

RESOLUTION NO. 22 – 18

**RESOLUTION OF THE NEW JERSEY INFRASTRUCTURE AUTHORIZING
THE AWARD OF A CONTRACT FOR AN INFORMATION TECHNOLOGY MANAGED SECURITY SERVICES
PROVIDER**

WHEREAS, the New Jersey Infrastructure Bank (“I-Bank”) is authorized to make and enter all contracts necessary or incidental to the performance of its duties pursuant to N.J.S.A. 58:11B-5(d);

WHEREAS, at its August 13, 2020 meeting, the Board of Directors of the I-Bank (“Board”) approved Resolution No. 20-50 authorizing the Executive Director to prepare and distribute a Request for Proposals (“RFP”) for the appointment of an Information Technology Managed Security Services Provider (“IT MSSP”);

WHEREAS, the I-Bank distributed an RFP for the appointment of an IT MSSP for a two-year period with an option for two additional one-year periods upon approval of the Board in accordance with the I-Bank Policy No. 4.00 Purchase of Goods and Services;

WHEREAS, the RFP solicited proposals and enumerated the criteria and associated weights to be applied in the evaluation process;

WHEREAS, the I-Bank received two proposals, both of which were compliant with the requirements of the RFP; and

WHEREAS, the Executive Director of the I-Bank appointed an Evaluation Committee (“Committee”) consisting of three I-Bank staff members to review and score the proposals;

WHEREAS, the Committee members independently reviewed and ranked the proposals;

WHEREAS, Committee members’ rankings were tabulated and the highest ranking firm was invited to make a Best and Final Offer (“BAFO”). The Committee recommended that the contract for IT MSSP be awarded to MGT of America (“MGT”);

WHEREAS, the Executive Director concurred with the recommendation of the Committee and recommends that the I-Bank engage MGT to serve as I-Bank’s IT MSSP.

NOW THEREFORE, BE IT RESOLVED that the I-Bank Board selects and appoints MGT as the IT MSSP, and conduct the scope of work set forth in the RFP, which appointment shall be for a two-year period with the option to extend for two one-year periods upon approval by the Board (“Contract Term”) and contingent upon the subsequent execution by all parties of an agreement substantially in the form presented to this meeting, which is hereby approved; provided that the Chairperson, Vice-Chairperson, and Secretary of the I-Bank are hereby authorized, with the advice of the State Attorney General, to make such changes, insertions and deletions to and omissions from such form as may be necessary or appropriate; and

BE IT FURTHER RESOLVED, the Executive Director is hereby authorized to send a confirming letter to MGT confirming its appointment as the I-Bank’s IT MSSP for the Contract Term described above; and

BE IT FURTHER RESOLVED, the Chairperson, Vice-Chairperson, and Secretary of the I-Bank are hereby authorized to execute and deliver such agreement, substantially in the form of the agreement authorized by the Attorney General, with MGT. The terms and conditions of that agreement shall include but not be limited to:

- a. The provision of services as outlined in the I-Bank’s RFP distributed on January 12, 2022;
- b. The payment for all services and fees as detailed in the proposal submitted by MGT dated February 25, 2022 as modified by MGT’s best and final offer submitted on March 2, 2022; and
- c. Such other terms and conditions as may be contemplated by the RFP and the materials enclosed therewith as deemed necessary and appropriate by the Chairperson, Vice-Chairperson, or Secretary of the I-Bank.

Adopted Date: March 10, 2022

Motion Made By: Mr. Mark Longo

Motion Seconded By: Mr. Jack Kocsis

Ayes: 8

Nays: 0

Abstentions: 0

Proposal

FEBRUARY 25, 2022



Submitted by:

ALTON KIZZIAH

EVP & GM, TECHNOLOGY SOLUTIONS GROUP

4320 West Kennedy Boulevard
Suite 200

Tampa, Florida 33609

813.327.4717

Akizziah@mgtconsulting.com

IT Managed Security Services Provider

NEW JERSEY INFRASTRUCTURE BANK



Letter of Transmittal

February 25, 2022

David E. Zimmer
Executive Director
New Jersey Infrastructure Bank
3131 Princeton Pike, Building 4, Suite 216
Lawrenceville, NJ 08648

Dear Mr. Zimmer:

MGT of America (MGT) is a recognized leader as an IT managed security service provider (MSSP). We provide holistic, cost-effective solutions to financial institutions, public education districts, state and government organizations, and other public sector enterprises. Through our unparalleled Technology Solutions Group, we are committed to partnering with the New Jersey Infrastructure Bank (the I-Bank) to provide you with proactive short-term and long-term IT management and supplemental services to support your business goals, operations, and IT-related functions.



We trust that as you review the details presented on the following pages you will agree that MGT can meet and exceed your managed services requirements. **If successful, MGT will be the Prime Contractor performing all IT managed service projects in partnership with the I-Bank's in-house information technology department.** If you have any questions regarding our services or pricing, please contact our Project Director, Alton Kizziah, at (813) 327-4717, or Akizziah@mgtconsulting.com. We hope to have the opportunity to help you ensure a safe, private, and secure environment for the staff, investors, customers, and community of the I-Bank.

Sincerely,



Patrick J. Dyer
Vice President



Table of Contents

- BUSINESS INFORMATION 8**
 - MGT BACKGROUND AND CAPABILITIES 8
 - FINANCIAL CAPABILITY 9
 - MGT BRINGS THE I-BANK OUR UNMATCHED CAPABILITIES 12
 - FINANCIAL INSTITUTIONS AND MSSP EXPERTS 13
 - COMPLIANCE 13
 - MGT’S EXPERT CERTIFIED AND QUALIFIED STAFF 14

- METHODOLOGY AND APPROACH 17**
 - MANAGED NETWORK SERVICES 17
 - MGT’S EXCEPTIONAL, TAILORED MDR SOLUTION 18
 - NETWORK ADMINISTRATION SERVICES 21
 - SERVER ADMINISTRATION SERVICES 22
 - DESKTOP AND HELP DESK SERVICES 23
 - SECURITY ASSET MONITORING 24
 - CYBERSECURITY PROTECTION 26
 - STRATEGIC PLANNING 30
 - SERVICE LEVEL AGREEMENTS: 31
 - PROJECT GOVERNANCE AND COMMUNICATION PLAN 33
 - POTENTIAL CHALLENGES 34

- EMERGENCY PREPAREDNESS PLAN 37**

- EXPERIENCE AND REFERENCES 40**

- APPENDIX A: RESUMES 44**

- APPENDIX B: ISO CERTIFICATE 65**

- APPENDIX C: FINANCIAL STATEMENTS 66**

- APPENDIX D: REQUIRED FORMS 84**

Business Information

MGT Background and Capabilities

Founded in 1974, MGT provides comprehensive IT Managed Services to financial systems, public sector organizations, and state agencies to help them achieve high-value, transformational change through our capabilities and industry knowledge. We have served over 13,000 clients across the United States through our ISO 27001-certified, US-based, 24x7 SOC operated by over 100, on-staff, cyber security engineers.

