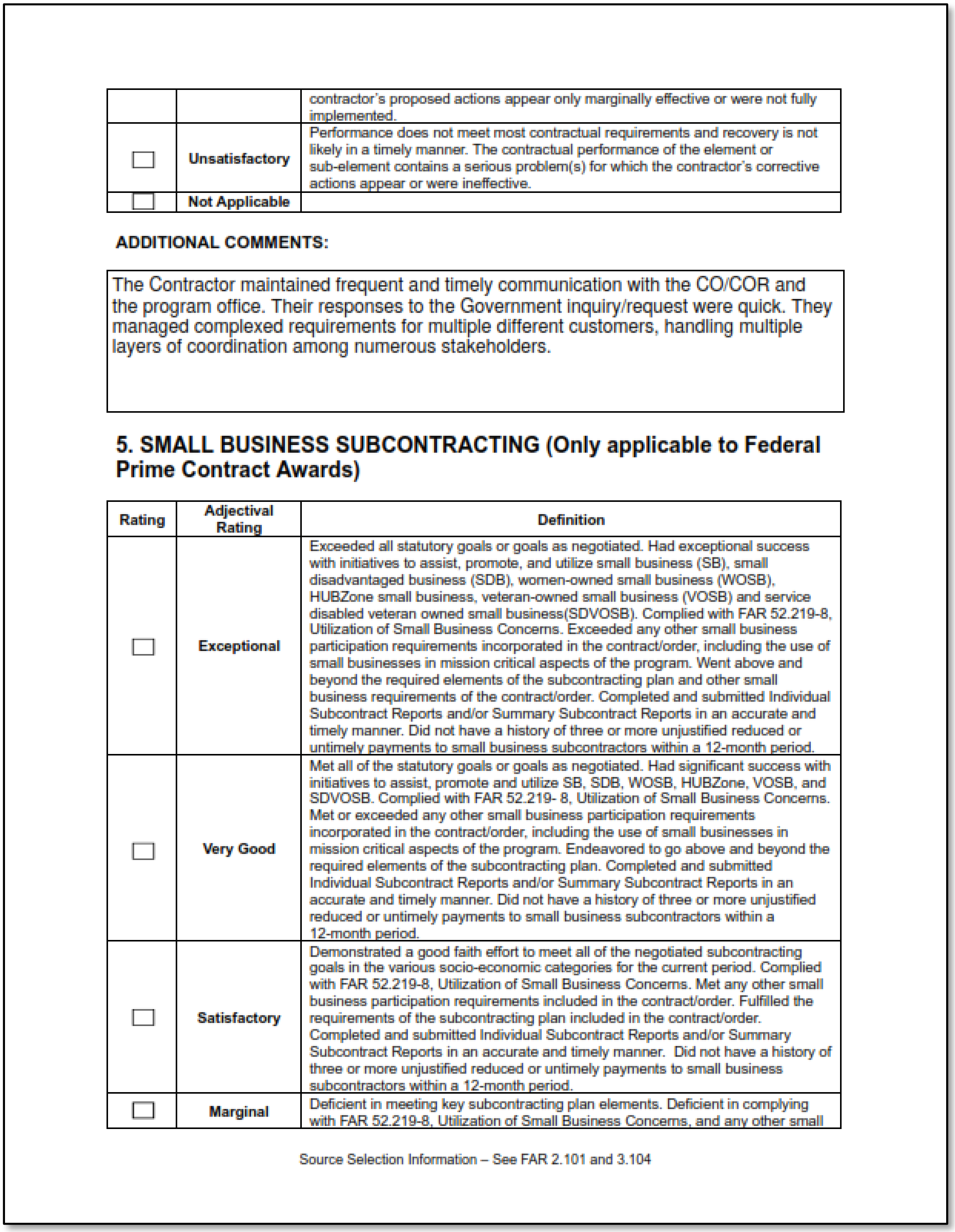
ADDITIONAL COMMENTS:

Overall, the Contractor performed a good burn rate management, making the best efforts to keep actual expenditure under the allocated funding level and proactively informing the government officials of potential funding issues.

4. MANAGEMENT

Rating	Adjectival Rating	Definition
□	Exceptional	Performance meets contractual requirements and exceeds many to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with few minor problems for which corrective actions taken by the contractor were highly effective.
☑	Very Good	Performance meets contractual requirements and exceeds some to the Government's/customer's benefit. The contractual performance of the element or subelement being evaluated was accomplished with some minor problems for which corrective actions taken by the contractor were effective.
□	Satisfactory	Performance meets contractual requirements. The contractual performance of the element or subelement contains some minor problems for which corrective actions taken by the contractor appear or were satisfactory.
□	Marginal	Performance does not meet some contractual requirements. The contractual performance of the element or subelement being evaluated reflects a serious problem for which the contractor has not yet identified corrective actions. The

Source Selection Information – See FAR 2.101 and 3.104



		contractor's proposed actions appear only marginally effective or were not fully implemented.
□	**Unsatisfactory**	Performance does not meet most contractual requirements and recovery is not likely in a timely manner. The contractual performance of the element or sub-element contains a serious problem(s) for which the contractor's corrective actions appear or were ineffective.
□	**Not Applicable**	

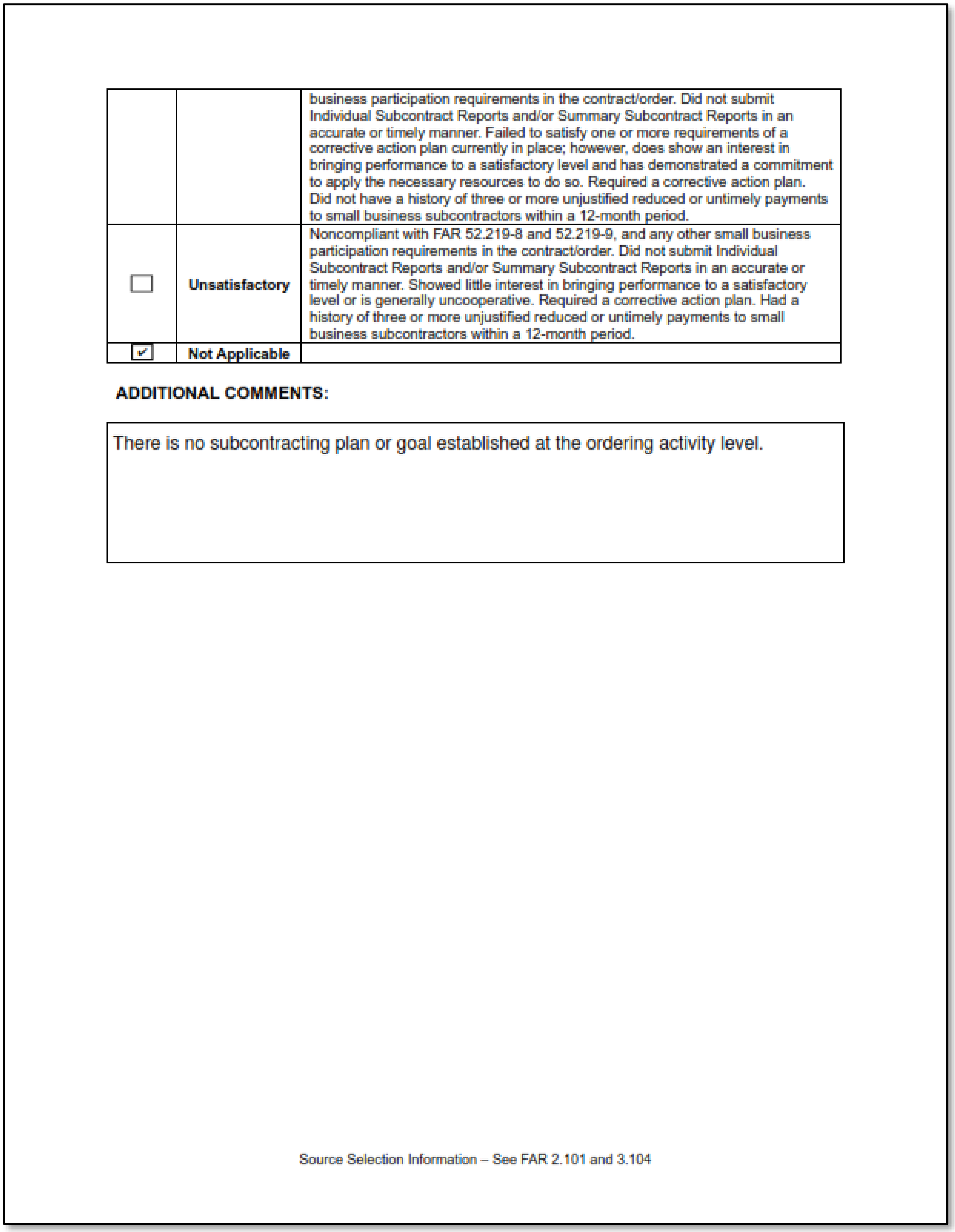
ADDITIONAL COMMENTS:

The Contractor maintained frequent and timely communication with the CO/COR and the program office. Their responses to the Government inquiry/request were quick. They managed complexed requirements for multiple different customers, handling multiple layers of coordination among numerous stakeholders.

5. SMALL BUSINESS SUBCONTRACTING (Only applicable to Federal Prime Contract Awards)

Rating	Adjectival Rating	Definition
□	**Exceptional**	Exceeded all statutory goals or goals as negotiated. Had exceptional success with initiatives to assist, promote, and utilize small business (SB), small disadvantaged business (SDB), women-owned small business (WOSB), HUBZone small business, veteran-owned small business (VOSB) and service disabled veteran owned small business(SDVOSB). Complied with FAR 52.219-8, Utilization of Small Business Concerns. Exceeded any other small business participation requirements incorporated in the contract/order, including the use of small businesses in mission critical aspects of the program. Went above and beyond the required elements of the subcontracting plan and other small business requirements of the contract/order. Completed and submitted Individual Subcontract Reports and/or Summary Subcontract Reports in an accurate and timely manner. Did not have a history of three or more unjustified reduced or untimely payments to small business subcontractors within a 12-month period.
□	**Very Good**	Met all of the statutory goals or goals as negotiated. Had significant success with initiatives to assist, promote and utilize SB, SDB, WOSB, HUBZone, VOSB, and SDVOSB. Complied with FAR 52.219- 8, Utilization of Small Business Concerns. Met or exceeded any other small business participation requirements incorporated in the contract/order, including the use of small businesses in mission critical aspects of the program. Endeavored to go above and beyond the required elements of the subcontracting plan. Completed and submitted Individual Subcontract Reports and/or Summary Subcontract Reports in an accurate and timely manner. Did not have a history of three or more unjustified reduced or untimely payments to small business subcontractors within a 12-month period.
□	**Satisfactory**	Demonstrated a good faith effort to meet all of the negotiated subcontracting goals in the various socio-economic categories for the current period. Complied with FAR 52.219-8, Utilization of Small Business Concerns. Met any other small business participation requirements included in the contract/order. Fulfilled the requirements of the subcontracting plan included in the contract/order. Completed and submitted Individual Subcontract Reports and/or Summary Subcontract Reports in an accurate and timely manner. Did not have a history of three or more unjustified reduced or untimely payments to small business subcontractors within a 12-month period.
□	**Marginal**	Deficient in meeting key subcontracting plan elements. Deficient in complying with FAR 52.219-8, Utilization of Small Business Concerns, and any other small

Source Selection Information – See FAR 2.101 and 3.104



		business participation requirements in the contract/order. Did not submit Individual Subcontract Reports and/or Summary Subcontract Reports in an accurate or timely manner. Failed to satisfy one or more requirements of a corrective action plan currently in place; however, does show an interest in bringing performance to a satisfactory level and has demonstrated a commitment to apply the necessary resources to do so. Required a corrective action plan. Did not have a history of three or more unjustified reduced or untimely payments to small business subcontractors within a 12-month period.
□	**Unsatisfactory**	Noncompliant with FAR 52.219-8 and 52.219-9, and any other small business participation requirements in the contract/order. Did not submit Individual Subcontract Reports and/or Summary Subcontract Reports in an accurate or timely manner. Showed little interest in bringing performance to a satisfactory level or is generally uncooperative. Required a corrective action plan. Had a history of three or more unjustified reduced or untimely payments to small business subcontractors within a 12-month period.
☑	**Not Applicable**	

ADDITIONAL COMMENTS:

There is no subcontracting plan or goal established at the ordering activity level.

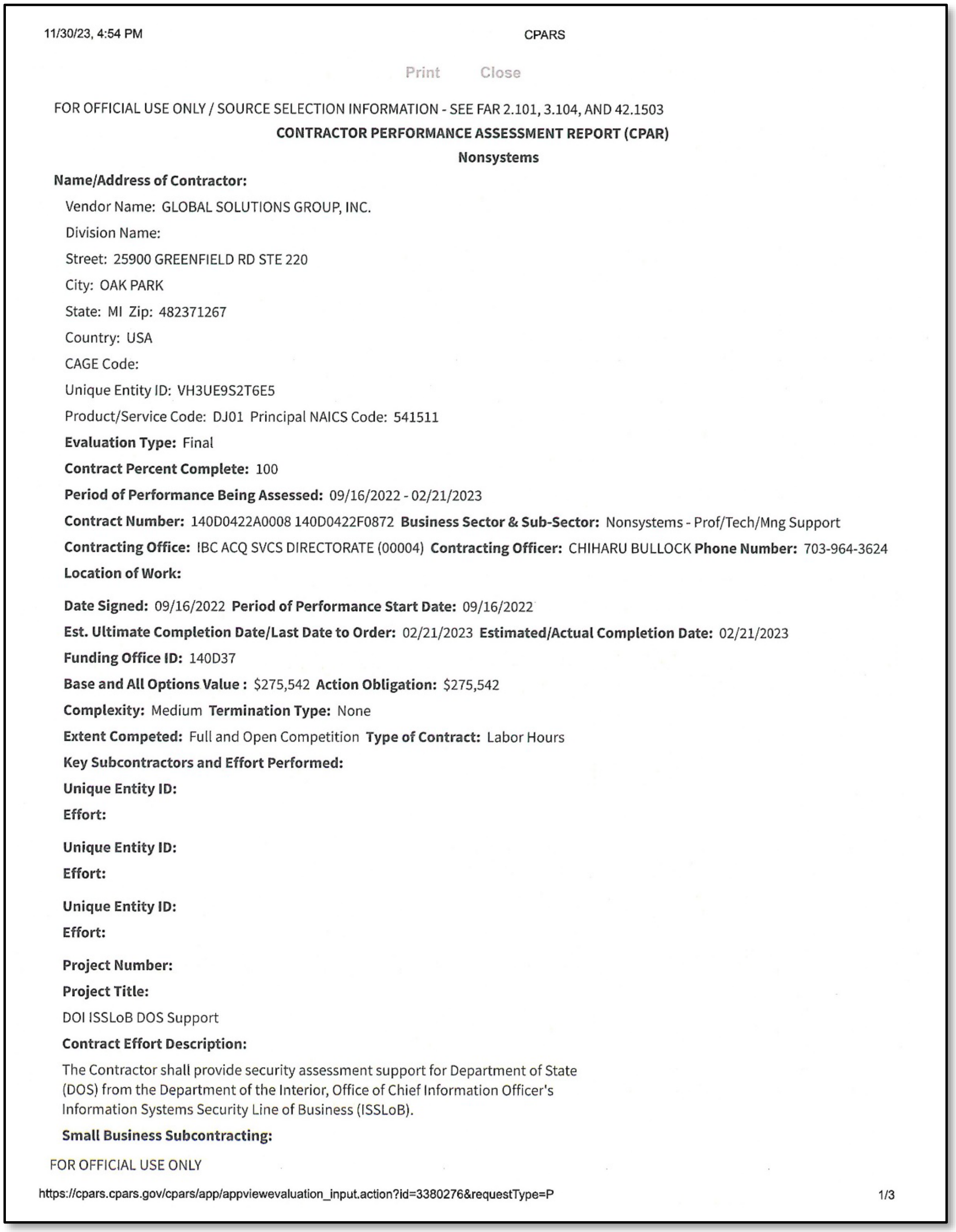
Source Selection Information – See FAR 2.101 and 3.104

8.3 Contract Performance Assessment Reporting System (CPARS)

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

8.3.1 2023 Security Assessment Support for Department of State (via the Department of the Interior ISSLoB Program)

Synopsis: Quality, Schedule, Cost Control, and Management is Very Good



11/30/23, 4:54 PM CPARS

Print Close

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

CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)

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: VH3UE9S2T6E5

Product/Service Code: DJ01 Principal NAICS Code: 541511

Evaluation Type: Final

Contract Percent Complete: 100

Period of Performance Being Assessed: 09/16/2022 - 02/21/2023

Contract Number: 140D0422A0008 140D0422F0872 **Business Sector & Sub-Sector:** Nonsystems - Prof/Tech/Mng Support

Contracting Office: IBC ACQ SVCS DIRECTORATE (00004) **Contracting Officer:** CHIHARU BULLOCK **Phone Number:** 703-964-3624

Location of Work:

Date Signed: 09/16/2022 **Period of Performance Start Date:** 09/16/2022

Est. Ultimate Completion Date/Last Date to Order: 02/21/2023 **Estimated/Actual Completion Date:** 02/21/2023

Funding Office ID: 140D37

Base and All Options Value : $275,542 **Action Obligation:** $275,542

Complexity: Medium **Termination Type:** None

Extent Competed: Full and Open Competition **Type of Contract:** Labor Hours

Key Subcontractors and Effort Performed:

Unique Entity ID:

Effort:

Unique Entity ID:

Effort:

Unique Entity ID:

Effort:

Project Number:

Project Title:

DOI ISSLoB DOS Support

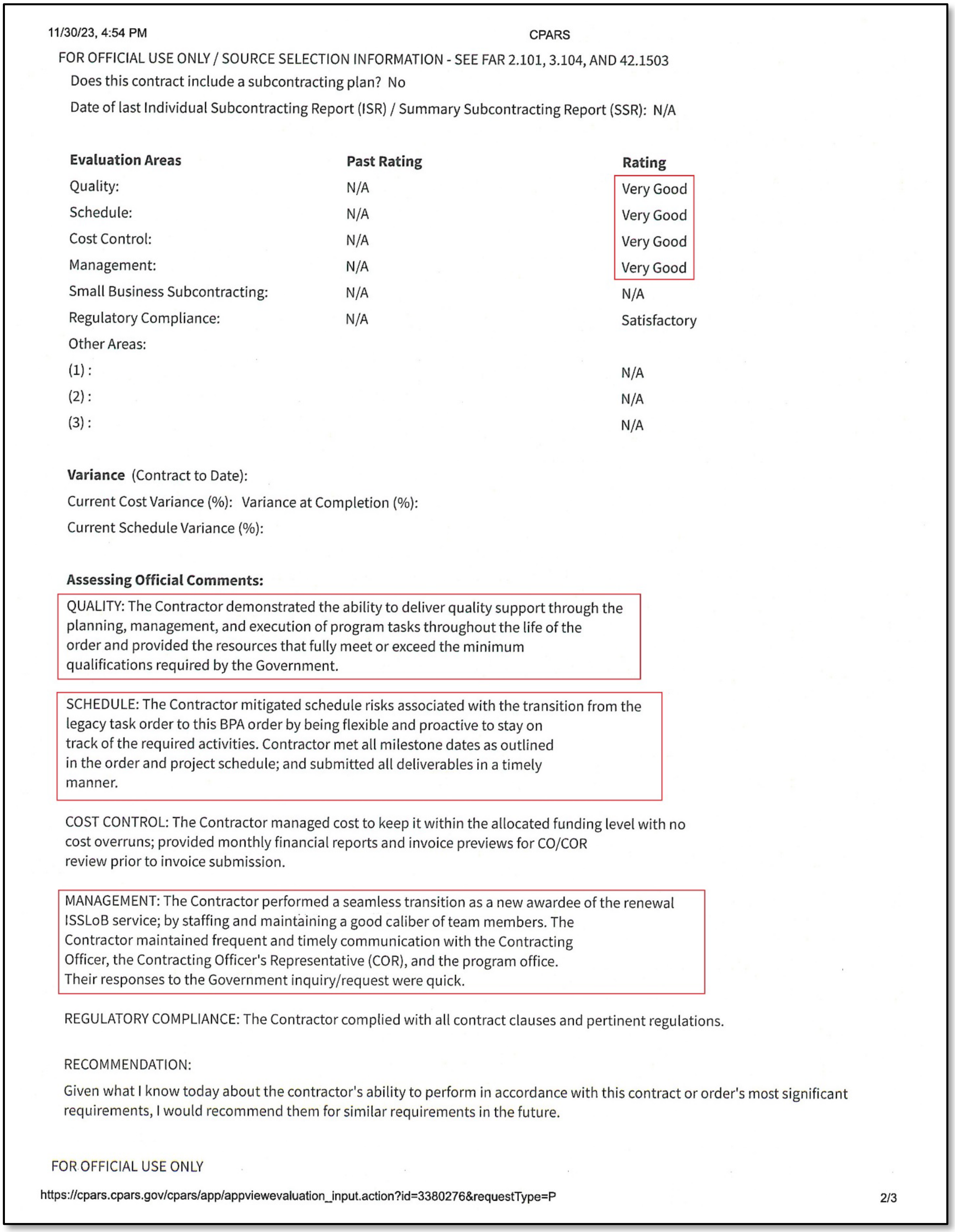
Contract Effort Description:

The Contractor shall provide security assessment support for Department of State (DOS) from the Department of the Interior, Office of Chief Information Officer's Information Systems Security Line of Business (ISSLoB).