Making a profound impact on your organization and community is at the heart of who we are and what we do.

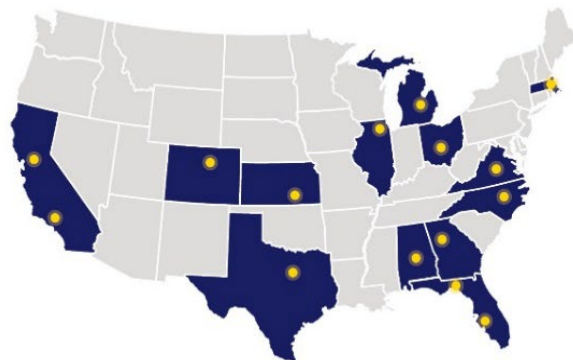
CONVENIENT LOCATIONS

Incorporated and headquartered in Tampa, Florida MGT has grown exponentially in the past 47 years. Our experience is synonymous with excellence in quality and delivery.

MGT's offices are located throughout the United States. Our offices are staffed with 220+ full time employees, including a full marketing and HR department. Our office located in Tampa, Florida will be the principal and responsible office fulfilling all terms of contract.

NATIONAL FIRM LOCAL FOCUS

ALABAMA Montgomery	KANSAS Wichita	OHIO Columbus
CALIFORNIA Sacramento Pasadena	ILLINOIS Chicago	TEXAS Dallas
COLORADO Denver	MASSACHUSETTS Boston	VIRGINIA Richmond
FLORIDA Tallahassee Tampa	MICHIGAN Bay City	
GEORGIA Atlanta	NORTH CAROLINA Raleigh	



The MGT Difference

We have worked with thousands of public entities around the world supporting managed cyber security improvements in every aspect of performance and organization. MGT has successfully delivered more than 13,000 projects through a careful balance of addressing the immediate needs of our clients, while maintaining the vision and direction toward their short- and long-term goals and monitoring industry best practices Our focus is on:

- ◆ Tailored services to the client requirements and cost-efficient solutions
- ◆ Strategy and tactical execution customized to the public sector
- ◆ Flexibility and a vendor agnostic philosophy to adapt to public sector needs and resources
- ◆ Deep bench of security experts to address the talent shortage the public sector faces

Financial Capability

As a long-standing contractor, MGT has the financial capacity to undertake and complete a project of this scope. MGT has been in continuous business since 1974 and has the necessary financial ability to perform the functions required by this RFP and to provide those services represented in this response. MGT does not anticipate any organizational changes or have any conditions that may impede our ability to complete any future projects. We have over 47 years of experience in providing sound, practical, implementable solutions to state and local governments around the country. In addition, MGT has not been involved in any litigation or court proceedings whereby a court or any other administrative agency has ruled against MGT in any matter related to the professional activities of our firm. A copy of our audited financial statement for the most recent fiscal year has been provided in the Appendix section. Also, there has been no litigation, major disputes, contract defaults or non-ordinary course of business liens against or involving MGT of America Consulting, LLC during the period. Further, MGT of America Consulting, LLC is not aware of any potential or contemplated actions, disputes, defaults, or liens.

The last 12 months of revenues directly related to providing MSSP services is detailed below:

- 24x7MDR & MSSP Rev: 62%
- One-time implementation engineering services: 28%
- Hardware/Software: 8%
- Other: 2%
- 5%-10% of our company's revenue is spent on MSSP and MDR Research and Development, varying by year. MGT's SOC also houses a cyber security lab that serves as a testing field for assessing software and hardware solutions against the latest threat intel landscape. This serves as a springboard to incorporate the most efficient solutions on our clients' monitoring environment while training and security engineers on the latest threats.



Defined by Impact

We are committed to fully aligning with the I-Bank and how we maximize social impact to your community. As part of our IT Managed Services in response to this RFP, we will provide holistic IT services to assist with future upgrades to your IT infrastructure that promotes network protection, data security, and performance maximization of the overall information system, enabling the I-Bank to continue driving your two-generation education model to put your students and parents on a path to

Our Social Impact and IT Managed Services

HOW HAS MGT IMPROVED COMMUNITIES WITH OUR SOCIAL IMPACT?

- ✓ 24x7 Managed Detection and Response at school districts across the nation protecting the students on an on-going basis

BUSINESS INFORMATION

- ✓ Providing leading HBCU's such as Tuskegee University with a full network refresh and 24x7 monitoring leading to an enhanced on-campus student experience with technology, while remaining protected
- ✓ Assessments and penetration testing with several international airports in the US ensuring their environment is not disrupted by bad actors affecting travelers.

Authorized Point of Contact

For any questions regarding contracts, our qualification, pricing, or our IT managed services, we would be delighted to answer any questions. Below we have provided contact information as well as our authorized representatives and main point of contact.



MGT Headquarters

4320 West Kennedy Boulevard,
Suite 200
Tampa, FL 33609 5
P: 813.327.4717
proposals@mgtconsulting.com
Tax Identification #: 81-0890071



Security Operations Center

5755 North Point Parkway
Suite 82
Alpharetta GA 30022
proposals@mgtconsulting.com
ISO 2700:1 Certified



Authorized Representatives

Patrick J. Dyer
Executive Vice President

A. Trey Traviesa
CEO and Chairman of the Board



Point of Contact

Alton Kizziah
EVP & GM, Technology Solutions Group
4320 West Kennedy Boulevard, Suite 200
Tampa, FL 33609
P: 813.327.4717
Email: Akizziah@mgtconsulting.com

For any specific questions regarding contracts, please contact Alton Kizziah, EVP & GM of our Technology Solutions Group.

Strong Presence in New Jersey's Public Sector



MGT's education practice has provided a variety of planning, analysis, research and strategic services as part of master planning engagements for PK-12 and higher education entities across the country. We are proud to have a long history in New Jersey, supporting public sector education organizations. Below is a list of our current clients for whom we have completed cyber security services:

NEW JERSEY

New Jersey Commission on Higher Education
Ramapo College of New Jersey
The Richard Stockton College of New Jersey
Thomas Edison State College

Our Clients

MGT's ability to excel has been driven by our expertise, quality, and our commitment to exceeding client expectations. Part of MGT's success is based upon our promise to be flexible and clients to the highest degree. We have provided Managed IT services to enable our clients to align with their mission and vision to serve their communities effectively and safely.

“What I liked most about working with MGT staff is their creative approach in providing solutions to each project. The County has implemented MGT's recommendations...”

Lisa Davidson
Director of Human Resources
York County, South Carolina

A 47-year focus on driving innovation through educating the student, parent, staff, and community.

“We partner with clients to advance and lift up the communities they serve.”




MGT Brings the I-Bank Our Unmatched Capabilities

MGT’s Cyber Solutions team will be a true extension of the I-Bank’s IT team. Our goal is to partner with your team to bring tailored managed security solutions leveraging the latest enterprise-grade security services to the I-Bank’s organization. Per the scope of this RFP, we will help the I-Bank navigate risk, capitalize on opportunities, and achieve successful outcomes as needed.



Flexible Managed Security Solutions. Deep Engineering Expertise. On Your Terms.

Whether you need hands-on cyber security engineering and remediation work, 24x7 network monitoring, full firewall management capabilities, or require a complete managed security program, our flexible suite of security solutions are meant to augment your internal capabilities to fight threat adversaries on an on-going basis. We’ll be in the security trenches with you.

 <p>Managed Detection & Response</p>	 <p>Next-Gen Firewall Management</p>	 <p>Assessments & Testing</p>	 <p>Compliance Programs</p>	 <p>Staff Augmentation</p>	 <p>Professional Services</p>
---	---	--	--	---	--

24x7 Managed Detection & Response

- Real-time threat hunting to identify, detect and intercept cyber attacks
- Full visibility and live protection of your entire environment through our 24x7 Security Operations Center
- Dedicated team for on-going guided remediation of identified vulnerabilities
- Monthly strategic security reviews and security KPIS

Next-Gen Firewall Management Experts

- End-to-end NGFW management (procurement through long-term management)
- 24x7 alert and monitoring from our Network Operations Center
- Certified engineers across all major OEMs to optimize firewall performance and configuration reporting and KPIS
- Monthly security and performance

Assessments & Testing

- Actionable NIST-based security assessments with tangible remediation guidance
- Comprehensive pen testing team with the needed expertise to apply organizational context to testing engagements (red, blue and purple team)
- Social Engineering exercises to mitigate the “human” threat

Compliance Programs

- HIPAA, PCI, CJIS, IRS p 1075 compliance programs.
- We help you manage your compliance requirements through a consolidated compliance advisor program that integrates with your security governance strategy
- Full audit and remediation management and support

Staff Augmentation

- Recruitment precision by security experts to match your technical needs
- Short-term and long-term engagements
- On-going vetted pool of cyber security experts with guaranteed performance

Professional Services

- Over 100 cyber security engineers on staff providing a full suite of sec ops professional services
- Flexible engagement structures to adjust to your operational needs
- Experience across all security domains and major OEMs
- 24x7 availability

Financial Institutions and MSSP Experts

MGT has the experience and capacity to support the I-Bank across the entire scope of work as presented in the RFP. MGT currently is partnered with multiple financial systems IT teams, quasi-governmental entities, transportation and municipal agencies, commercial companies, public-sector organizations, school districts, higher education institutions, and state governments across the United States to help them achieve high-value, transformational change through our capabilities and industry knowledge, all powered by technology.

We bring a unique angle to our IT services. Whether it is getting training on specific technical functions around hardware and software solutions, our deep bench allows us to help you become a security center of excellence.

Compliance

We are ISO 27001 certified and comply by the highest level of standards in information security governance.

Policies include, but are not limited to:

<p><u>On-going Cybersecurity Policies and Procedures</u></p> <ul style="list-style-type: none"> Anti-Virus Software Policy Backup Data Policy Confidential Data Policy Data Classification Policy Data Loss Prevention Policy Data Security Audit Policy Guest Access and/or Third-Party Connection Policy Network Security Policy Online Currency Collection Policy Physical Security Audit Policy Physical Security Policy Recover Time and Recovery Point Policy Remote Access and/or Virtual Private Network (VPN) Policy Retention Policy Sensitive Data Protection and Encryption Policy 	<p><u>Staff Cybersecurity Policy Acknowledgments</u></p> <ul style="list-style-type: none"> Acceptable Use Policy Data Security Training Policy Email Policy Employee Termination Security Policy Mobile Device / Bring Your Own Device (BYOD) Policy Website Privacy Policy and Customer Notice Policy Network Access Policy Password Policy Staff Social Media Conduct Policy Wireless Policy
<p><u>Cybersecurity Breach Protocol</u></p> <ul style="list-style-type: none"> Breach Notification Policy Business Continuity Plan Formalized Incident Response Plan 	<p><u>Cybersecurity Post-Breach Protocol</u></p> <ul style="list-style-type: none"> Disaster Recovery Plan Post-Breach Investigation Policy

Any information provided by the I-Bank because of this engagement will be considered confidential and will not be released unless otherwise contracted with the participant or required by law. MGT will ensure once collected, data are securely stored in a locked area and are accessible only to authorized personnel (i.e., members of the MGT team). Names associated with raw data will be replaced at the first opportunity by a letter or numerical coding system. All reports will use a coded system of references; no identifying information, which could directly or inadvertently breach confidentiality, will be used. Participants will be made aware of the arrangements in place to ensure confidentiality of data, the length of time the data will be retained and the purpose(s) for which the data will be used. MGT also will advise participants of any plan to allow access to the aggregated, anonymous data by others. When no longer required, data will be destroyed in a manner, which protects the participants' identities (e.g., shredding of records, erasing of tapes, etc.).

PRIVACY ACT SAFEGUARDS

MGT's procedures for maintaining Privacy Act safeguards in collecting, maintaining, using, or disseminating data are detailed below.

MGT will maintain Privacy Act safeguards as required under 5 U.S.C. 552a(m) with respect to such data. We will adhere to the Department of Education's *Handbook for the Protection of Sensitive But Unclassified Information*, OCIO-15, and other Department policies related to collecting, maintaining, using, or disseminating data. MGT's employee policies include the requirement that all employees (and subcontractors, if applicable) sign an employee acknowledgement form as well as an Individuals with Disabilities Education Act and Family Educational Rights and Privacy Act Confidentiality Agreement to ensure the non-disclosure of confidential information.

MGT will:

- ◆ Safeguard all electronic files using permissions to allow only password-protected team member accounts with access.
- ◆ Ensure that all team members' (and subcontractors) have password-protected screen savers that will initialize after 10 minutes of inactivity.
- ◆ Ensure our data center is in a secure, locked room with access only by the corporate network administrators.

Our Security Operations Center is US Based ISO 27001 Certified. We have provided the certificate in the Appendix section.

Our ISO 27001 documentation is available upon request for auditing purposes.

MGT's Expert Certified and Qualified Staff

MGT's in-house team includes 100+ IT engineers with dedicated, certified teams with the key skills, knowledge, and experience needed to ensure a successful IT Managed Service deliverables to the I-Bank. Many of MGT's certified, subject area specialists have worked in leadership positions at state and local government agencies, PK-12 public sector, universities, community colleges and other public sector organizations. They have first-hand experience in the challenges encountered when delivering innovative solutions to the technology and organizational needs of public sector and financial organizations, achieving results efficiently and effectively.

Recruitment, Certifications and Training

At MGT, we adhere to a very stringent candidate pre-screening process, developing a highly qualified pipeline of security professionals to meet various business needs. Once we have identified a suitable candidate, our team will:

- ✓ **HR background check**
- ✓ **Initial "company culture" interview**
- ✓ **Scenario-based technical interview including incident identification, response, through containment and remediation**
- ✓ **Solution-stack technical interview**
- ✓ **Certifications verification**

BUSINESS INFORMATION

- ✓ **“Business” interview. (How does security impact business performance?)**
- ✓ **On-boarding training plan**
- ✓ **Long-term training plan**
- ✓ **OKR-based goals**

All SOC analysts go through an FBI background check. If the candidate has a criminal conviction of any nature, it is our policy to determine if it would materially interfere with or pose an unacceptable safety risk about the performance of the employee’s job duties or is part of an ongoing and sustained pattern of illegal conduct. If such determination is made, the offer of employment will be rescinded.