Small Business Subcontracting:

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=3380276&requestType=P 1/3



11/30/23, 4:54 PM CPARS

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

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:	N/A	Very Good
Schedule:	N/A	Very Good
Cost Control:	N/A	Very Good
Management:	N/A	Very Good
Small Business Subcontracting:	N/A	N/A
Regulatory Compliance:	N/A	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: The Contractor demonstrated the ability to deliver quality support through the planning, management, and execution of program tasks throughout the life of the order and provided the resources that fully meet or exceed the minimum qualifications required by the Government.

SCHEDULE: The Contractor mitigated schedule risks associated with the transition from the legacy task order to this BPA order by being flexible and proactive to stay on track of the required activities. Contractor met all milestone dates as outlined in the order and project schedule; and submitted all deliverables in a timely manner.

COST CONTROL: The Contractor managed cost to keep it within the allocated funding level with no cost overruns; provided monthly financial reports and invoice previews for CO/COR review prior to invoice submission.

MANAGEMENT: The Contractor performed a seamless transition as a new awardee of the renewal ISSLoB service; by staffing and maintaining a good caliber of team members. The Contractor maintained frequent and timely communication with the Contracting Officer, the Contracting Officer's Representative (COR), and the program office. Their responses to the Government inquiry/request were quick.

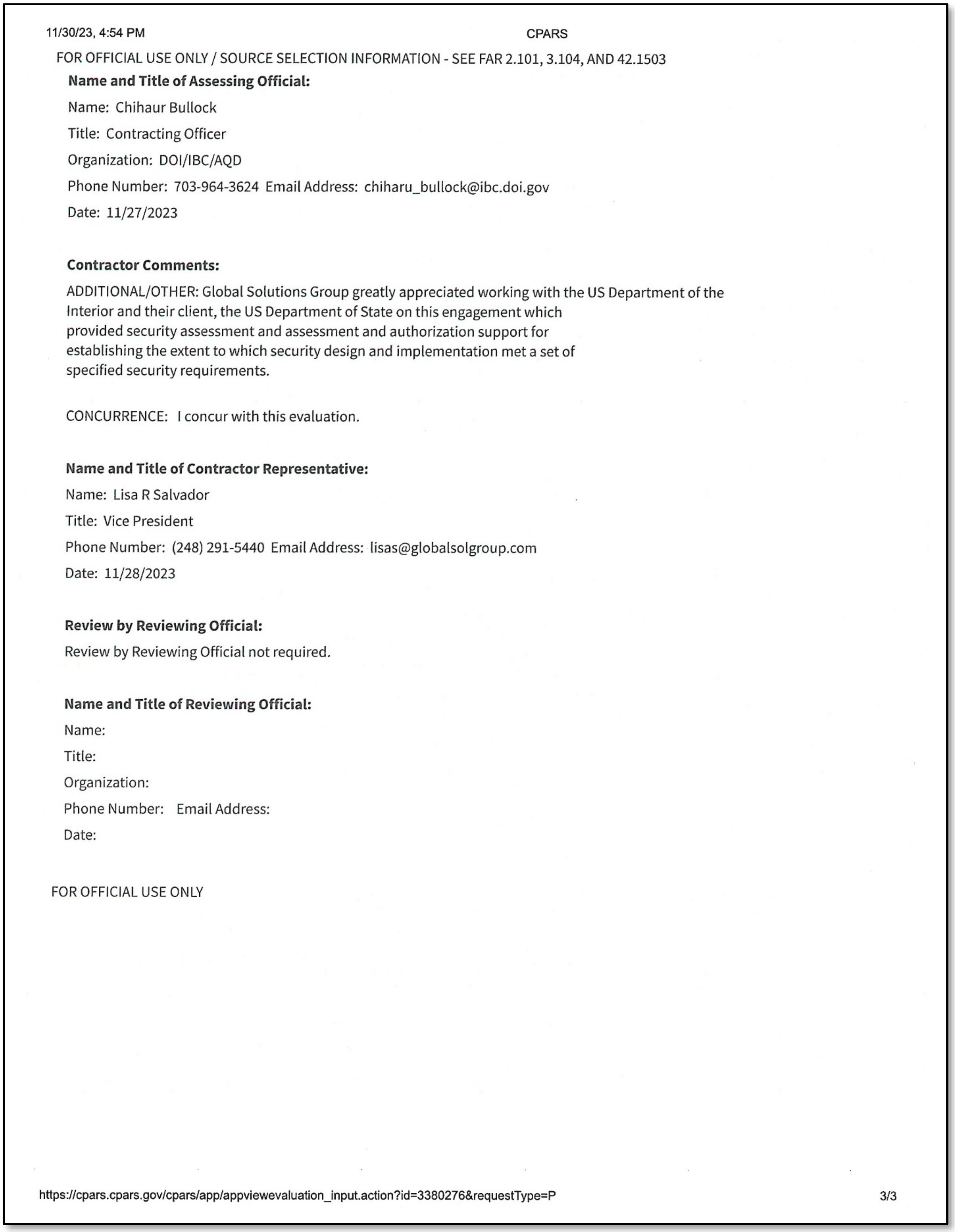
REGULATORY COMPLIANCE: The Contractor complied with all contract clauses and pertinent regulations.

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.

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=3380276&requestType=P 2/3



11/30/23, 4:54 PM CPARS

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

Name and Title of Assessing Official:

Name: Chihaur Bullock

Title: Contracting Officer

Organization: DOI/IBC/AQD

Phone Number: 703-964-3624 Email Address: chiharu_bullock@ibc.doi.gov

Date: 11/27/2023

Contractor Comments:

ADDITIONAL/OTHER: Global Solutions Group greatly appreciated working with the US Department of the Interior and their client, the US Department of State on this engagement which provided security assessment and assessment and authorization support for establishing the extent to which security design and implementation met a set of specified security requirements.

CONCURRENCE: I concur with this evaluation.

Name and Title of Contractor Representative:

Name: Lisa R Salvador

Title: Vice President

Phone Number: (248) 291-5440 Email Address: lisas@globalsolgroup.com

Date: 11/28/2023

Review by Reviewing Official:

Review by Reviewing Official not required.

Name and Title of Reviewing Official:

Name:

Title:

Organization:

Phone Number: Email Address:

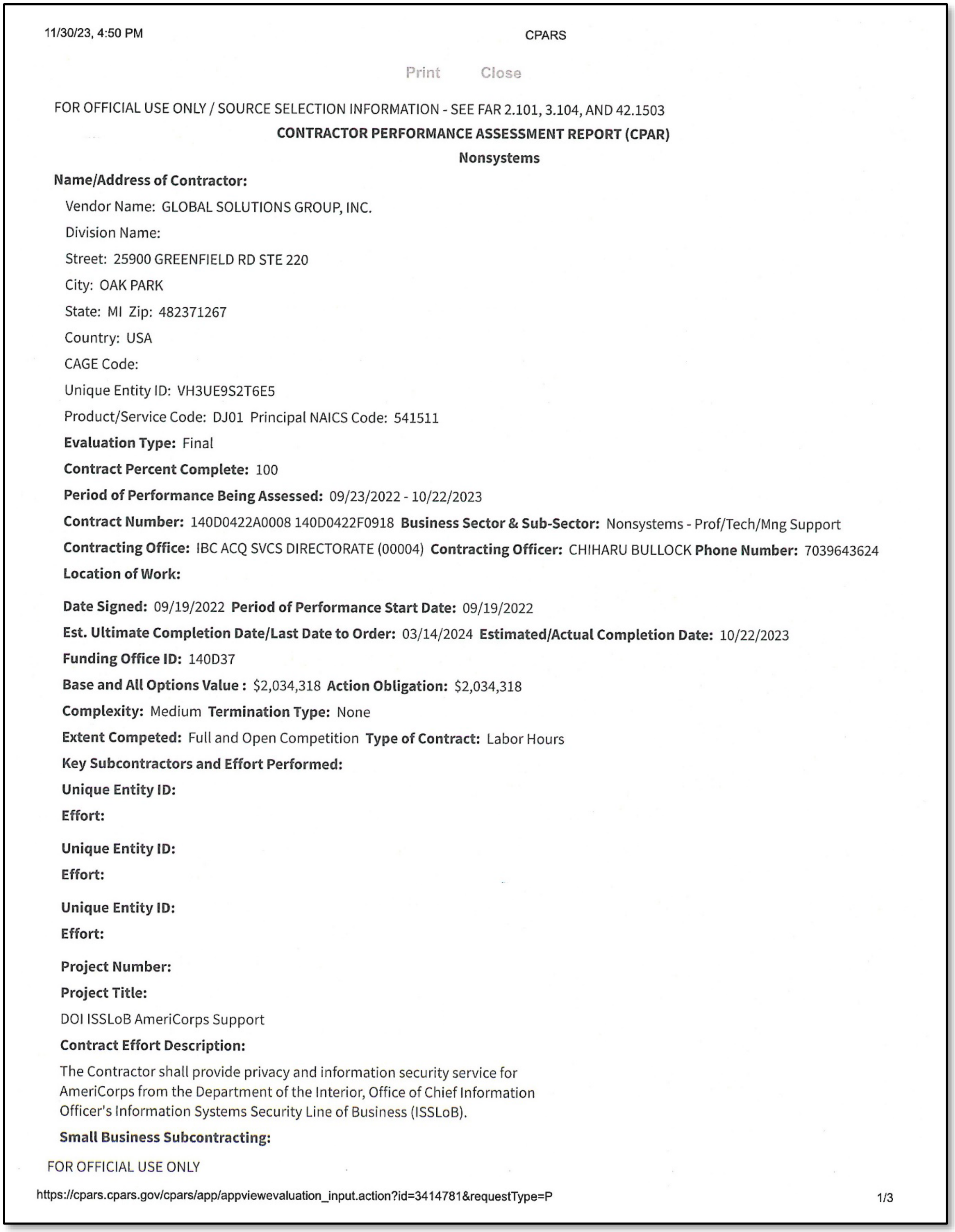
Date:

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=3380276&requestType=P 3/3

8.3.2 2023 Privacy and Information Security Services for AmeriCorps (via the Department of the Interior ISSLoB Program)

Synopsis: Quality, Schedule, Cost Control, and Management is Very Good



11/30/23, 4:50 PM CPARS

Print Close

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

CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)

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: VH3UE9S2T6E5
Product/Service Code: DJ01 Principal NAICS Code: 541511

Evaluation Type: Final

Contract Percent Complete: 100

Period of Performance Being Assessed: 09/23/2022 - 10/22/2023

Contract Number: 140D0422A0008 140D0422F0918 **Business Sector & Sub-Sector:** Nonsystems - Prof/Tech/Mng Support

Contracting Office: IBC ACQ SVCS DIRECTORATE (00004) **Contracting Officer:** CHIHARU BULLOCK **Phone Number:** 7039643624

Location of Work:

Date Signed: 09/19/2022 **Period of Performance Start Date:** 09/19/2022

Est. Ultimate Completion Date/Last Date to Order: 03/14/2024 **Estimated/Actual Completion Date:** 10/22/2023

Funding Office ID: 140D37

Base and All Options Value : $2,034,318 **Action Obligation:** $2,034,318

Complexity: Medium **Termination Type:** None

Extent Competed: Full and Open Competition **Type of Contract:** Labor Hours

Key Subcontractors and Effort Performed:

Unique Entity ID:

Effort:

Unique Entity ID:

Effort:

Unique Entity ID:

Effort:

Project Number:

Project Title:

DOI ISSLoB AmeriCorps Support

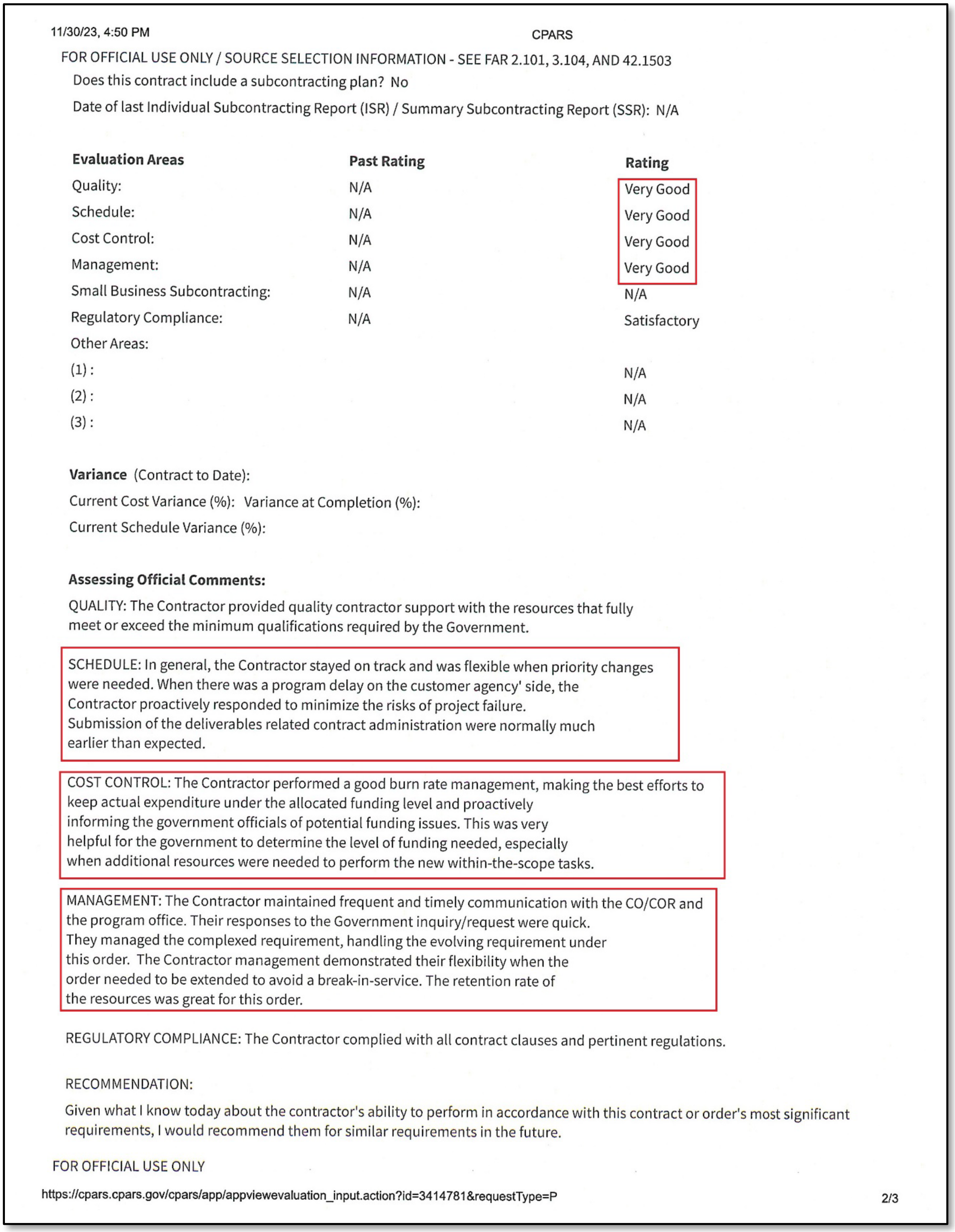
Contract Effort Description:

The Contractor shall provide privacy and information security service for AmeriCorps from the Department of the Interior, Office of Chief Information Officer's Information Systems Security Line of Business (ISSLoB).

Small Business Subcontracting:

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=3414781&requestType=P 1/3



11/30/23, 4:50 PM CPARS

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

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:	N/A	Very Good
Schedule:	N/A	Very Good
Cost Control:	N/A	Very Good
Management:	N/A	Very Good
Small Business Subcontracting:	N/A	N/A
Regulatory Compliance:	N/A	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: The Contractor provided quality contractor support with the resources that fully meet or exceed the minimum qualifications required by the Government.

SCHEDULE: In general, the Contractor stayed on track and was flexible when priority changes were needed. When there was a program delay on the customer agency' side, the Contractor proactively responded to minimize the risks of project failure. Submission of the deliverables related contract administration were normally much earlier than expected.

COST CONTROL: The Contractor performed a good burn rate management, making the best efforts to keep actual expenditure under the allocated funding level and proactively informing the government officials of potential funding issues. This was very helpful for the government to determine the level of funding needed, especially when additional resources were needed to perform the new within-the-scope tasks.

MANAGEMENT: The Contractor maintained frequent and timely communication with the CO/COR and the program office. Their responses to the Government inquiry/request were quick. They managed the complexed requirement, handling the evolving requirement under this order. The Contractor management demonstrated their flexibility when the order needed to be extended to avoid a break-in-service. The retention rate of the resources was great for this order.