All team members are certified in their respective fields with an average 20+ years’ experience on enterprise-scale managed security projects. Certifications held by our security staff include, but are not limited to:

- ◆ AWS- Cloud practitioner
- ◆ Certified Information Systems Security Professional
- ◆ Microsoft Certified Azure Fundamentals
- ◆ Microsoft certified Azure fundamentals AZ-900
- ◆ Microsoft certified Azure Administrator- AZ-104
- ◆ Check Point Certified Security Associate
- ◆ Check Point SandBlast Agent Specialist
- ◆ Check Point Cloud Guard SaaS Administrator
- ◆ Zscaler certified cloud administrator Internet Access
- ◆ Zscaler certified cloud administrator Private Access
- ◆ ZScaler- ZCCA-IA Security specialist
- ◆ Logrhythm (LRSALRPA)
- ◆ Rapid7 Insight IDR certified
- ◆ Extrahop certified
- ◆ Check Point Certified Expert
- ◆ Cisco Certified Network Associate Security
- ◆ Cisco Certified Network Associate Routing and Switching
- ◆ Cisco Certified Network Professional, CCNP Switch
- ◆ Palo Alto Networks Certified Networks Certified Network Security Engineer (PCNSE)
- ◆ Palo Alto Certified Engineer, ACE 8.0
- ◆ Fortinet NSE Professional Certified
- ◆ Juniper Networks Certified Internet Associate
- ◆ Splunk
- ◆ Certified Ethical Hacker
- ◆ CompTIA Security +
- ◆ Lean Six Sigma White Belt
- ◆ McAfee – ePO, ENS
- ◆ Authorized Support – Proofpoint

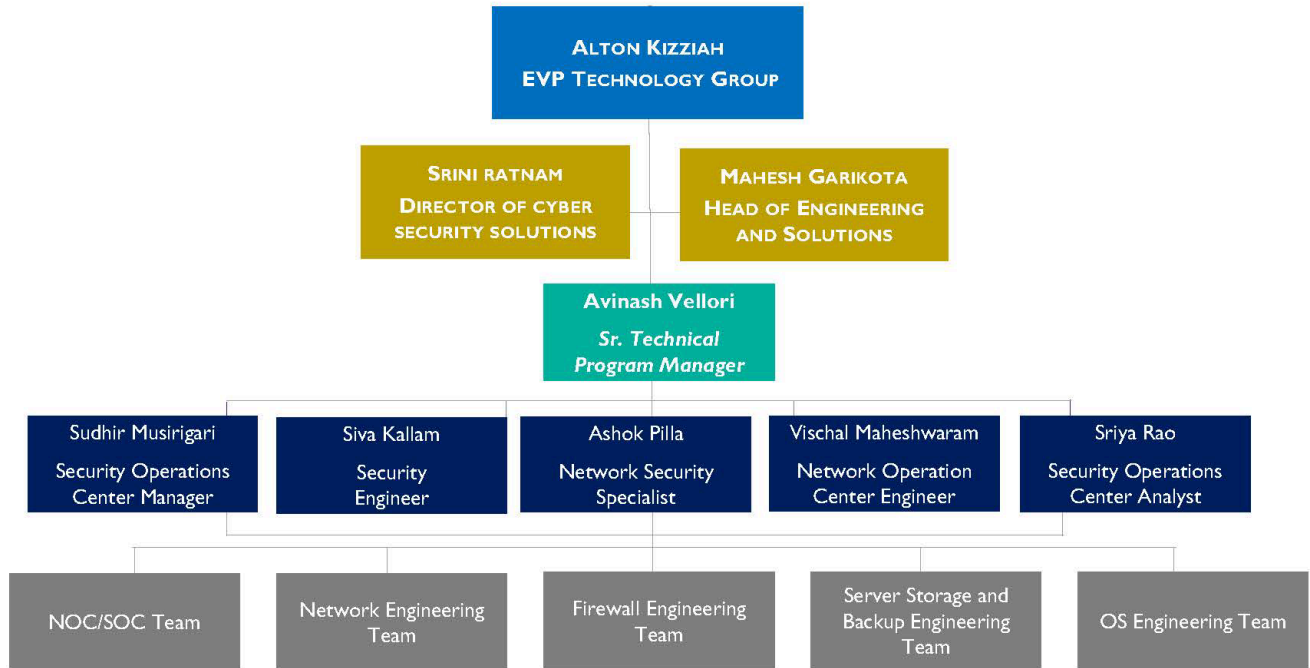
100% of the Cyber Security team supporting BPHC will be US-based with legal resident status. We do not have specific citizenship requirements for our SOC staff. We comply fully with all E-verify procedures to hire employees with proper work authorization as per DHS/USCIS. All SOC staff undergo extensive FBI background check including CJIS clearance.

We have over 100 qualified and certified IT security professionals on staff. Resumes have been provided in Appendix B for all key management and delivery personnel who will be proposed for this engagement:

We require mandatory, period cybersecurity awareness training as well as providing new vendor on-boarding training fall security monitoring staff.

Most of our analysts have more than 10 years of direct experience and the average employment time of an MSSP/MDR Analyst with our company is over 5 years employment.

The ratio of monitored customers to personnel is 1 (customer): 7 (analysts). The ratio of managed security devices to personnel is approximately 7,000.



Project Team Resumes

Resumes for key management and delivery team members are provided in an Appendix to express our team’s expertise to provide the I-Bank the services requested in the RFP. MGT’s personnel are professionals who will provide expert services for this project. *If for any reason, a team member needs to be replaced, MGT has the resources to quickly identify and orient an equally qualified professional and continue delivery on the project uninterrupted.*

Methodology and Approach

Our mission is to bring tailored managed information technology services leveraging the latest enterprise-grade security products the I-Bank. We are committed to partnering with your in-house IT teams to harden your security posture and ensuring that all key constituents across your organization (students, educators, staff, parents, and the community at large) are protected. With our half a century technology experience and our long-term involvement in the State of Texas we look forward to expanding our commitment as needed to the I-Bank.

In response to the RFP scope of work, we will provide the following services to the I-Bank. During project kick-off we will discuss with you the rules of engagement of the specific project, personnel roles and responsibilities, and finalization of the work plan and schedule.

Managed Network Services

MGT’s managed network services are specifically designed around the unique needs your organization. Our services are delivered from our Network and Security Operations Center in Alpharetta, Georgia where we monitor your critical systems for anomalous patterns and take immediate action whenever trouble is detected. MGT can also augments existing network infrastructure staff to provide a level of coverage that would otherwise be impractical or unaffordable. Our network experts have broad experience, ongoing training, and access to cutting edge tools and the world’s most up-to-the-minute threat databases.



Our 24/7/365 services will improve your security profile, reduce your costs, and help you drive risk out of your systems. MGT’s managed network services include:

- ◆ Continuous monitoring of network, systems, and data.
- ◆ Incident response and recovery.
- ◆ Security software installation, configuration, and management.
- ◆ Technical support for device installation and moves.
- ◆ Regular security health assessments and reporting.
- ◆ Digital forensic support.

MGT's Exceptional, Tailored MDR Solution

MGT Proposes Industry Leading (Gartner's Magic Quadrant Leader) SIEM Solution Rapid7 InsightIDR as SIEM Solution bundled with MGT Intelligent Security Center from our 24x7 Monitoring & Response Team

The Solution includes Hybrid AWS Cloud Hosted instance with 1 Year Retention (3 Months Hot Dataset which can be retrieved in less than 10 minutes and 9 Months in Cold retention which we can retrieve in less than 2 hours). In the event St Lucie has longer data retention requirements, MGT shall appropriately provide solution with additional storage in the AWS Cloud.

MDR solution has the following essential components:

(1) InsightIDR Collector: (Installed On-Prem using VM Ware or Hyper V)

The Collector is the on-premises component of InsightIDR, on St Lucie network running Rapid7 software that polls data and receives data from Event Sources and makes it available for InsightIDR analysis. An Event Source represents a single device that sends logs to the Collector. A VM can be provisioned as Collector. We recommend deploying Collectors based on the network topology of St Lucie. At a minimum we shall have 2 Collector per site for fault tolerant. We expect St Lucie to provision the VM resources while MGT shall install the software and configure the software as well as monitoring 24x7.

(2) Data Collector for Log Collection from Firewalls, Routers and Switches: (Installed On-Prem using VM Ware or Hyper V)

The Collector is the on-premises component of InsightIDR. All Syslog's from Firewalls, Routers and Switches across both the Data Centers are forwarded to Dedicated Data Collector. We recommend one syslog collector at each data center.

(3) Insight Agent (Installed on all Servers at Both the Data Centers)

The lightweight Agent is deployed on all Servers and Desktops/Laptops owned by St Lucie at Data Centers as well as campus. We recommend deploying the agents using software distribution package utility or GPO.

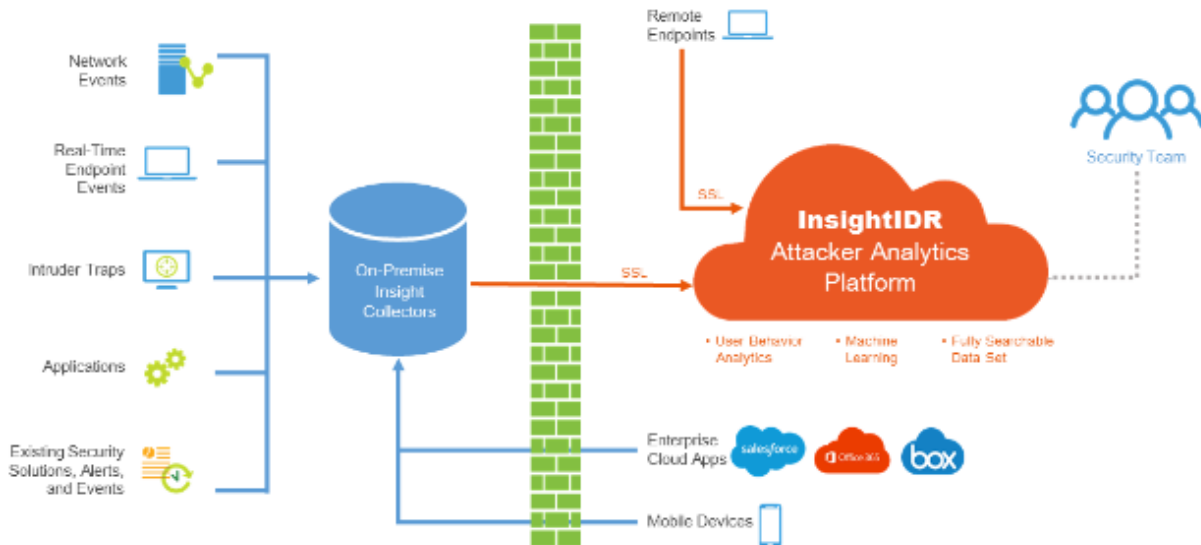
(4) Cloud Deployments (Configured on the Cloud and Integrated with On Prem DC)

Rapid7 InsightIDR can be deployed in the Cloud including Microsoft Azure and AWS and integrated with the on-prem data collectors so the InsightIDR Dashboard process this as one single event. Along with this MGT shall integrate cloud/SaaS applications into monitoring either through native log or custom log ingestion and the goal is to have maximum visibility leveraging logs across all the sources whether on prem or Cloud.

MGT shall be responsible for the implementation and management of the solution at the I-Bank on a 24x7x365 basis from our US-based Intelligence Security Operations Center for 24x7 threat monitoring alerts and policy exceptions (security events) generated by the MDR platform. As alerts come in and analysis by our SOC analysts is performed, security events may be classified as security Incidents and assign appropriate priority. Whether a security event is considered a security incident is determined solely by MGT. Identified security events will be classified, prioritized, and escalated as MGT deems appropriate in coordination with the I-Bank team. Security events that are not eliminated as benign triggers are classified as a security incident.