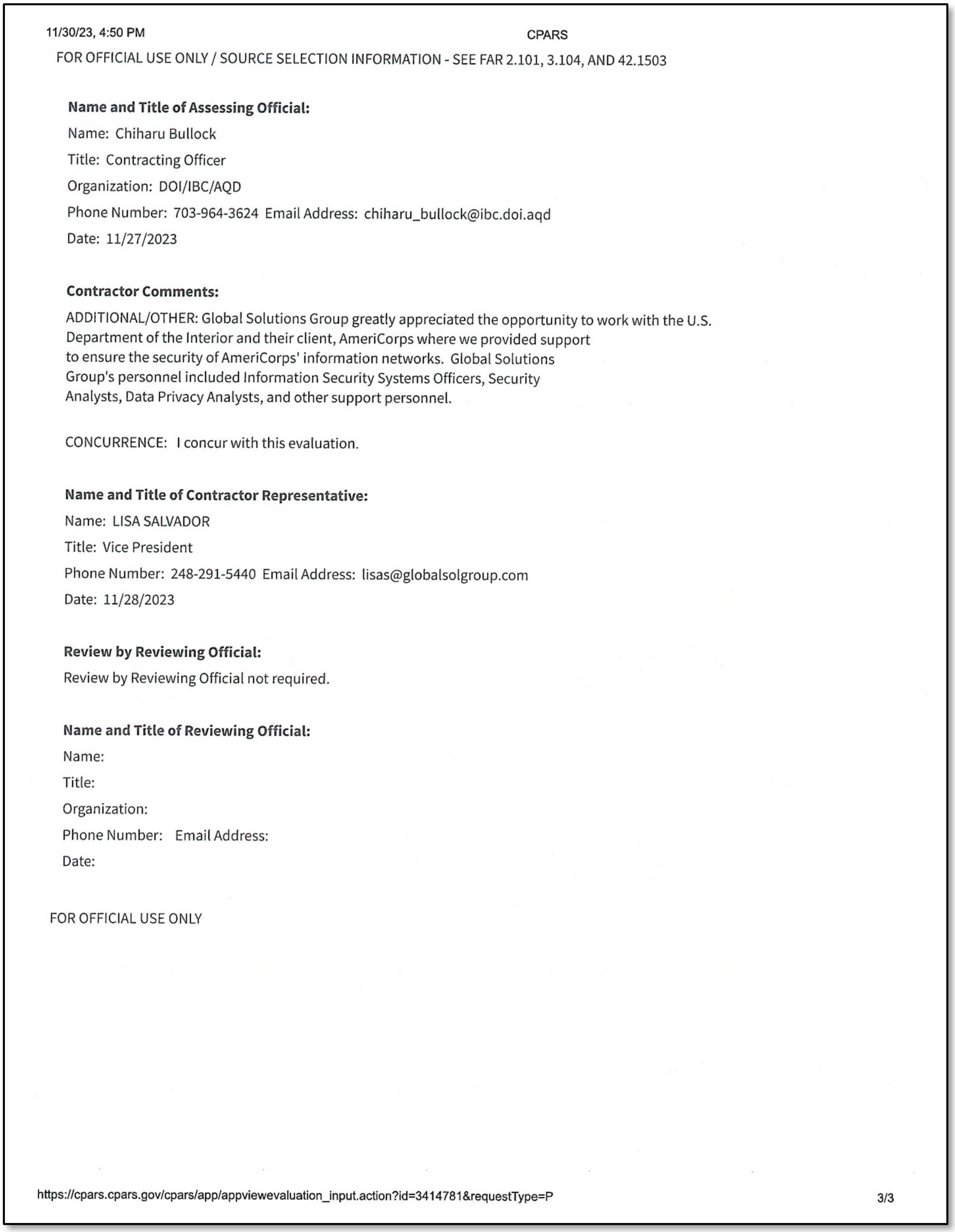
REGULATORY COMPLIANCE: The Contractor complied with all contract clauses and pertinent regulations.

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.

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=3414781&requestType=P 2/3



11/30/23, 4:50 PM CPARS

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

Name and Title of Assessing Official:

Name: Chiharu Bullock

Title: Contracting Officer

Organization: DOI/IBC/AQD

Phone Number: 703-964-3624 Email Address: chiharu_bullock@ibc.doi.aqd

Date: 11/27/2023

Contractor Comments:

ADDITIONAL/OTHER: Global Solutions Group greatly appreciated the opportunity to work with the U.S. Department of the Interior and their client, AmeriCorps where we provided support to ensure the security of AmeriCorps' information networks. Global Solutions Group's personnel included Information Security Systems Officers, Security Analysts, Data Privacy Analysts, and other support personnel.

CONCURRENCE: I concur with this evaluation.

Name and Title of Contractor Representative:

Name: LISA SALVADOR

Title: Vice President

Phone Number: 248-291-5440 Email Address: lisas@globalsolgroup.com

Date: 11/28/2023

Review by Reviewing Official:

Review by Reviewing Official not required.

Name and Title of Reviewing Official:

Name:

Title:

Organization:

Phone Number: Email Address:

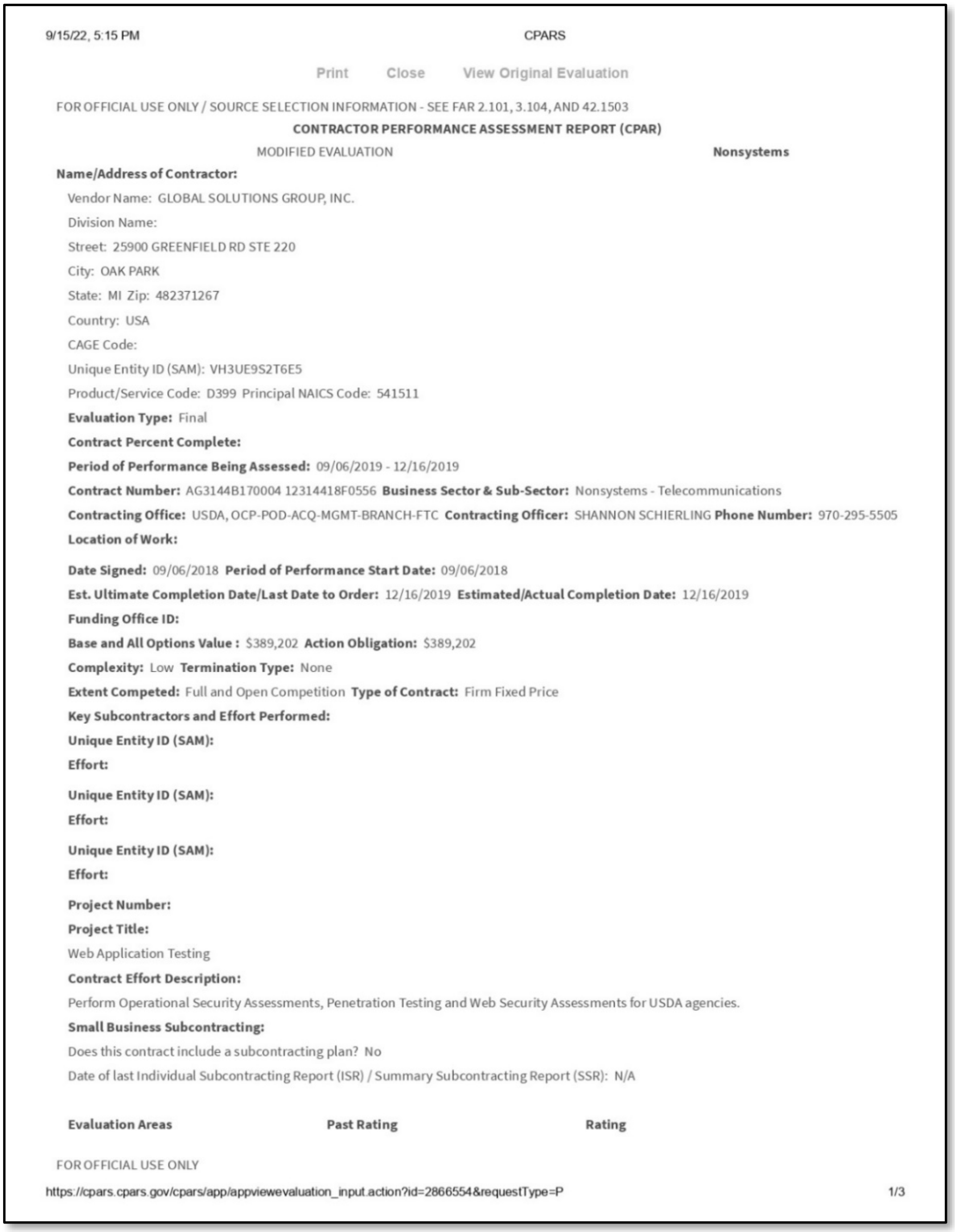
Date:

FOR OFFICIAL USE ONLY

https://cpars.cpars.gov/cpars/app/appviewevaluation_input.action?id=3414781&requestType=P 3/3

8.3.3 2019 Operational Security Assessments, Penetration Testing, and Web Security Assessments

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:

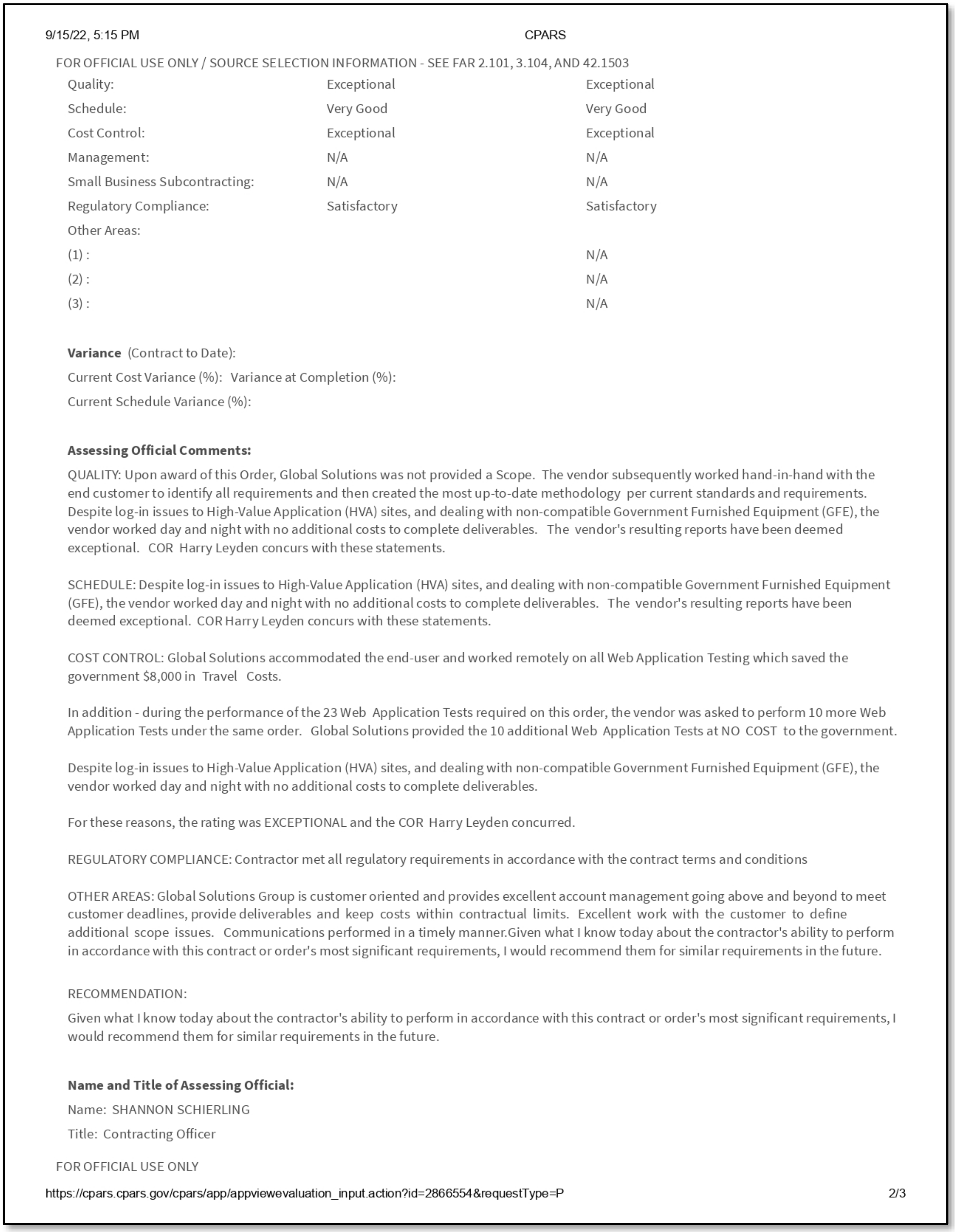
Unique Entity ID (SAM):
Effort:

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.

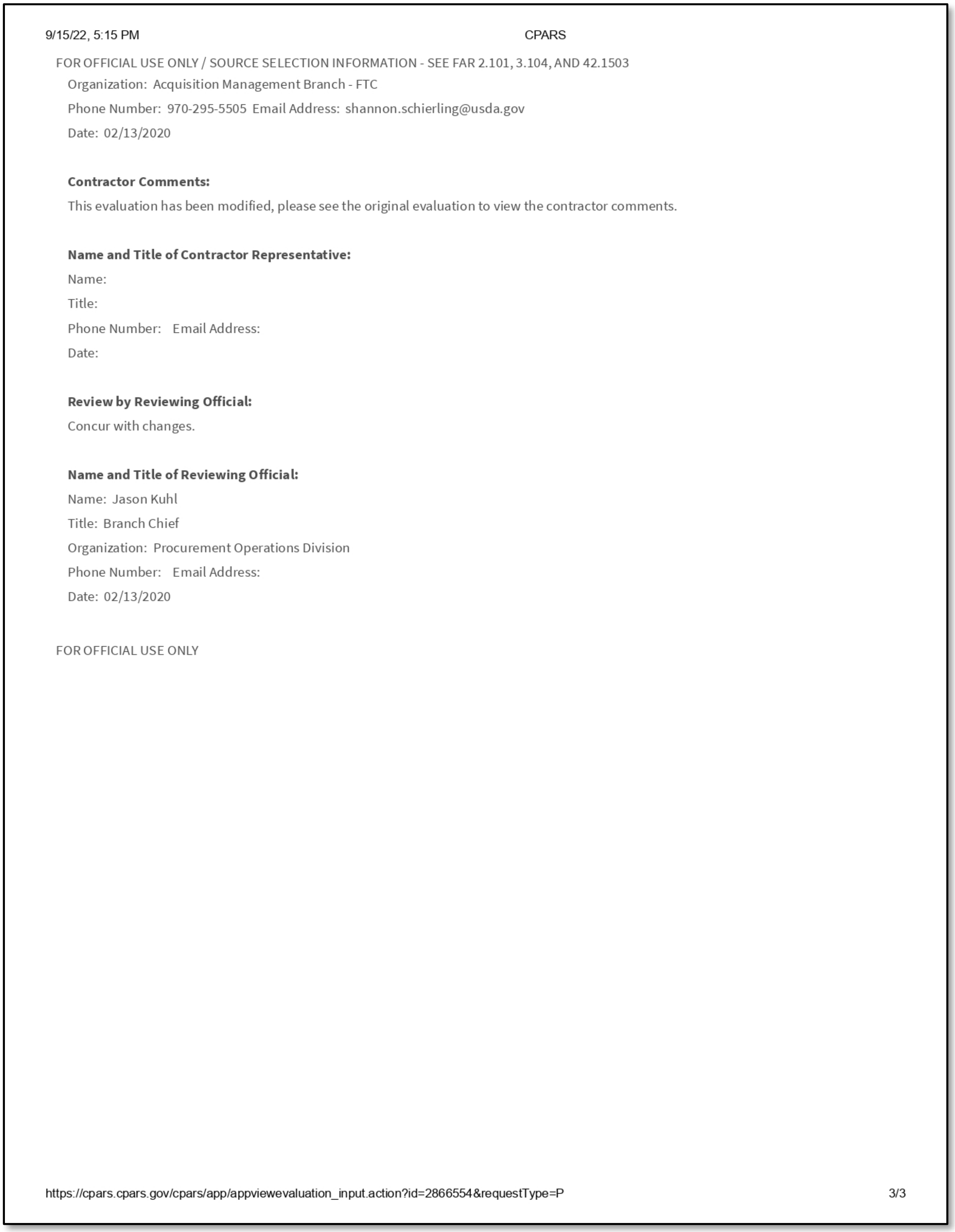
Name and Title of Assessing Official:

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



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

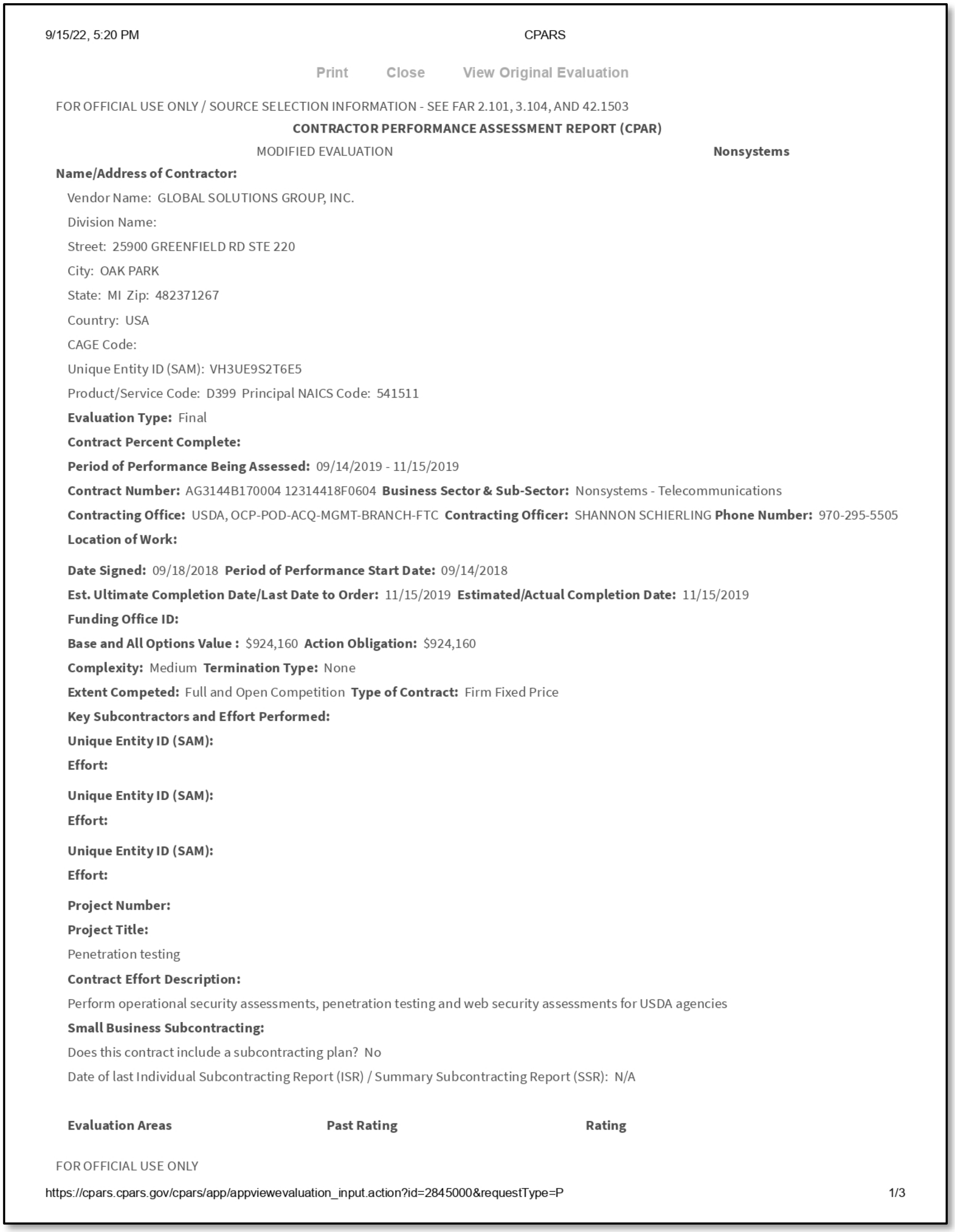
Phone Number: Email Address:

Date: 02/13/2020

FOR OFFICIAL USE ONLY

8.3.4 2019 Operational Security Assessment, Penetration Testing, and Web Security Assessment

Synopsis: Quality is 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:

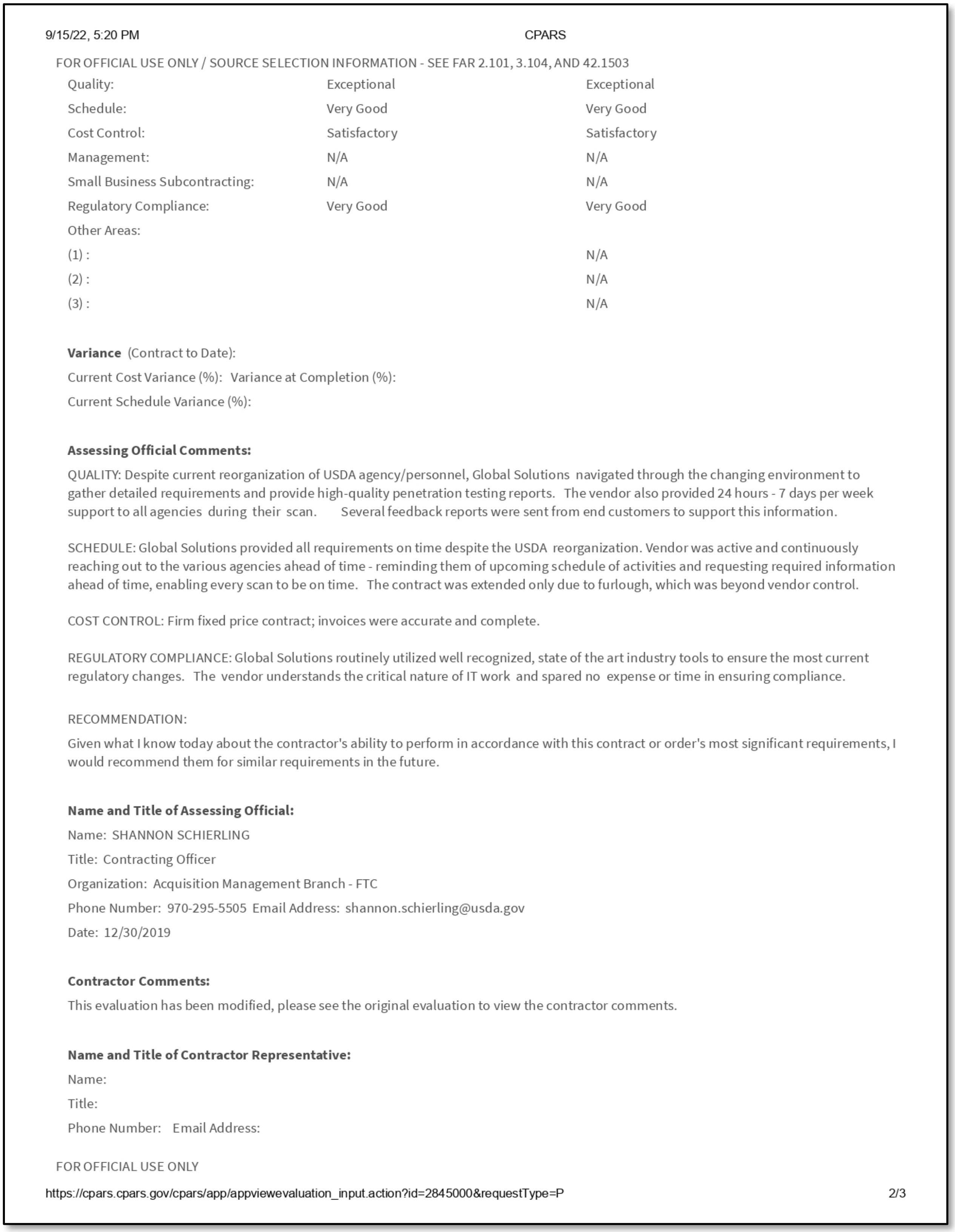
Does this contract include a subcontracting plan? No

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:

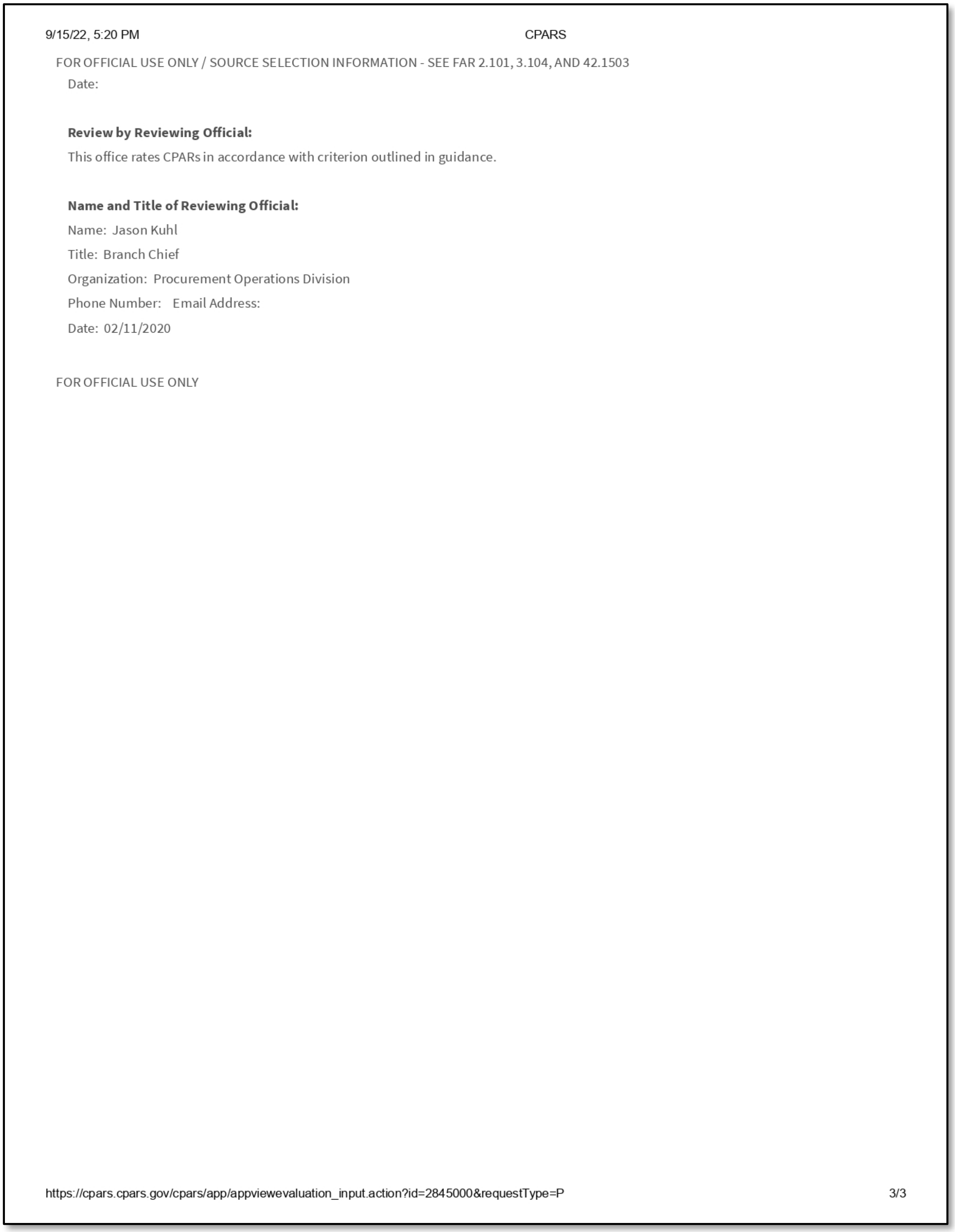
Name:

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:

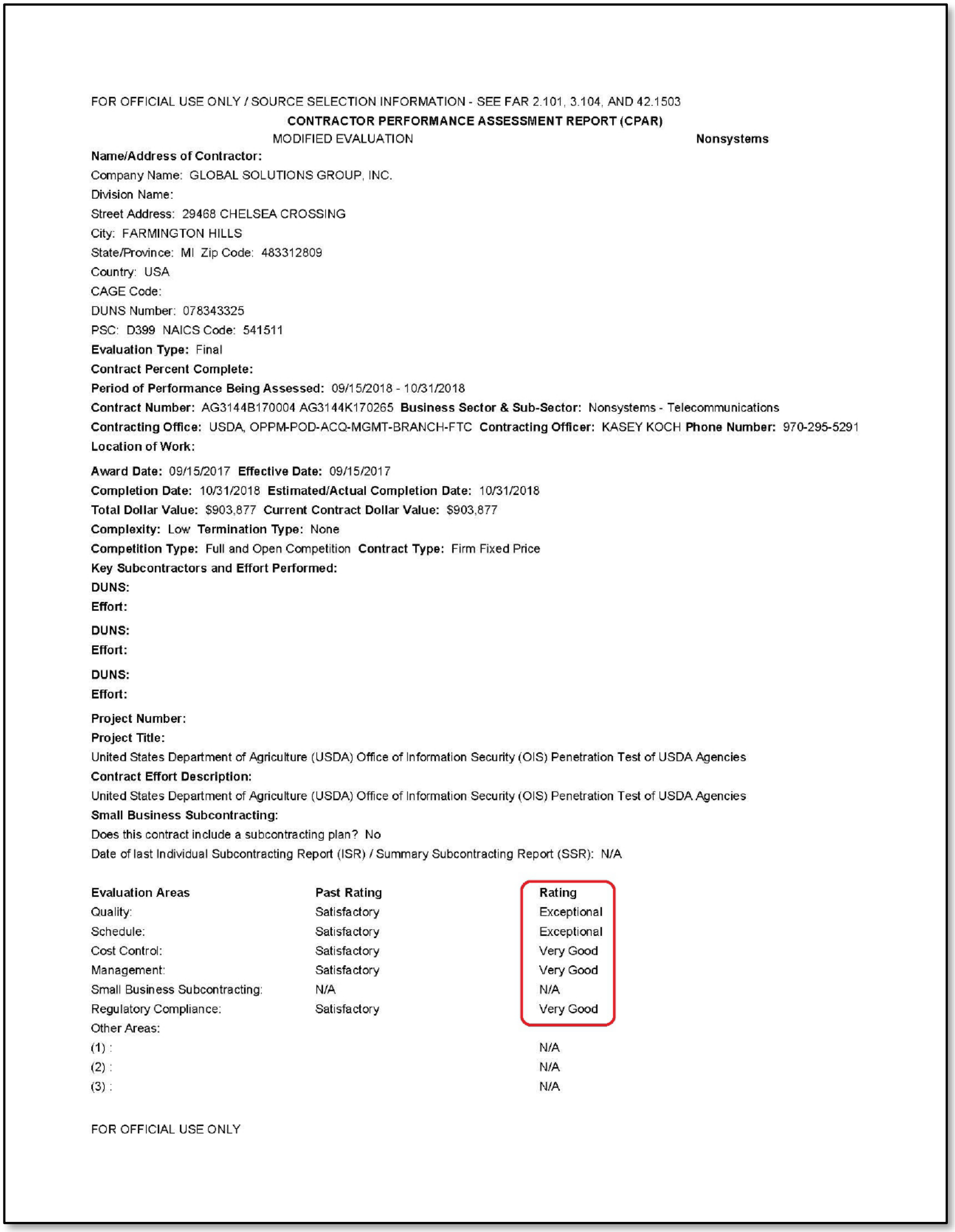
Date: 02/11/2020

FOR OFFICIAL USE ONLY

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

8.3.5 2018 Penetration Testing for USDA Agencies

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

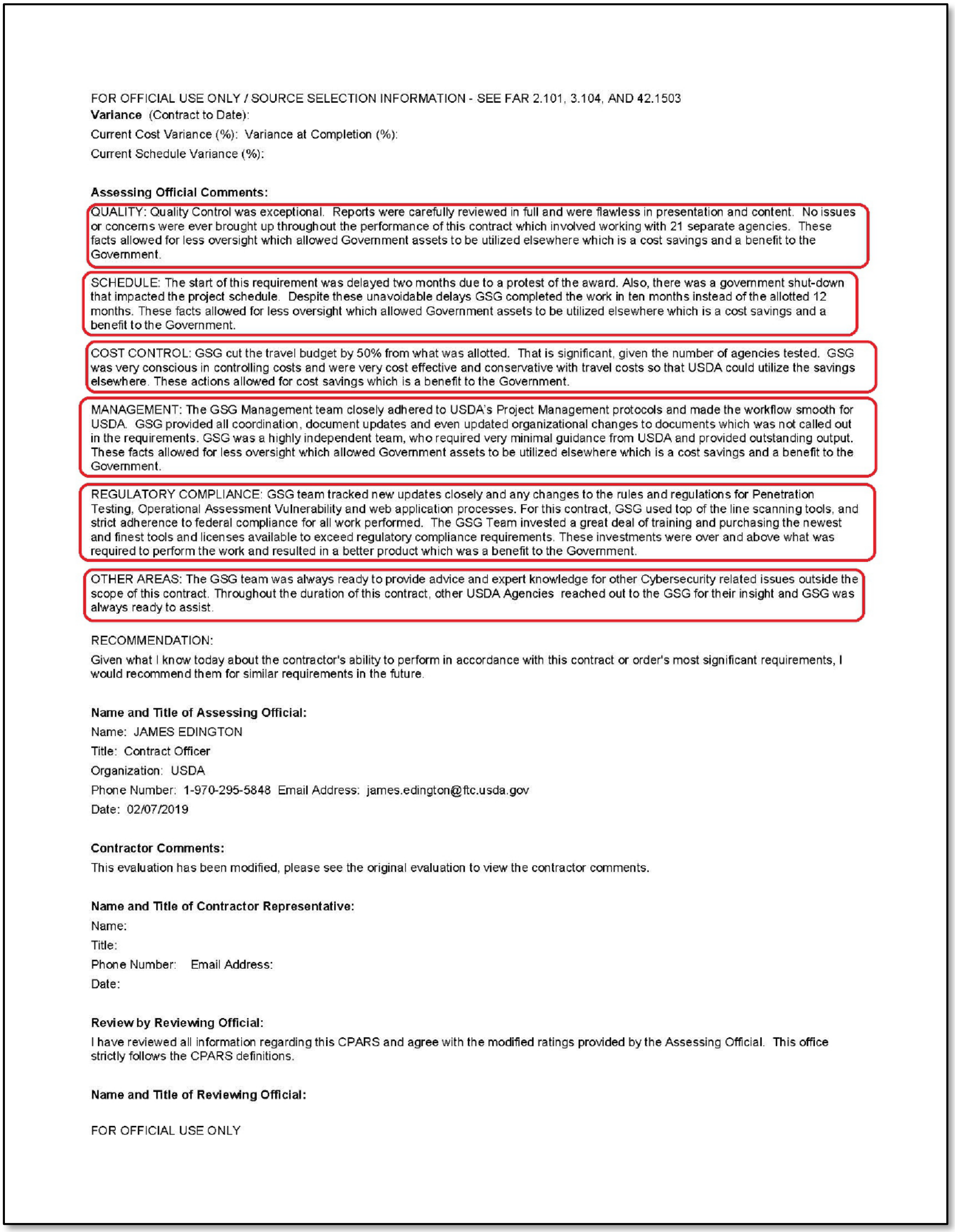
Small Business Subcontracting:

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:

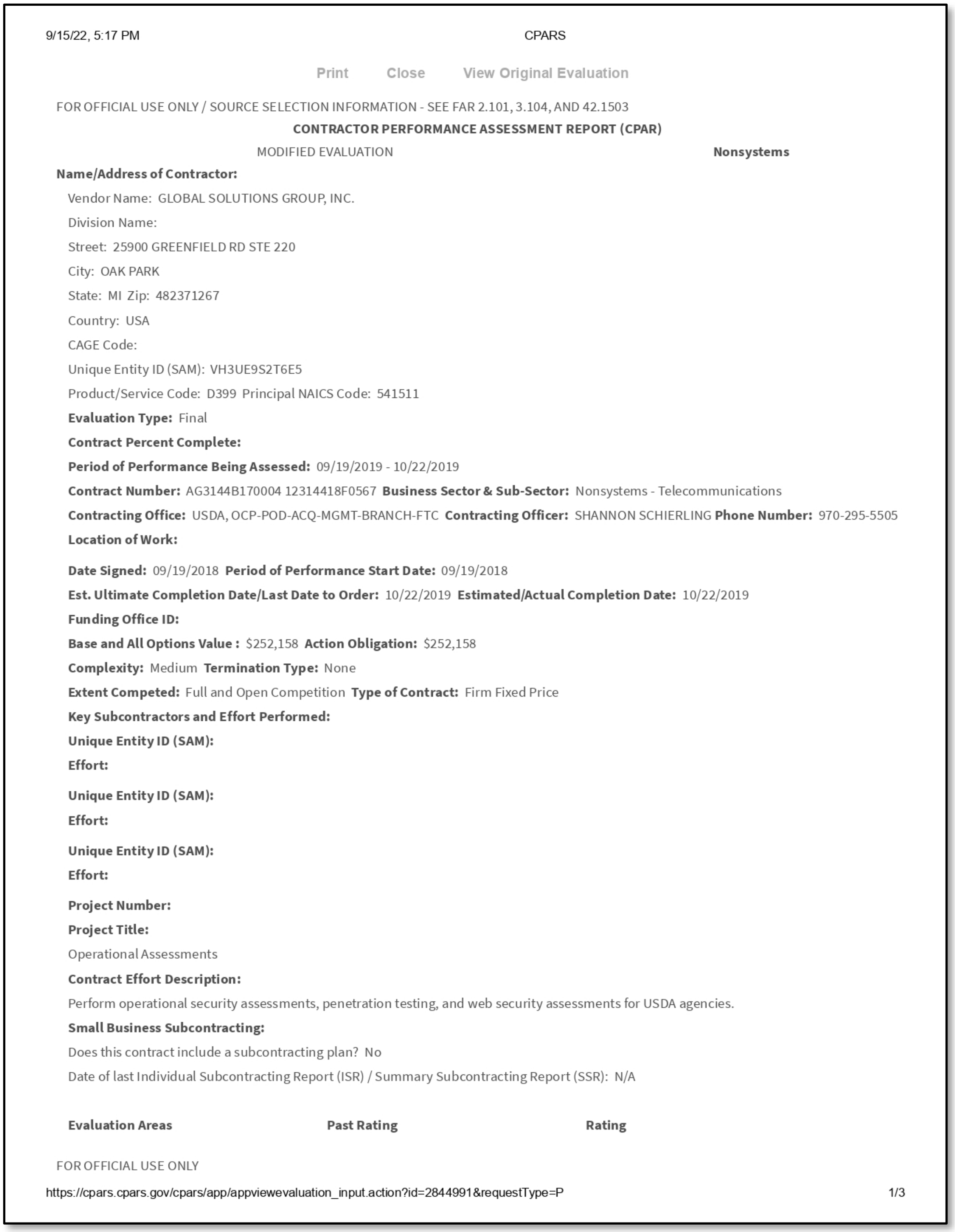
I have reviewed all information regarding this CPARS and agree with the modified ratings provided by the Assessing Official. This office strictly follows the CPARS definitions.