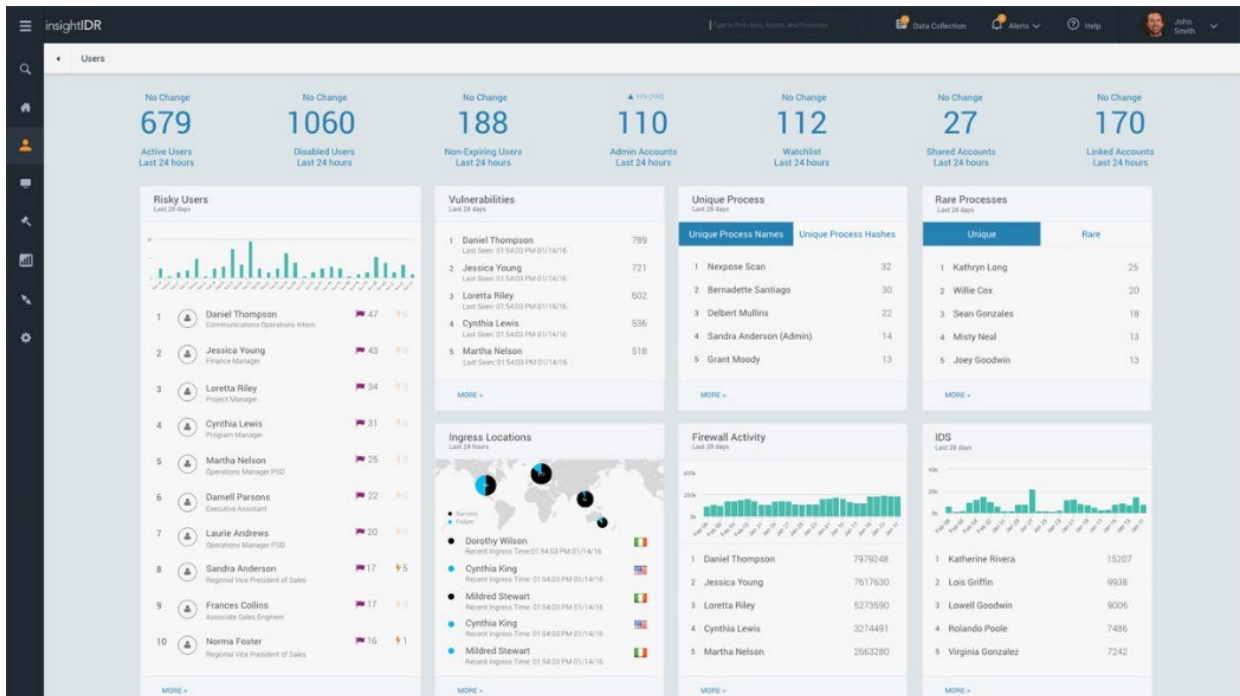
InsightIDR Architecture

insightIDR



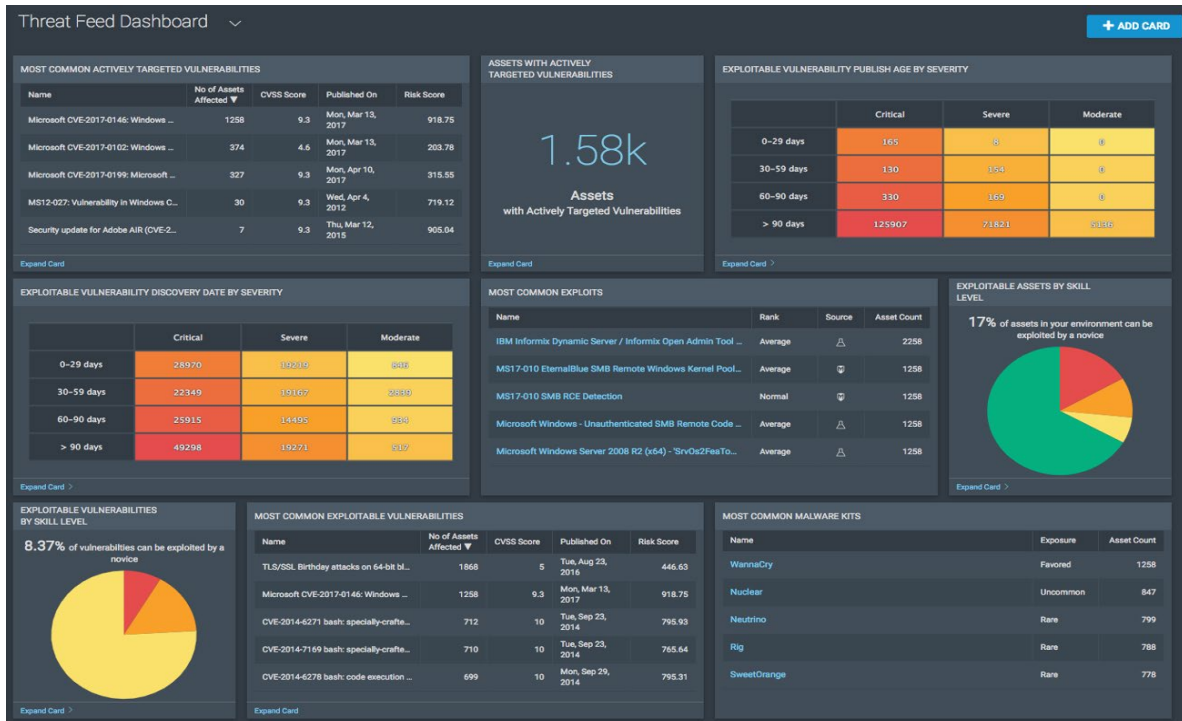
RAPID7

- ◆ Threats can be used to track indicators of compromise, also known as "IoC." Our MDR Solution enables creating customized threat definitions, as well as leverage other community threats to add to the I-Bank's defenses. All of these can be viewed through a single pane of glass and a dashboard.



METHODOLOGY AND APPROACH

- ◆ All Threat Intelligence is further contextualized by InsightIDR with the user, asset, account, and behaviors associated with the time frame the IOC was seen.
- ◆ Threat intelligence feeds that will match process activity, firewall logs, DNS logs, and web proxy logs against hashes, IP, domain name and URL can be configured in InsightIDR via the threat community function. The user can either subscribe to Rapid7 threat feeds, customer-generated feeds, or can create their own by inputting in hash, IP, domain name, and URL manually, or by uploading a .csv or STIX-formatted .xml file or via API key.
- ◆ Rapid7 proactively notifies customers in-app and via email when threat intelligence relating to particularly notable threats (e.g., WannaCry, Not Petya) has been delivered.
- ◆ InsightIDR automates the ingestion of a wide variety of Threat Intelligence -- both industry threat intel (ISACs) and commercial grade threat intel feeds -- through an API. Rapid7 also provides our customers additional Threat Intelligence (i.e., FBI Liaison Alert System) to augment any intelligence they already consume, as well as a community element for customers to opt to share IOCs they are discovering on their own. All Threat Intelligence is further contextualized by InsightIDR with the user, asset, account, and behaviors associated with the timeframe the IOC was seen. These are visible in the Threat feed dashboard of the console.



- ◆ Advanced analytics rules for InsightIDR are maintained by Rapid7 engineering. Our cloud deployment model enables us to prototype detection methods, based on our own research and what other users are witnessing, for new intruder techniques and test these methods against the dataset of our entire user population. After verifying they work properly with few false positives, we deploy them to customers.
- ◆ InsightIDR integrates with 3rd party offerings (both public and private threat feeds) to identify suspicious processes, URLs, hosts, and IPs. The frequency of threat intelligence feeds varies by source.
- ◆ InsightIDR comes standard with Deception Technology that creates an illusion for attackers and makes it easy to set intruder traps such as honey pots, honey users, honey files, and honey credentials to detect intruders when they are initially exploring the network before they have had a chance to do damage.

METHODOLOGY AND APPROACH

- ◆ The intruder traps included in InsightIDR are quick to set up and were built based on Rapid7's extensive knowledge of attacker behavior. This comes from continuous attacker research via the Heisenberg Project and Project Sonar, the Metasploit project, our pen testers, and our 24/7 SOC.
- ◆ The evidence panel can display the raw packet data seen by a honeypot, providing a new viewer that displays both formatted ASCII as well as a hex binary view of the raw data. This allows users conducting an investigation to know what the honeypot saw that triggered the alert.

Network Administration Services

Maintaining your network infrastructure and addressing operational IT needs requires experienced network engineers who are familiar with your environment and your business. MGT's in-house team includes 100+ cyber security engineers with dedicated, certified teams understand the latest network infrastructure components. We provide complete lifecycle management, from procurement through long-term management. Additionally, we can provide 24x7 monitoring, event management, incident management, change management configuration backup, reporting, hardware and software inventory, and service delivery management on request.

We can solve small and large problems with:

- ◆ Software, including system updates
- ◆ Connecting printers, routers, and home Internet access
- ◆ Hardware malfunctions
- ◆ Backing up or moving files

In addition, we provide comprehensive support of wired and wireless networks, guaranteeing the continuous performance of network infrastructure for both small and large companies.

- ◆ Supporting network wired environment (LAN, including Data Center Solutions)
- ◆ Supporting sites' connectivity environment (WAN)
- ◆ Supporting network wireless environment (WLAN)
- ◆ Supporting voice (including Voice over IP) solutions (VOIP)
- ◆ Supporting network infrastructure services systems (DNS, DHCP, NTP, etc.)
- ◆ Supporting traffic management systems (NLB, shapers, etc.)

FIREWALL MANAGEMENT AND IMPLEMENTATION

MGT will assign US based certified engineers for the project and a technical project manager who will track the progress of the project, schedule meetings, and provide regular updates to the client's stakeholder team.

INFORMATION GATHERING

- ◆ Build Implementation strategy and roadmap.
- ◆ Identify key elements of migration.
- ◆ Conduct site survey/documentation of all sites in scope of migration.
- ◆ Conduct firewall asset inventory for registration and licensing.
- ◆ Define migration priorities and sequence.
- ◆ Develop cutover schedule.
- ◆ Define project process and roles.
- ◆ Define performance metrics.
- ◆ Gather stakeholder communication list.

- ◆ Document any exceptions, sensitive or critical components from the risk/security /operations standpoint.
- ◆ Execute design review and freeze the implementation plan.

Server Administration Services

Windows Server administration includes:

1. Operating system installation, configuration, and licensing.
2. Operating system services management including, installation of roles and features, disk management, and network configuration.
3. Server patch management - Regular deployment of Microsoft OS patches including Service Packs and all MS*-* security bulletin patches for the Service Provider’s provided services. Microsoft security bulletins (e.g., MS16-001) are released and deployed monthly. The Windows Managed Server Service offering does not include patch services for other customer-installed Microsoft enterprise products such as SharePoint, SCCM, SCOM, Lync/Skype, and Exchange. Also excluded from routine patch operations are customer-installed third-party software such as Adobe Acrobat, Flash, ColdFusion, Java, or any other off the-shelf products.
4. Server health and availability monitoring - Managed Servers are monitored 24x7x365 and include DST incident notification and response. Standard monitored metrics include CPU, RAM, and disk space usage along with network response time, latency, and availability. Additional advanced monitoring is available upon request and as a Direct Service.
5. Security vulnerability scanning and remediation efforts – Additional security settings above and beyond the standard template can be set at customer request. Remediation efforts resulting from customer-managed audits must be explicitly requested by the customer and will be performed at an **additional cost**.
6. Malware protection - All malware protection software policy settings and exclusions, as well as threat intelligence, are administered and approved by DST Security. Includes installation, tuning, and on-going administration of malware protection software.
7. Remote host security log shipping – Security logs are stored separately from the generating system for a minimum of 30 days.
8. Virtual machine snapshots/backups - Virtual Machine snapshots are available upon request and are retained for a maximum of 5 business days. For longer term needs, clones and/or backups are available to provide point-in-time fallback.

Service Level Objectives: MGT will comply with the service level objectives with the I-Bank after the initial discussion during the call.

SERVICES	SEVERITY LEVEL 1	SEVERITY LEVEL 2	SEVERITY LEVEL 3	SEVERITY LEVEL 4	MGT RESPONSE
Business Impact Rating	High	Medium	Low	None	Yes
Acknowledge	20 minutes	30 minutes	2 hours	1 day	Yes
Notify the Company	20 minutes	1 hour	N/A	N/A	Yes
Resolution	4 hours	8 hours	48 hours	2 weeks	Yes

Desktop and Help Desk Services

MGT can establish and/or augment your IT Help Desk Services. We deliver proactive and predictive solutions for on-demand responses to the I-Bank's IT requests. We can provide seamless integration to the I-Bank's current help desk personnel for support via on-site presence, phone, email, and a portal to MGT's service request system. MGT will, in addition to critical or emergency issues, provide for a tiered response protocol geared to serve the needs of the I-Bank, balanced for responsiveness versus anticipated expense.

MGT can provide the I-Bank with comprehensive service desk functionality. Users will have the benefits of:

- ◆ Certified, US-based dispatch and technical staff
- ◆ 24x7 coverage capability and real-time monitoring
- ◆ Robust trouble ticket tracking and reporting solution
- ◆ Escalation to on-site team
- ◆ Versatile support for the full technology stack
- ◆ Web-based incident reporting and status tools for end users
- ◆ Tiered service levels and response protocols

Security Asset Monitoring

Security Operations Center

MGT's managed services leverage our deep network and security engineering bench to deliver precise and proactive administrative support, threat hunting and detection, strategic and tactical incident response and remediation, and intentional communications and reporting to create a transparent and efficient convergence between our Network/Security Operations Center (NOC/SOC) and your internal resources.

Tools

- ▶ Firewall Logs
- ▶ IPS Logs
- ▶ SIEM
- ▶ End Point Logs / AD Logs
- ▶ Cloud / SaaS Logs
- ▶ Live Monitoring
- ▶ Vulnerability Management
- ▶ Custom Scripts

Process

- ▶ Event Classification & Optimization
- ▶ Triage
- ▶ Analysis and Prioritization
- ▶ Remediation & Recovery Road Maps
- ▶ Assessments, Auditing & Compliance
- ▶ NIST CSF Best Practices



Team (SOC & NOC)

- ▶ 100 + Cyber Security Engineers
- ▶ Dedicated Security Engagement Specialist
- ▶ Experience Across all Environments
- ▶ Certified and Trained Experts
- ▶ All with Master's Degree or Higher

Threat Intelligence

- ▶ Behavioral Monitoring
- ▶ Broad Threat Intel Feeds
- ▶ Zero Day Threat Detection
- ▶ Cloud Intelligence
- ▶ Latest Malware and Ransomware Ana
- ▶ Dynamic/Static Analysis
- ▶ Machine Learning

We can support and assist in managing the I-Bank computer systems and networks remotely 24x7x365 from our NOC/SOC. With MGT's NOC/SOC the I-Bank receives the full benefits of a cloud hosted Gartner's Magic Quadrant Leader Solution bundled with a US Based ISO 27001 Certified 24X7X365 Security Operations Center (SOC) and staffed by an incomparable team of security experts.

Analyst	Description
Associate Analyst	Responsible for alert triage and investigation of IDS/IPS events and logs and threat hunting
NOC System Admin	Responsible for alert triage and investigation, threat hunting, alert tuning, and supporting Remote Incident Response
NOC Operator	Responsible for alert tuning, threat hunting, leading Remote Incident Response engagements, and handles escalated investigations.
Pod Lead	Manages the SOC teams. Responsible (along with the named Customer Advisor) for the MDR service delivered to their team's assigned customers.