Name and Title of Reviewing Official:

FOR OFFICIAL USE ONLY

8.3.6 2019 Operational Security Assessment, Penetration Testing, and Web Security Assessment

Synopsis: Quality is Very Good



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:

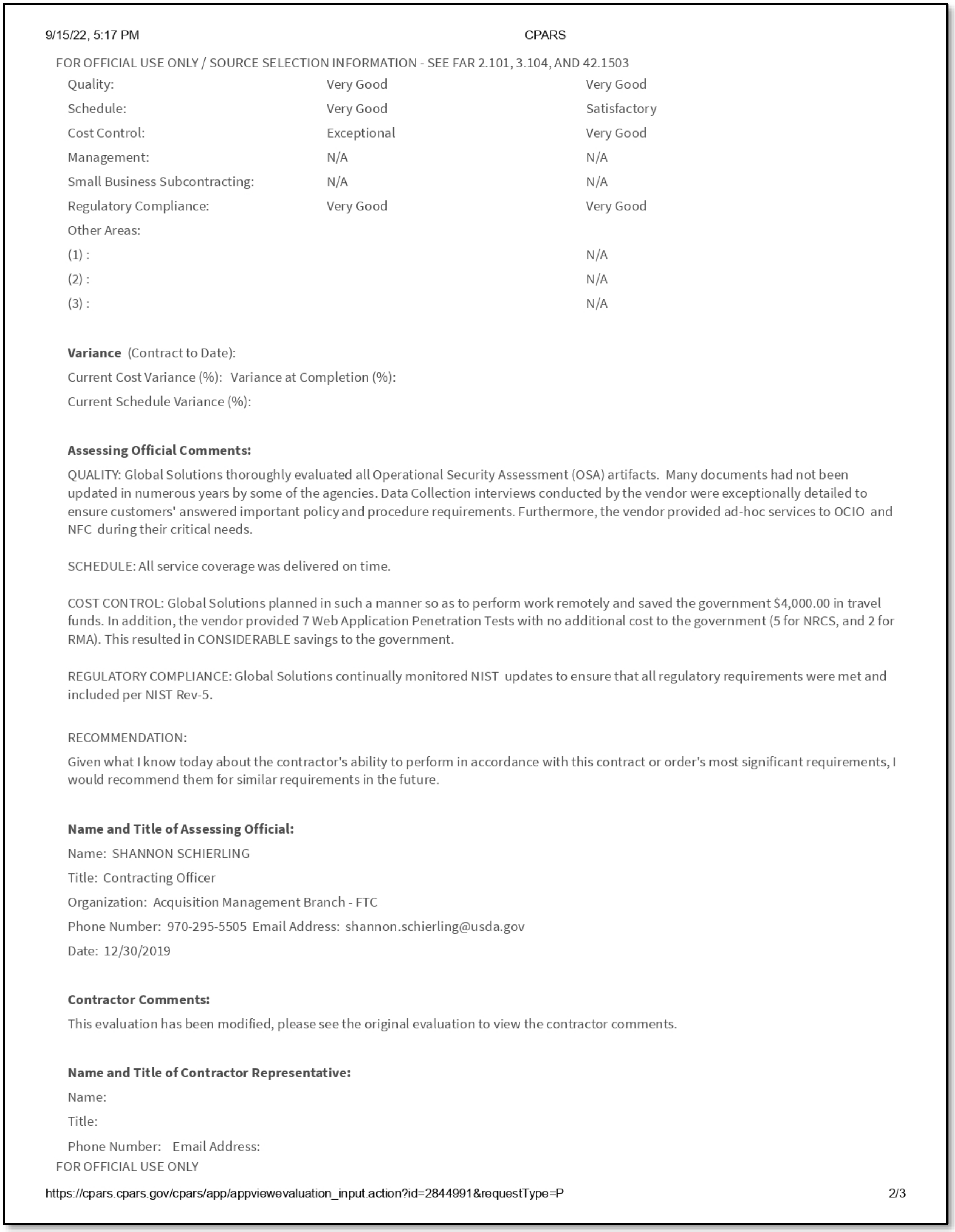
Does this contract include a subcontracting plan? No

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:

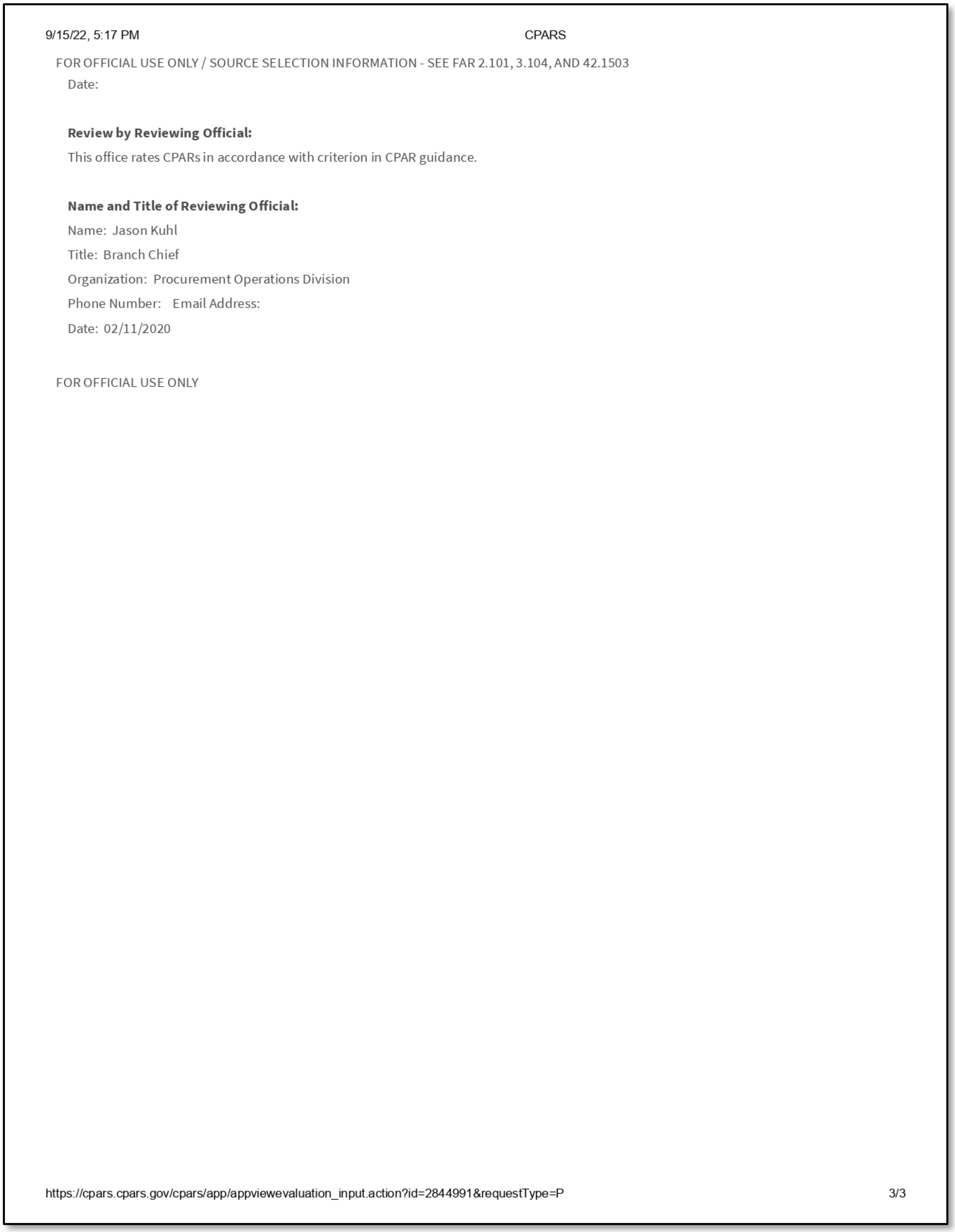
Name:

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:

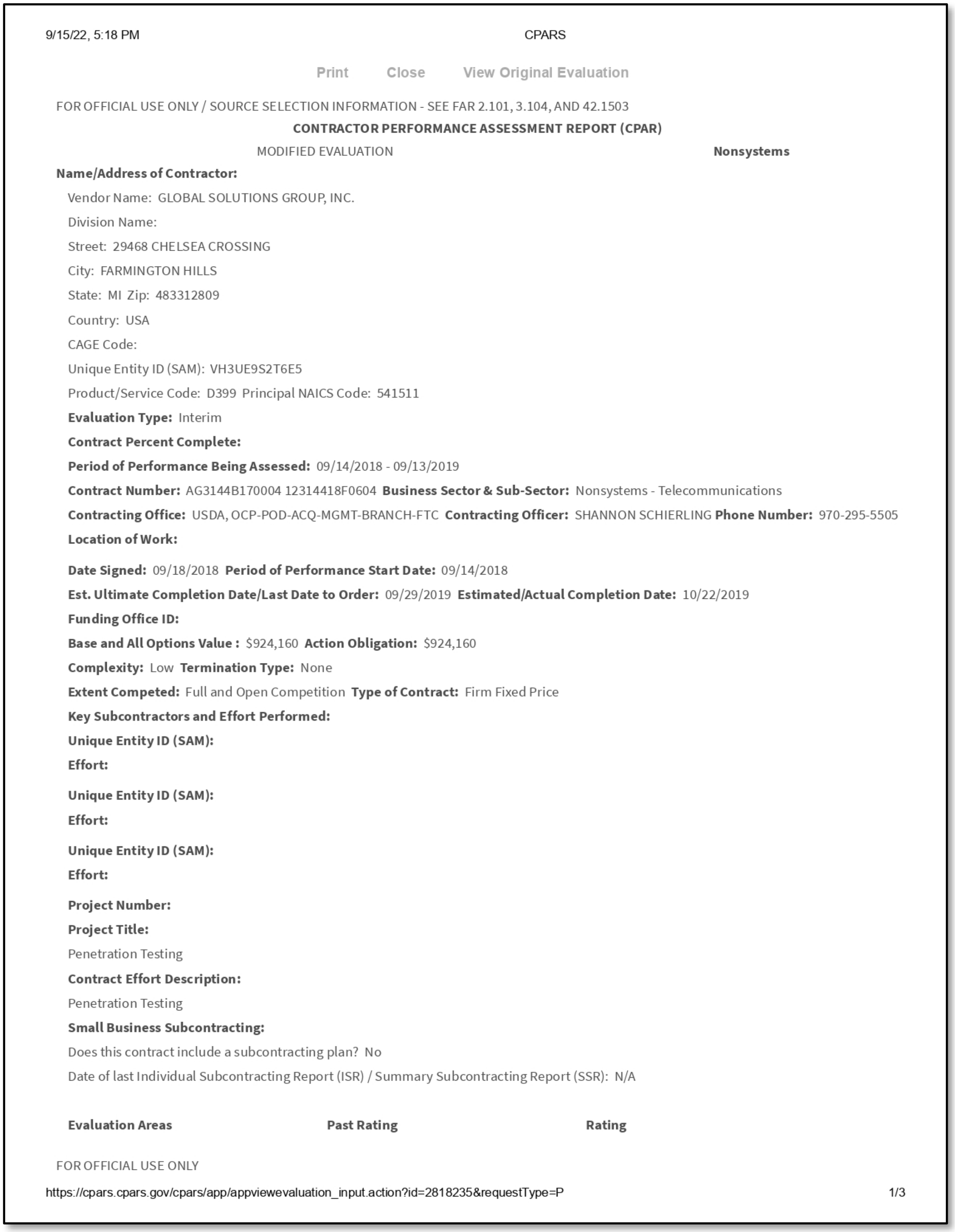
Date: 02/11/2020

FOR OFFICIAL USE ONLY

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

8.3.7 2019 Penetration Testing

Synopsis: Quality Exceptional



9/15/22, 5:18 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: 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:

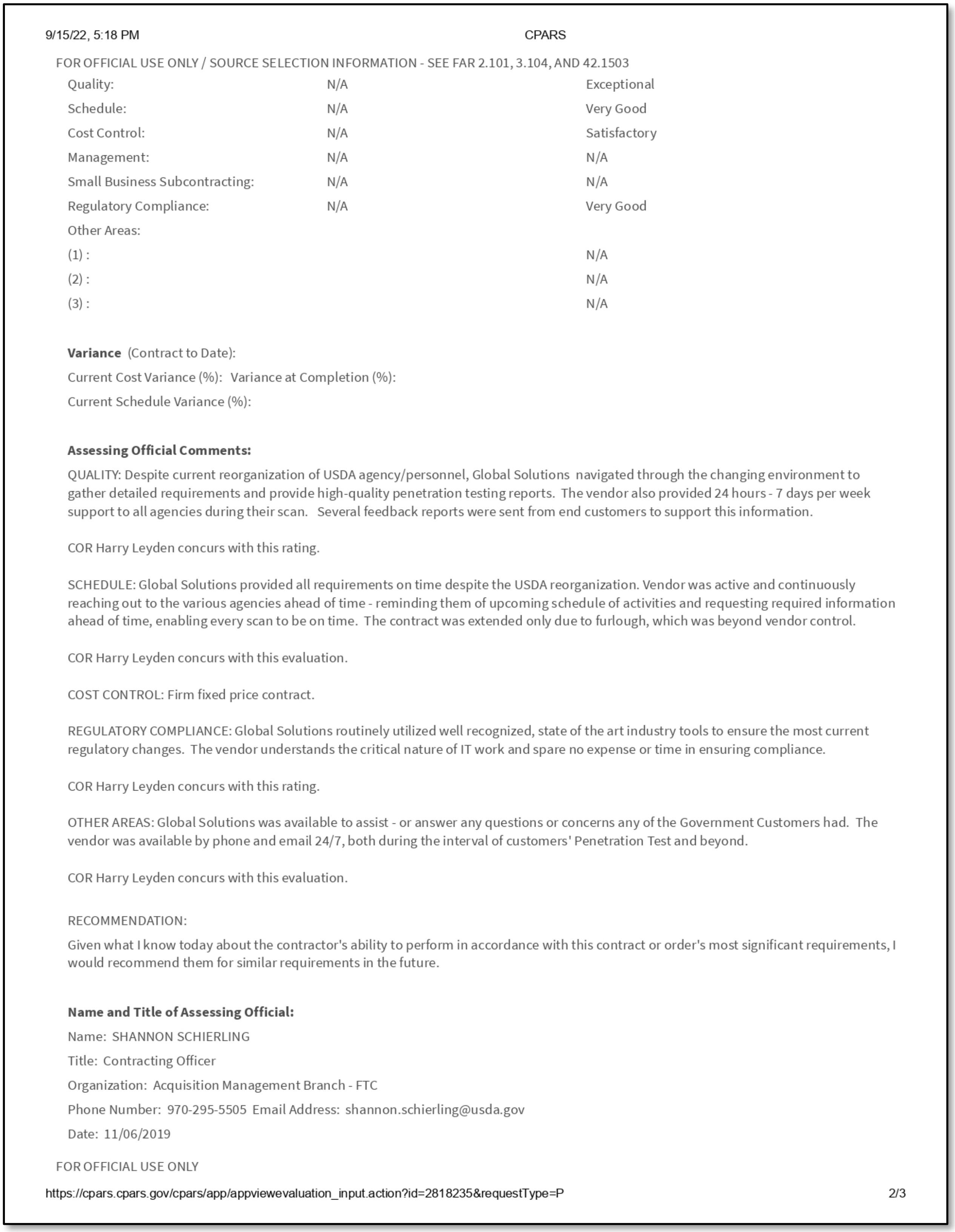
Does this contract include a subcontracting plan? No

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

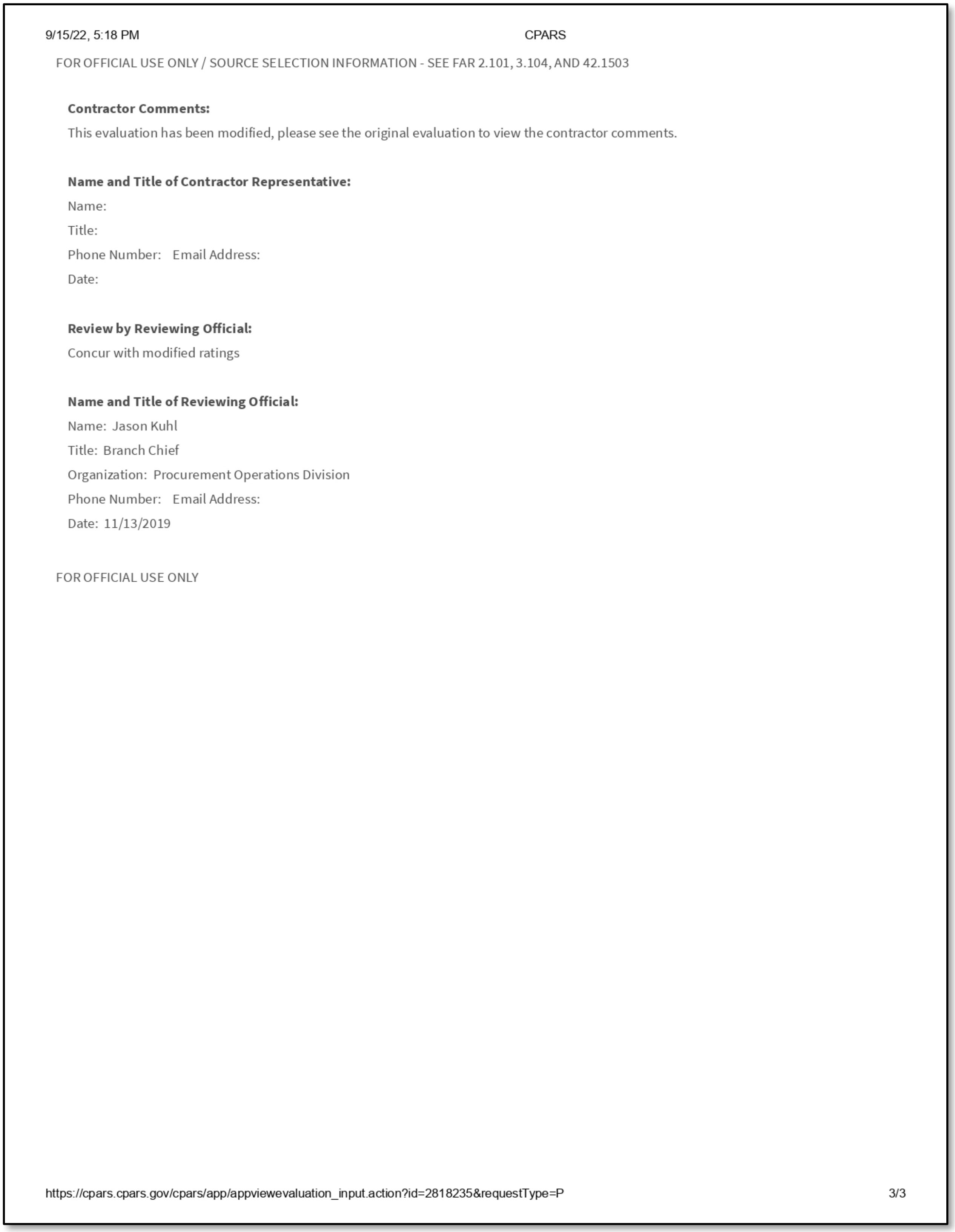
Organization: Acquisition Management Branch - FTC

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:

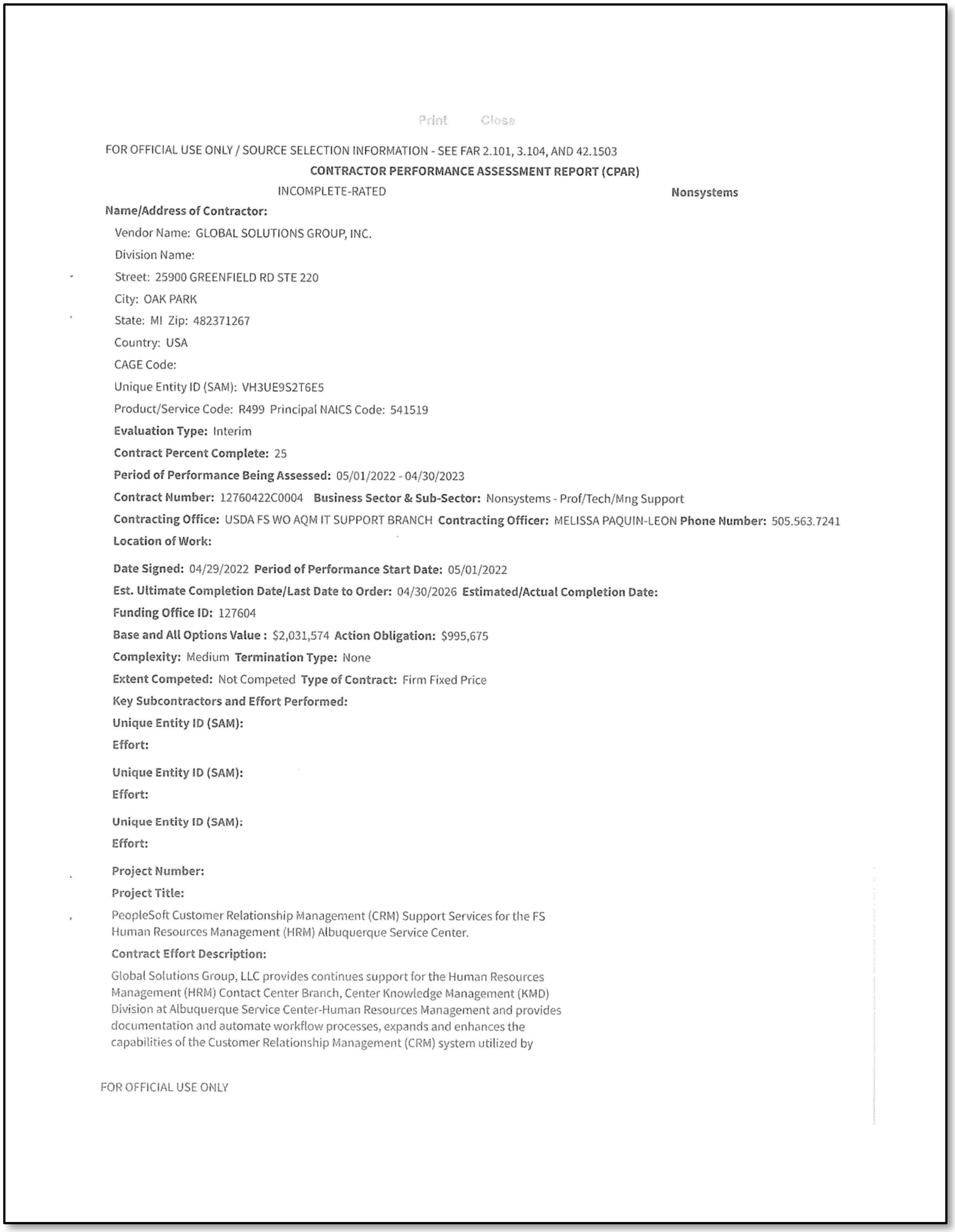
Name: Jason Kuhl
Title: Branch Chief
Organization: Procurement Operations Division
Phone Number: Email Address:
Date: 11/13/2019

FOR OFFICIAL USE ONLY

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

8.3.8 2023 People Soft Customer Relationship Support Services for the FS Human Resources Management Albuquerque Service Center

Synopsis: Very Good in All Areas



Print Close

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

CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)

INCOMPLETE-RATED **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: R499 Principal NAICS Code: 541519

Evaluation Type: Interim
Contract Percent Complete: 25
Period of Performance Being Assessed: 05/01/2022 - 04/30/2023
Contract Number: 12760422C0004 **Business Sector & Sub-Sector:** Nonsystems - Prof/Tech/Mng Support
Contracting Office: USDA FS WO AQM IT SUPPORT BRANCH **Contracting Officer:** MELISSA PAQUIN-LEON **Phone Number:** 505.563.7241
Location of Work:

Date Signed: 04/29/2022 **Period of Performance Start Date:** 05/01/2022
Est. Ultimate Completion Date/Last Date to Order: 04/30/2026 **Estimated/Actual Completion Date:**
Funding Office ID: 127604
Base and All Options Value : $2,031,574 **Action Obligation:** $995,675
Complexity: Medium **Termination Type:** None
Extent Competed: Not Competed **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:

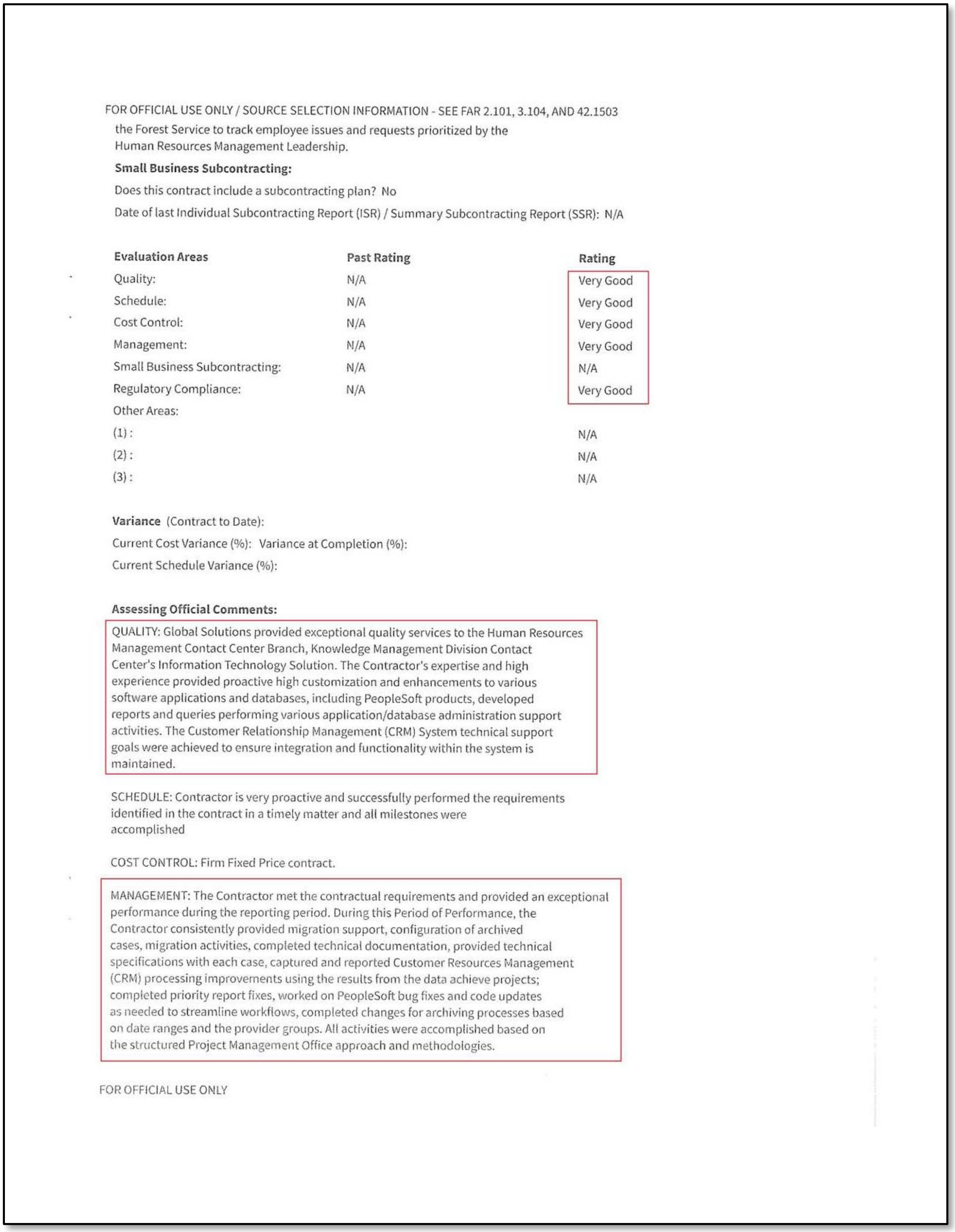
Project Number:
Project Title:

PeopleSoft Customer Relationship Management (CRM) Support Services for the FS Human Resources Management (HRM) Albuquerque Service Center.

Contract Effort Description:

Global Solutions Group, LLC provides continues support for the Human Resources Management (HRM) Contact Center Branch, Center Knowledge Management (KMD) Division at Albuquerque Service Center-Human Resources Management and provides documentation and automate workflow processes, expands and enhances the capabilities of the Customer Relationship Management (CRM) system utilized by

FOR OFFICIAL USE ONLY



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

the Forest Service to track employee issues and requests prioritized by the Human Resources Management Leadership.

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:	N/A	Very Good
Schedule:	N/A	Very Good
Cost Control:	N/A	Very Good
Management:	N/A	Very Good
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:

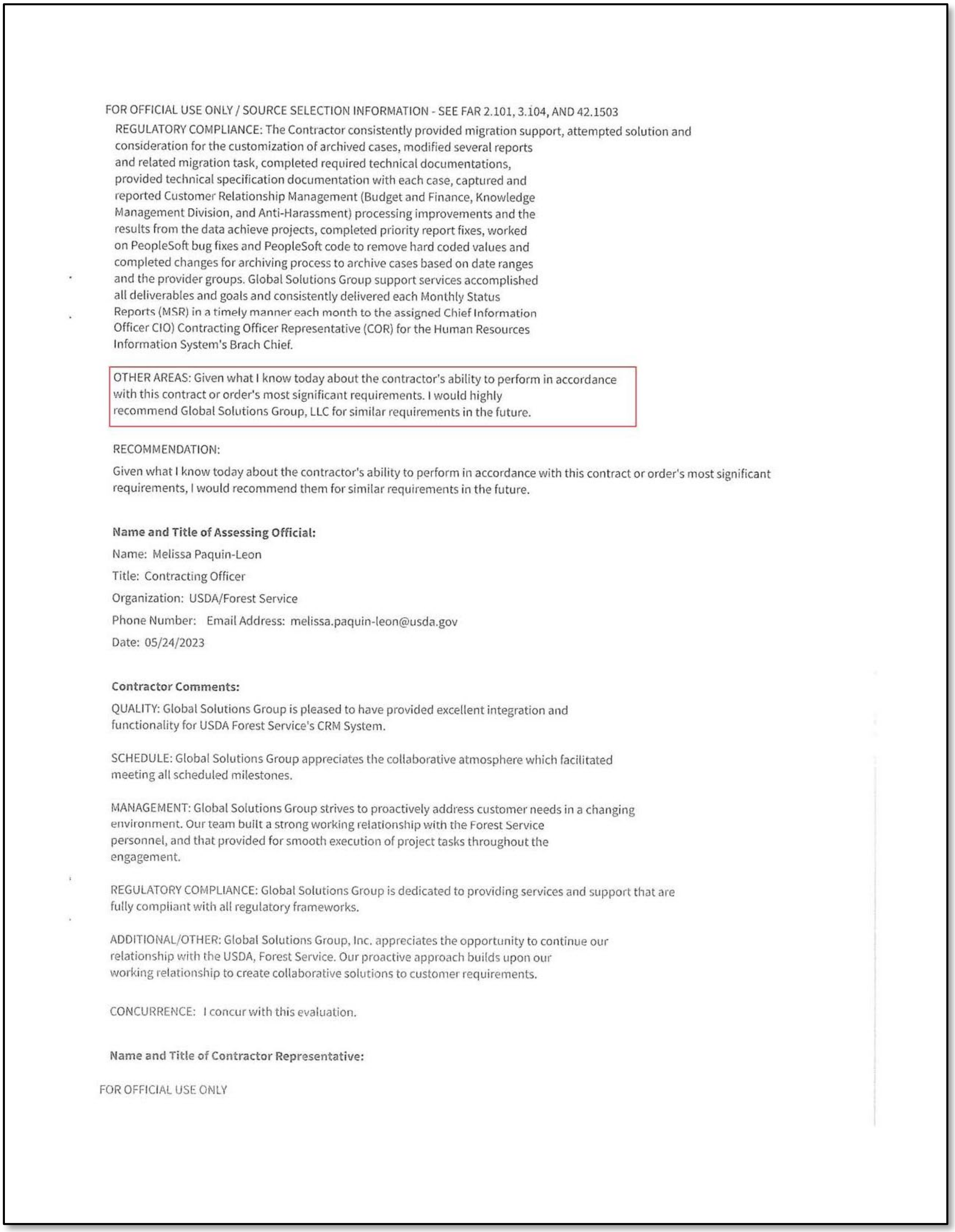
QUALITY: Global Solutions provided exceptional quality services to the Human Resources Management Contact Center Branch, Knowledge Management Division Contact Center's Information Technology Solution. The Contractor's expertise and high experience provided proactive high customization and enhancements to various software applications and databases, including PeopleSoft products, developed reports and queries performing various application/database administration support activities. The Customer Relationship Management (CRM) System technical support goals were achieved to ensure integration and functionality within the system is maintained.

SCHEDULE: Contractor is very proactive and successfully performed the requirements identified in the contract in a timely matter and all milestones were accomplished

COST CONTROL: Firm Fixed Price contract.

MANAGEMENT: The Contractor met the contractual requirements and provided an exceptional performance during the reporting period. During this Period of Performance, the Contractor consistently provided migration support, configuration of archived cases, migration activities, completed technical documentation, provided technical specifications with each case, captured and reported Customer Resources Management (CRM) processing improvements using the results from the data achieve projects; completed priority report fixes, worked on PeopleSoft bug fixes and code updates as needed to streamline workflows, completed changes for archiving processes based on date ranges and the provider groups. All activities were accomplished based on the structured Project Management Office approach and methodologies.

FOR OFFICIAL USE ONLY



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

REGULATORY COMPLIANCE: The Contractor consistently provided migration support, attempted solution and consideration for the customization of archived cases, modified several reports and related migration task, completed required technical documentations, provided technical specification documentation with each case, captured and reported Customer Relationship Management (Budget and Finance, Knowledge Management Division, and Anti-Harassment) processing improvements and the results from the data achieve projects, completed priority report fixes, worked on PeopleSoft bug fixes and PeopleSoft code to remove hard coded values and completed changes for archiving process to archive cases based on date ranges and the provider groups. Global Solutions Group support services accomplished all deliverables and goals and consistently delivered each Monthly Status Reports (MSR) in a timely manner each month to the assigned Chief Information Officer CIO) Contracting Officer Representative (COR) for the Human Resources Information System's Brach Chief.

OTHER AREAS: 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 highly recommend Global Solutions Group, LLC 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: Melissa Paquin-Leon

Title: Contracting Officer

Organization: USDA/Forest Service

Phone Number: Email Address: melissa.paquin-leon@usda.gov

Date: 05/24/2023

Contractor Comments:

QUALITY: Global Solutions Group is pleased to have provided excellent integration and functionality for USDA Forest Service's CRM System.

SCHEDULE: Global Solutions Group appreciates the collaborative atmosphere which facilitated meeting all scheduled milestones.

MANAGEMENT: Global Solutions Group strives to proactively address customer needs in a changing environment. Our team built a strong working relationship with the Forest Service personnel, and that provided for smooth execution of project tasks throughout the engagement.

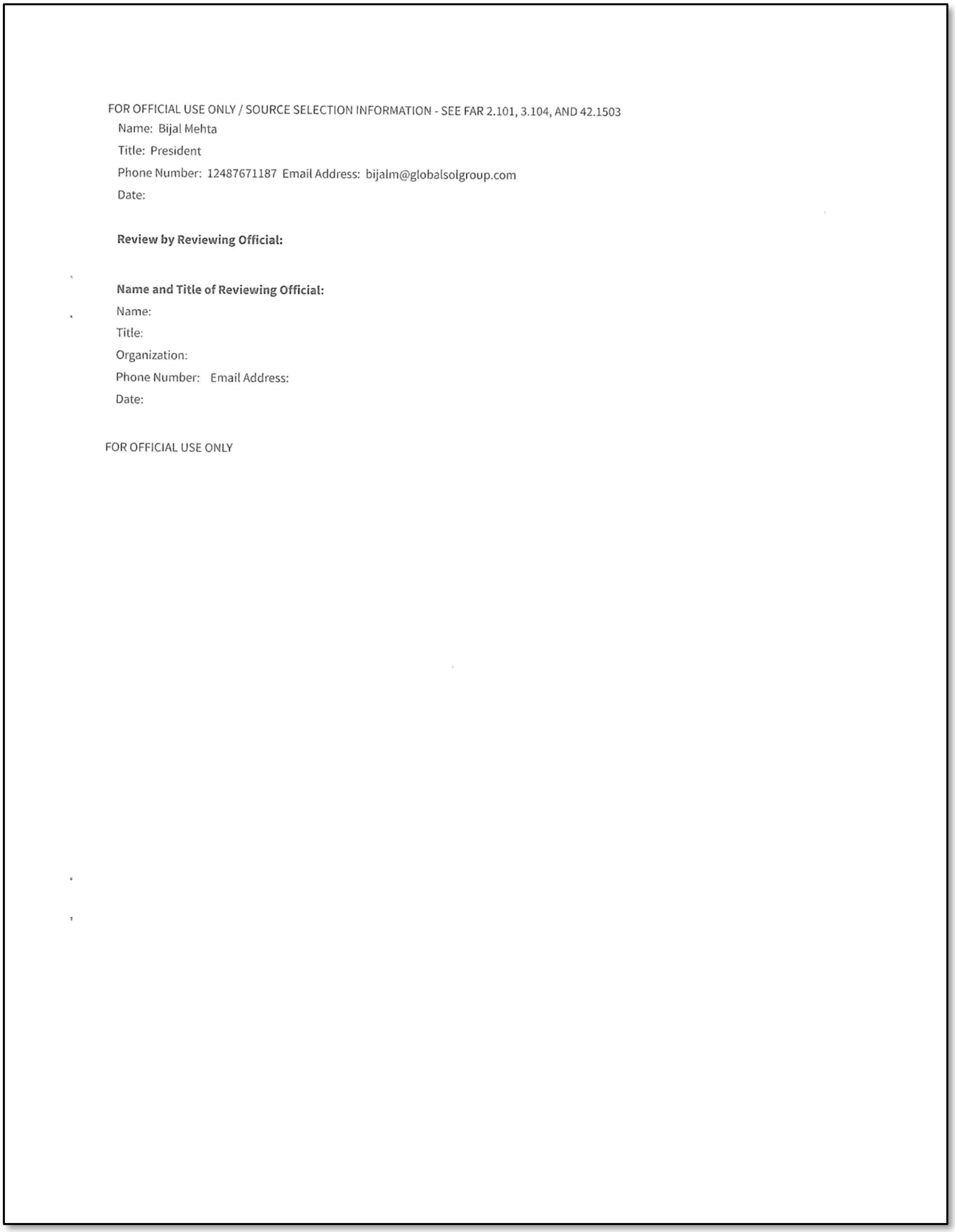
REGULATORY COMPLIANCE: Global Solutions Group is dedicated to providing services and support that are fully compliant with all regulatory frameworks.

ADDITIONAL/OTHER: Global Solutions Group, Inc. appreciates the opportunity to continue our relationship with the USDA, Forest Service. Our proactive approach builds upon our working relationship to create collaborative solutions to customer requirements.

CONCURRENCE: I concur with this evaluation.

Name and Title of Contractor Representative:

FOR OFFICIAL USE ONLY



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

Name: Bijal Mehta

Title: President

Phone Number: 12487671187 Email Address: bijalm@globalsolgroup.com

Date:

Review by Reviewing Official:

Name and Title of Reviewing Official:

Name:

Title:

Organization:

Phone Number: Email Address:

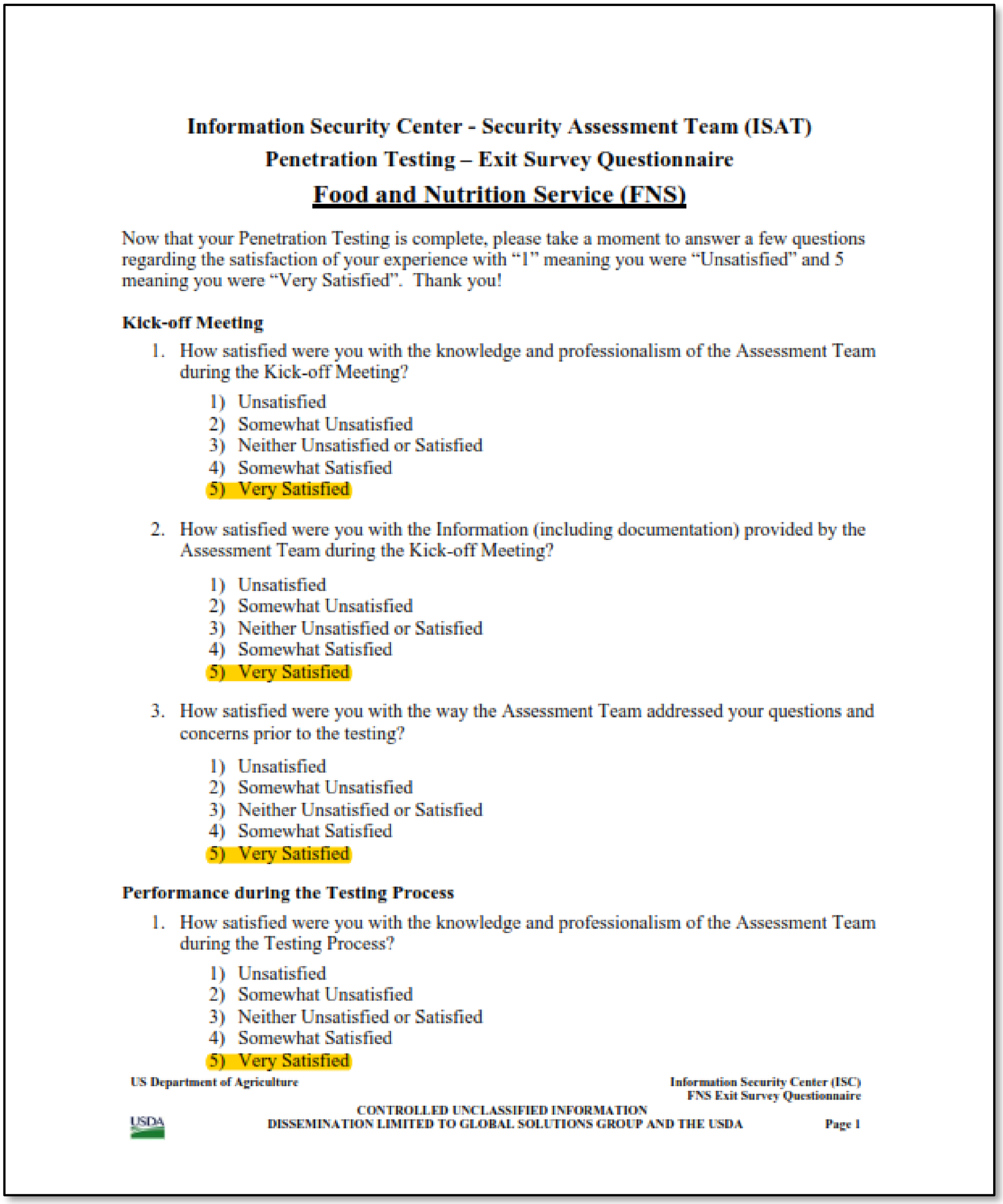
Date:

FOR OFFICIAL USE ONLY

8.4 Exit Surveys

8.4.1 Food and Nutrition Service, Information Security Center, Security Assessment Team, and 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]

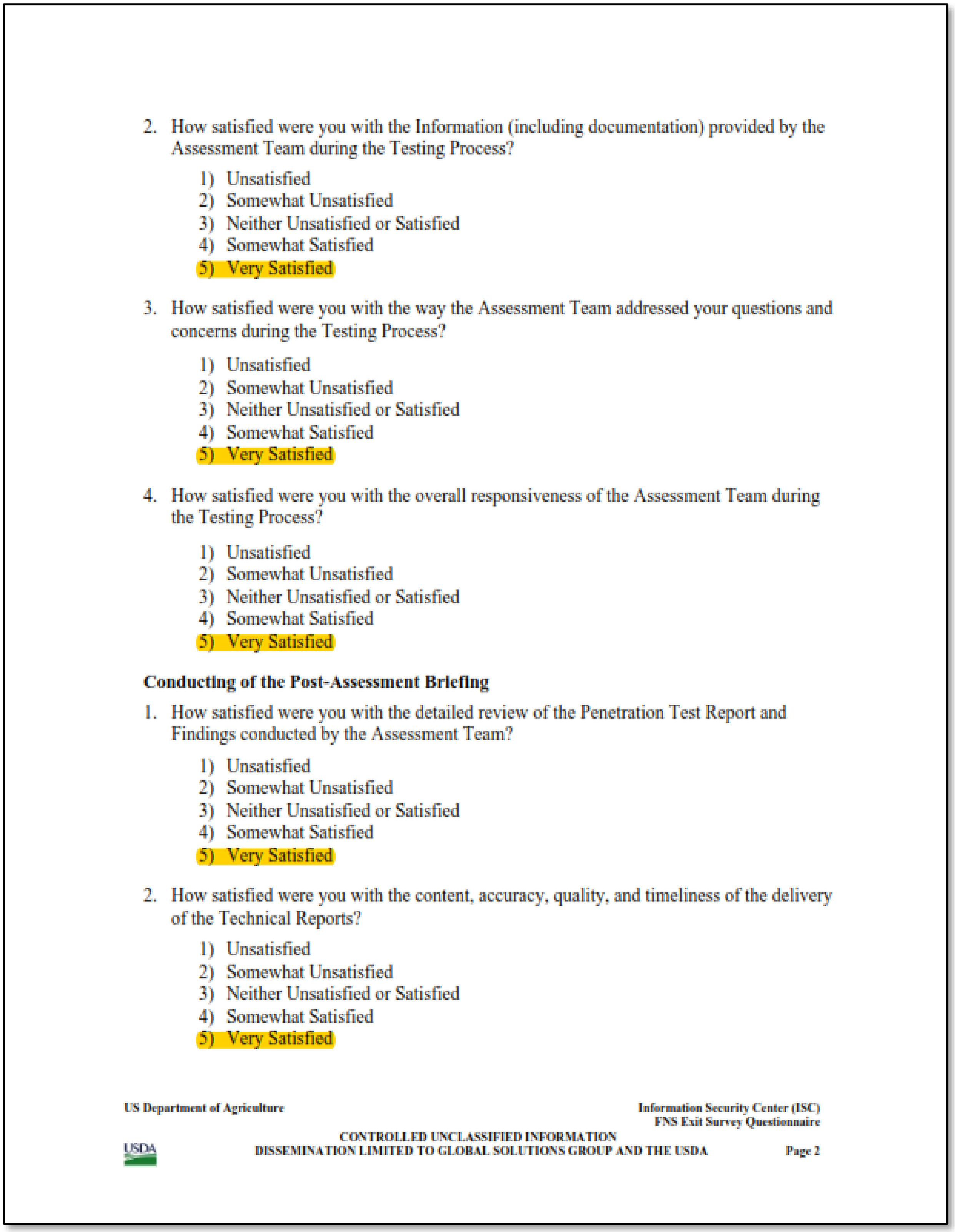
US Department of Agriculture

Information Security Center (ISC)
FNS Exit Survey Questionnaire

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

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]

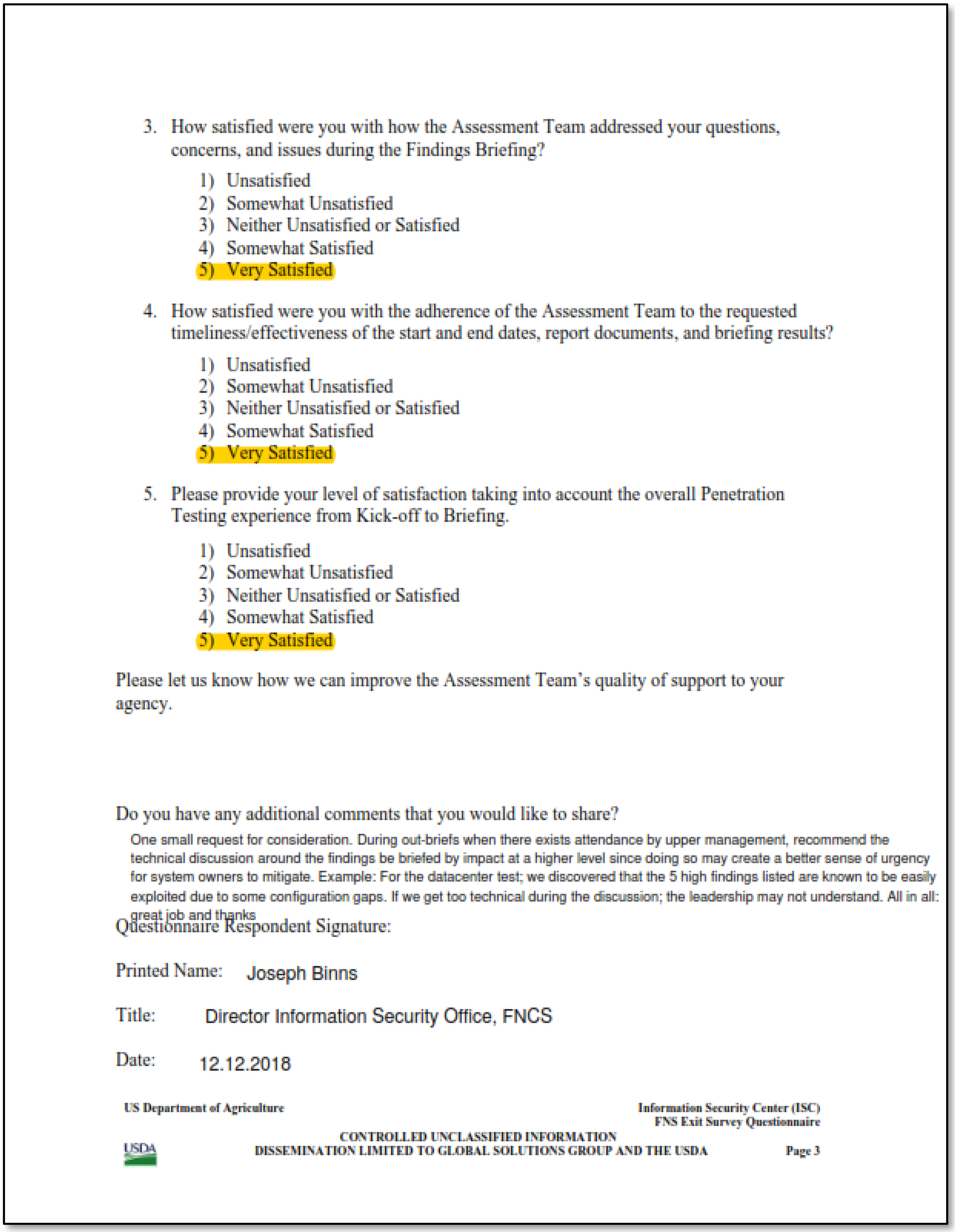
US Department of Agriculture

Information Security Center (ISC)
FNS Exit Survey Questionnaire

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

USDA

Page 2



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:

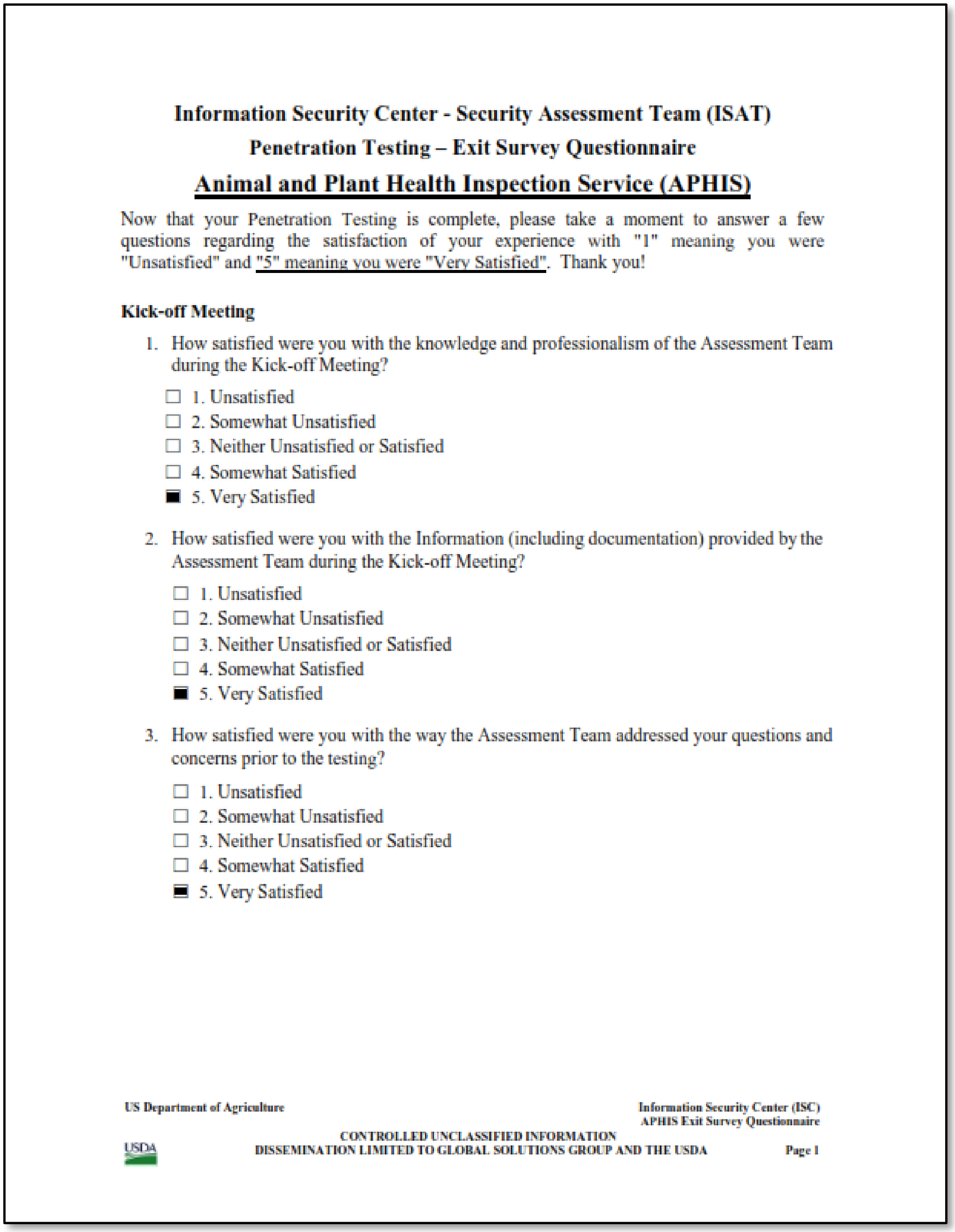
Printed Name: Joseph Binns

Title: Director Information Security Office, FNCS

Date: 12.12.2018

8.4.2 APHIS - Information Security Center – Security Assessment Team and 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

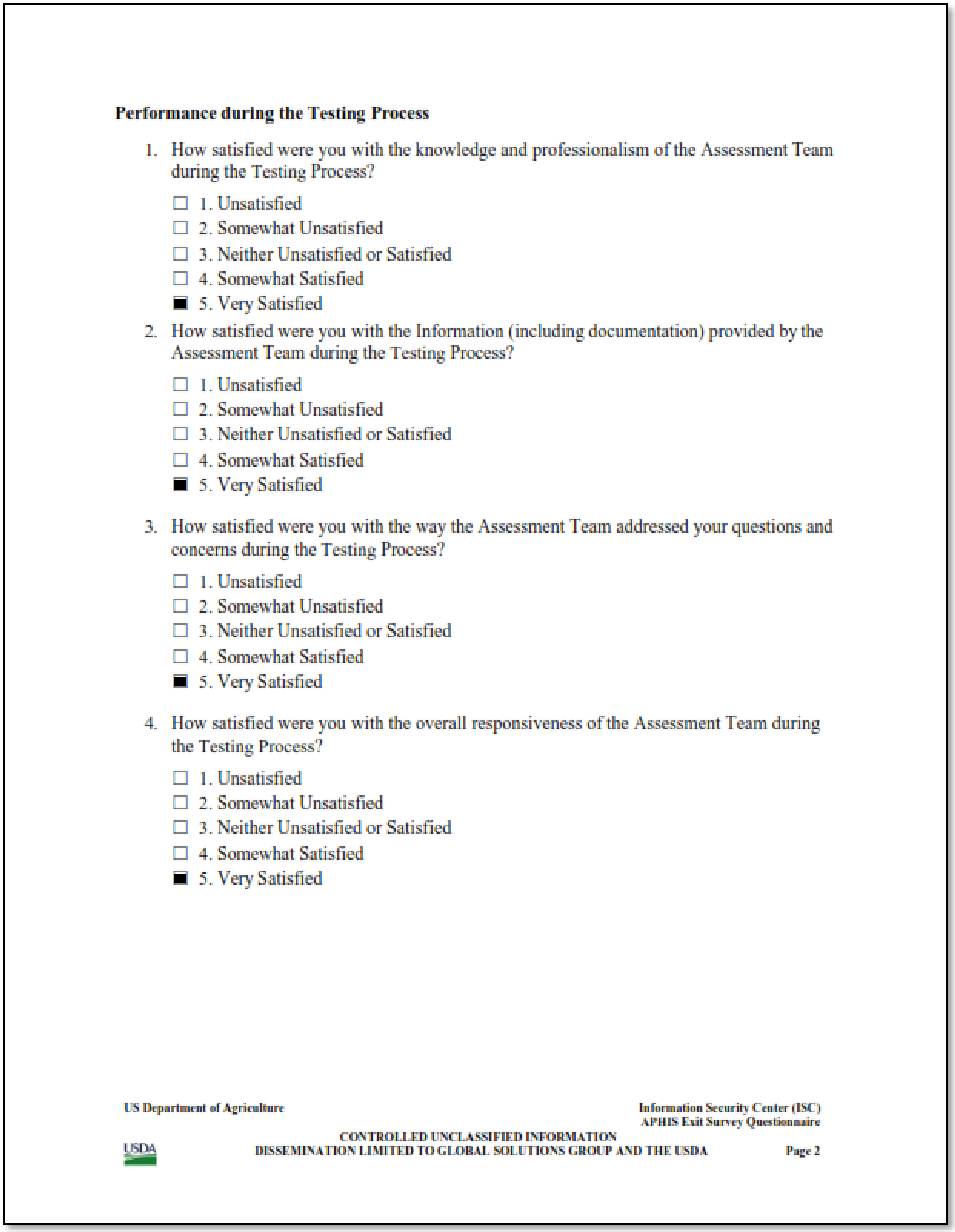
US Department of Agriculture

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

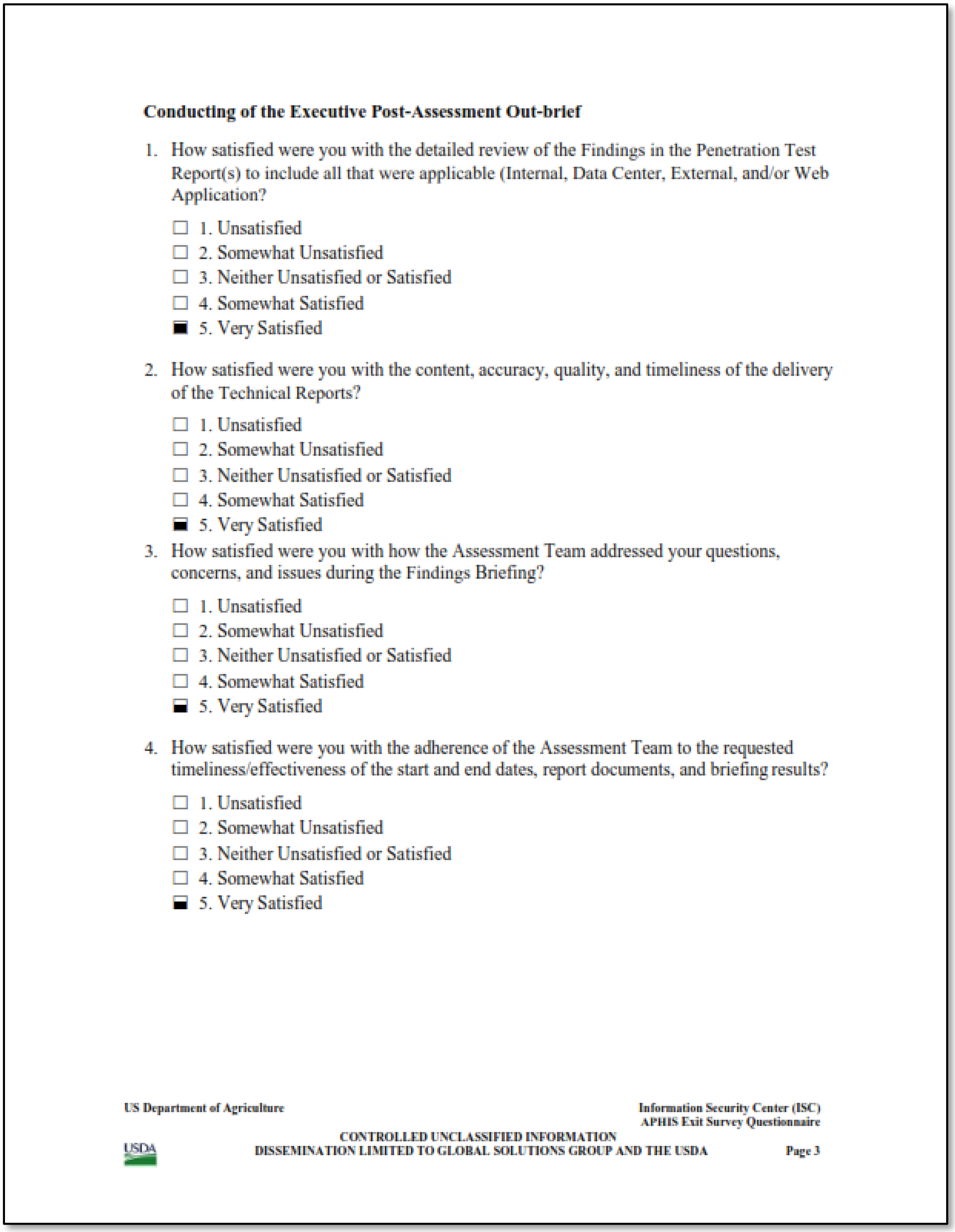
US Department of Agriculture

Information Security Center (ISC)
APHIS Exit Survey Questionnaire

USDA

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?

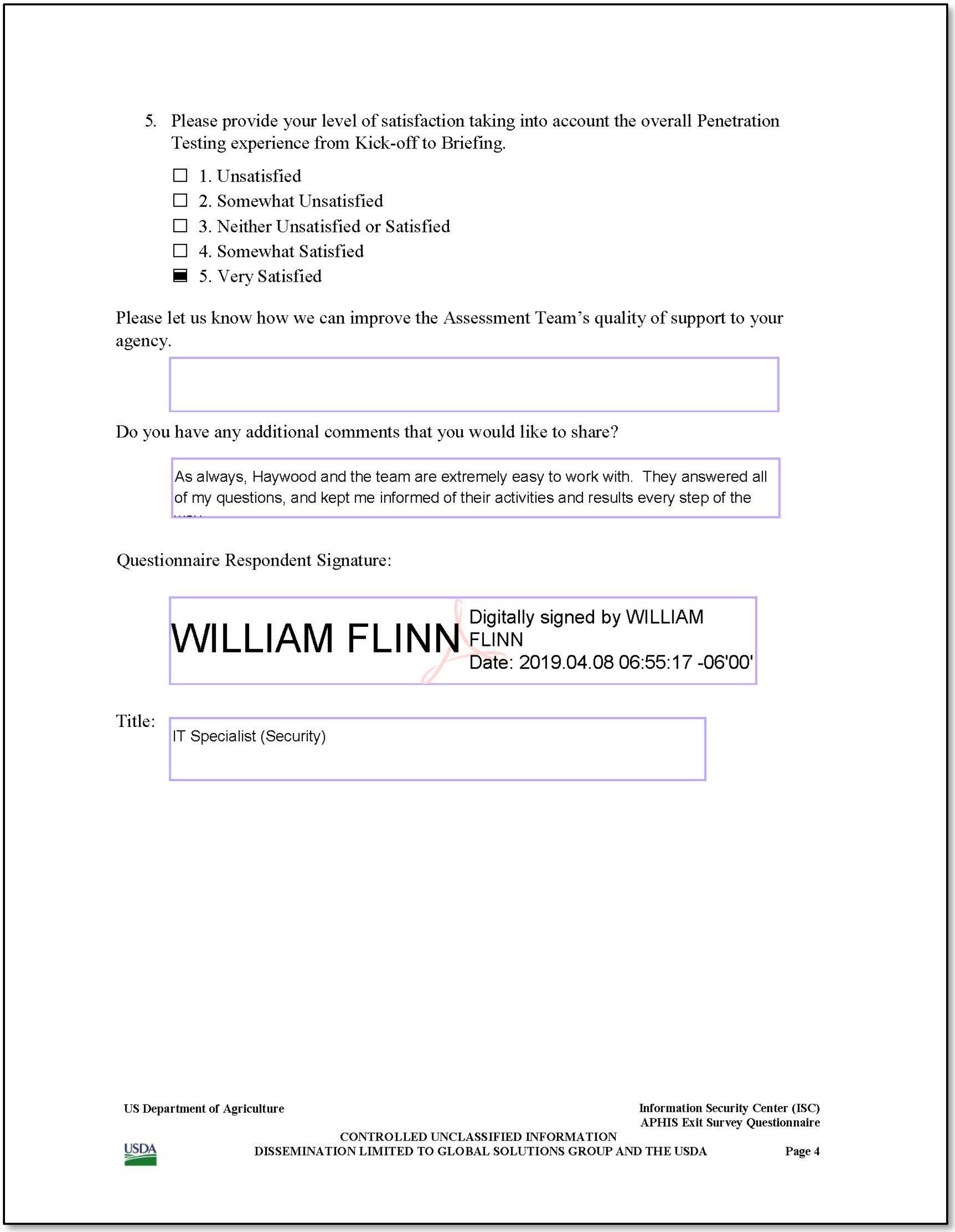
   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

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



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

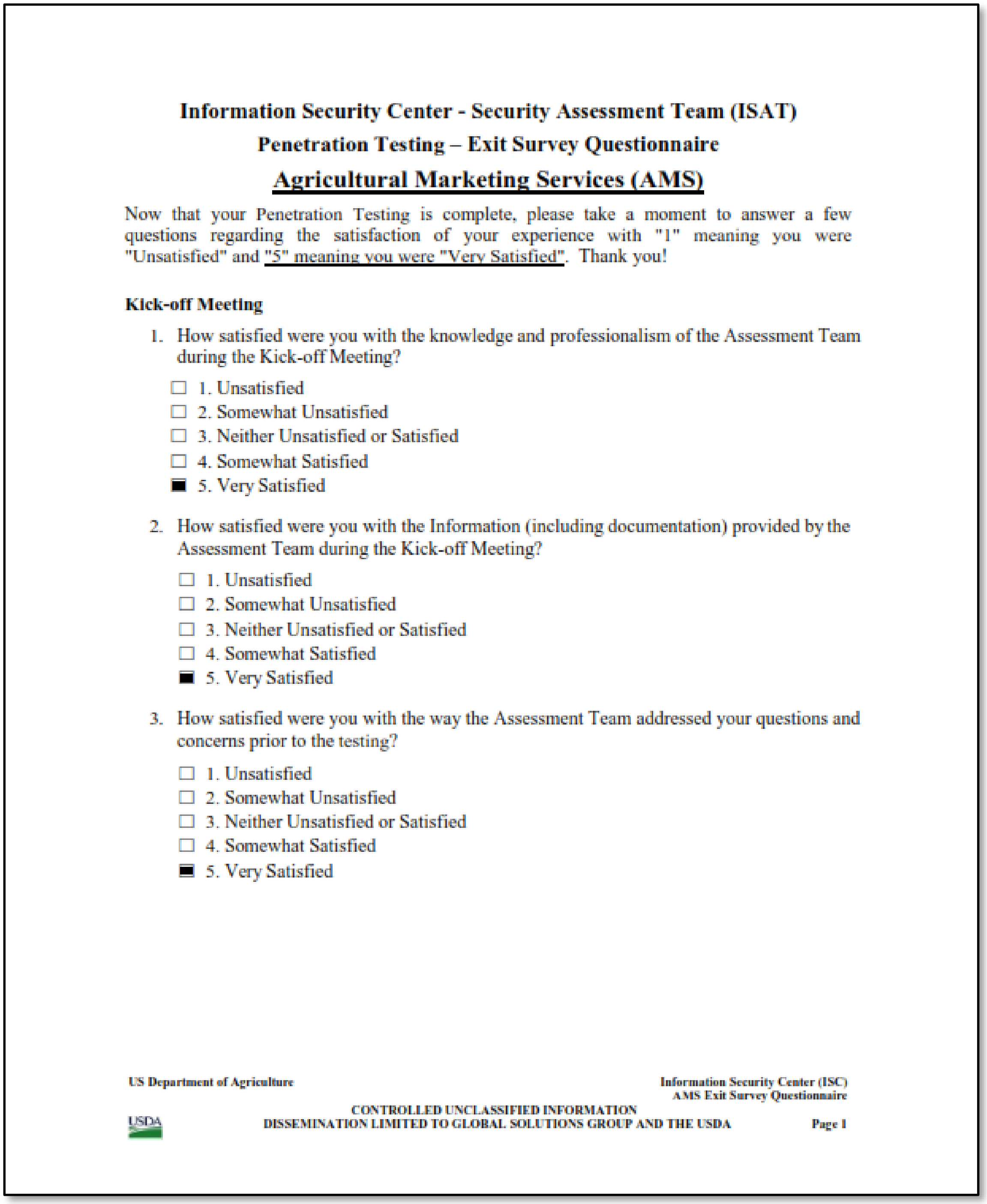
CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA

USDA

Page 4

8.4.3 AMS - Information Security Center – Security Assessment Team and 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

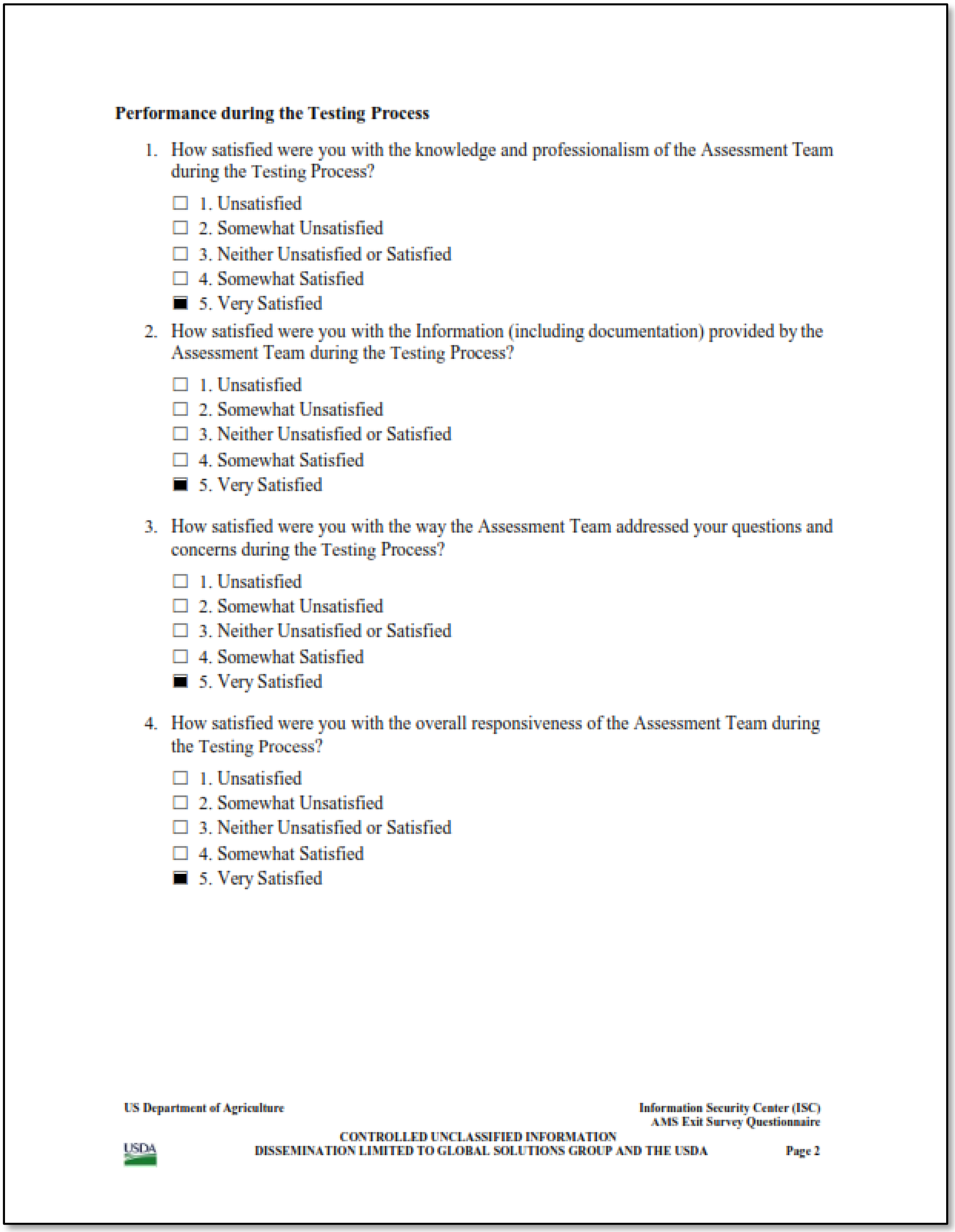
US Department of Agriculture

Information Security Center (ISC)
AMS Exit Survey Questionnaire

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

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?

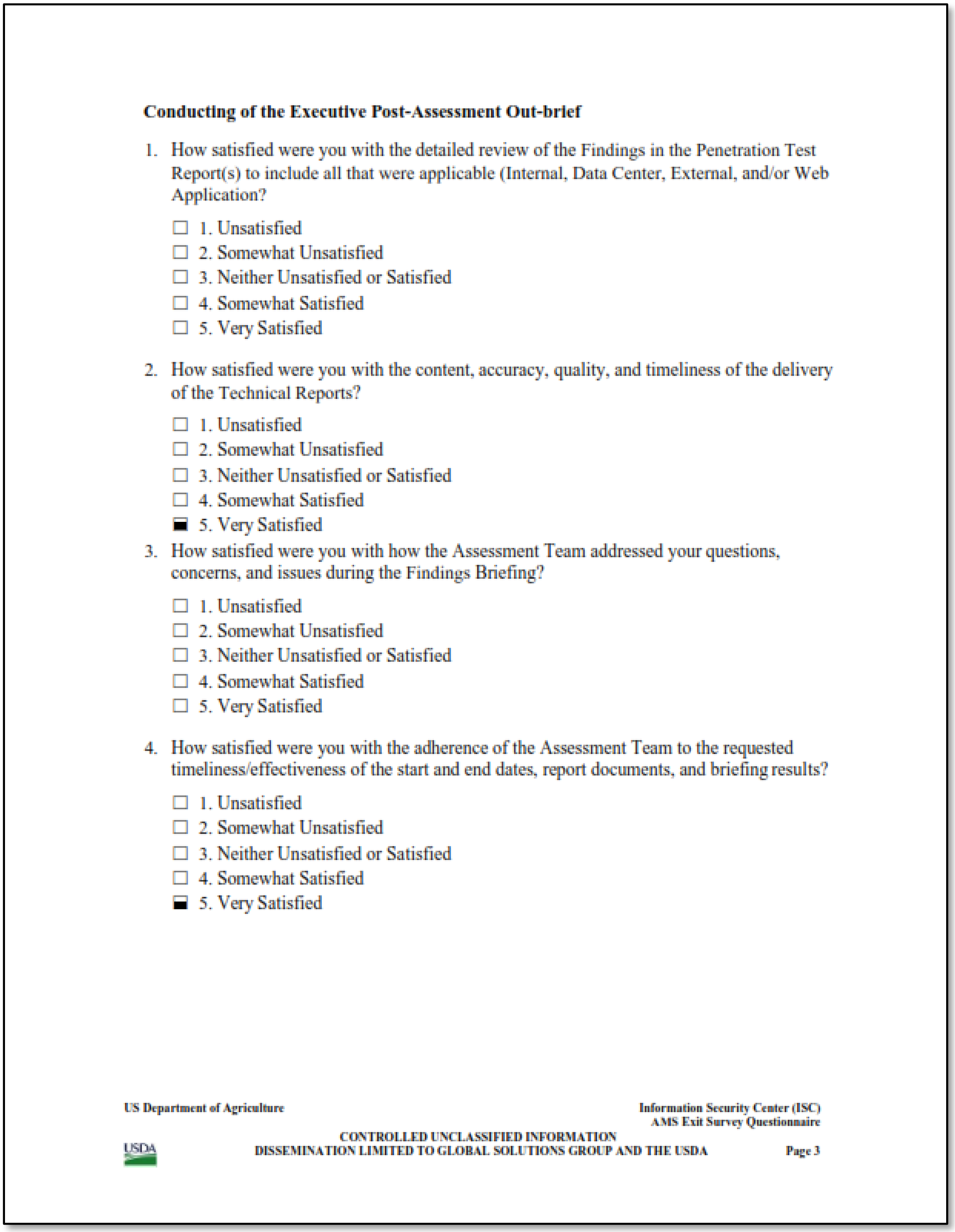
   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

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?

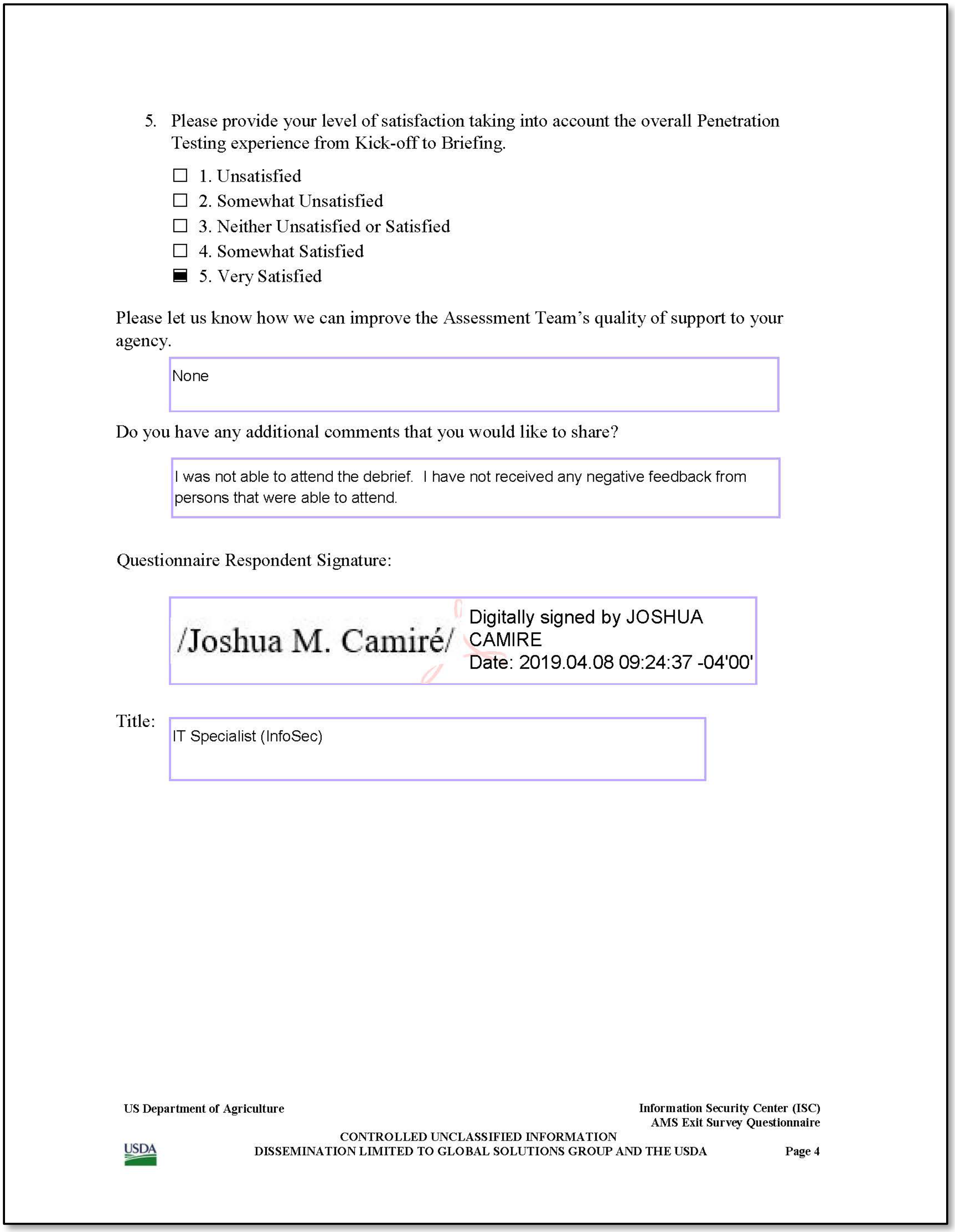
   □ 1. Unsatisfied
   □ 2. Somewhat Unsatisfied
   □ 3. Neither Unsatisfied or Satisfied
   □ 4. Somewhat Satisfied
   ■ 5. Very Satisfied

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 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.

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)

US Department of Agriculture

Information Security Center (ISC)
AMS Exit Survey Questionnaire

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

USDA

Page 4

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 web services
Partner Network