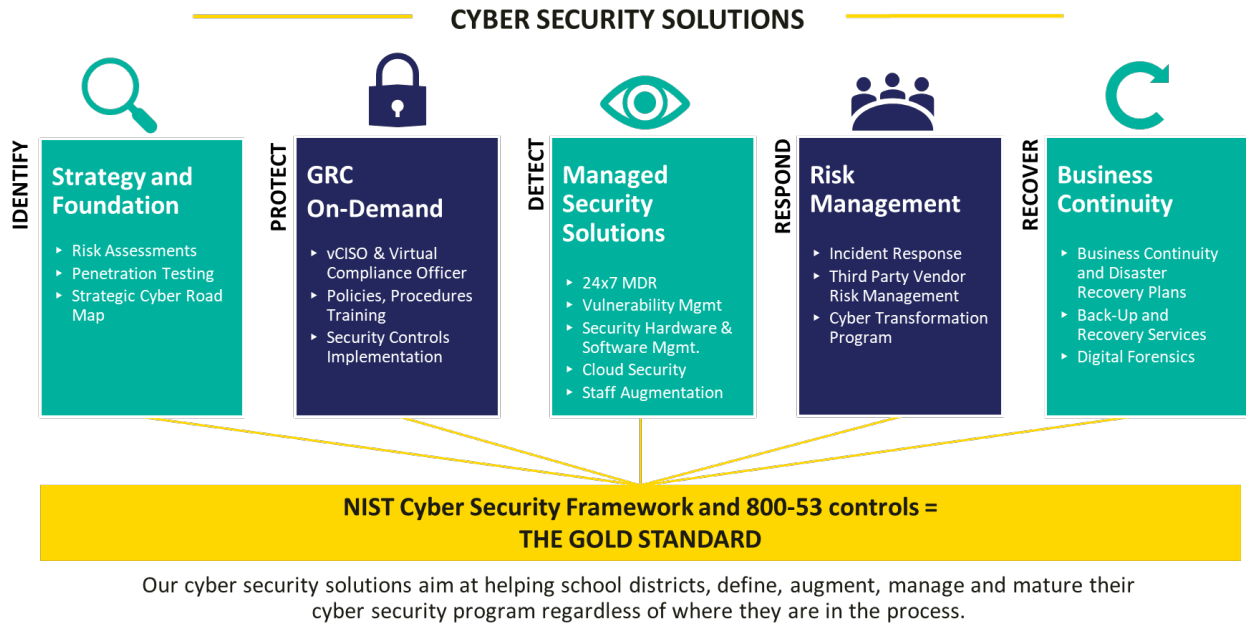
METHODOLOGY AND APPROACH

- a. MGT shall leverage its US based Network and Security Operations Center for 24x7 monitoring of alerts and policy exceptions (security events) generated by the system. After analysis by an Analyst, security events may be classified as security Incidents. Whether a security event is considered a security Incident is determined solely by MGT. Identified security events will be classified, prioritized, and escalated as MGT deems appropriate. Security events that are not eliminated as benign triggers are classified as a security Incident.
- b. Classify security Incidents into one of the three priorities described below:
 - (1) Priority 1 - a high priority security Incident in which MGT recommends immediate defensive action be taken.
 - (2) Priority 2 – a medium priority security Incident in which MGT recommends action be taken within 12 - 24 hours of notification; and
 - (3) Priority 3 – a low priority security incident in which MGT recommends action be taken within one to seven days of notification.
- c. When possible, eliminate false positives and benign triggers.
- d. Escalate security Incidents to an authorized security contact or designated services contact in accordance with processes as defined during the Integration and Transition Phase.
- e. Provide remediation/countermeasure recommendations, if applicable.
- f. Assist your security teams with performing root cause and impact analysis.
- g. Adjust alert prioritization options based on criticality.
- h. Consider ongoing policy improvements and notify you of MGT recommended policy changes.
- i. Perform analysis of potentially harmful security alerts.
- j. Perform updates to existing policy rules.
- k. Provide Incident handling support.

Cybersecurity Protection

MGT’s IT and Cybersecurity Solutions Framework

Our Cyber Security Office program has been designed to support security teams in augmenting the aspects of their infosec program they need help with and empower them to build and maintain a sustainable security posture over the long-term.



We help create “non sticky” security solutions so that security teams can be in control of how to evolve their program without having to be tied to outsourced resources. The result is an information security program that is tailored for your current needs, phased appropriately according to client priorities, resources, and limitations, with buy-in from across the organization, and designed to harden security in an efficient manner.

Best Practices Implementation

Our team utilizes multiple recognized Information Security best practices and standards while providing services to our clients. Some of the main standards include:

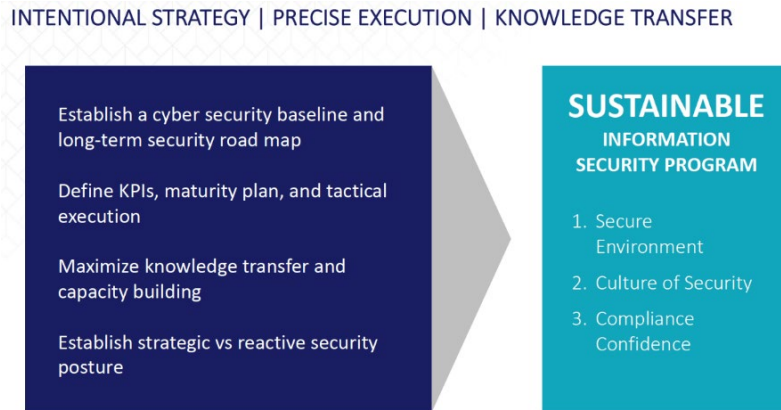
- ◆ IEC/ISO 27000 Series (Security Management and Control).
- ◆ National Institute of Standards and Technology (NIST) – Computer Security Standards.
- ◆ SANS Institute Guidance – Testing Methodologies and Approaches.
- ◆ Open Web Application Security Project (OWASP) – Web Application Testing and Assessment.
- ◆ Open-Source Security Testing Methodology Manual (OSSTMM) – Methodology for performing security tests and metrics.
- ◆ Payment Card Industry Data Security Standard (PCI-DSS).
- ◆ Information Systems Security Assessment Framework (ISSAF) – Methodology for information system security assessments.

- ◆ Penetration Testing Framework v0.58 – Community updated penetration testing framework.

Risk and Vulnerability Assessment Approach

Our vulnerability and risk assessment approach the I-Bank’s security risks and vulnerabilities. MGT’s assessment services give you the comprehensive understanding and insight you need to develop security controls that harden your system and keep your data safe. Our experts specialize in applying industry best practices and proven methodologies around NIST and other frameworks. As experts in complex vulnerability assessment engagements, we analyze your risk challenges and help you assess the critical elements as they relate to the context of your organizational context.

- ◆ Discovery
- ◆ Asset Classification
- ◆ Vulnerability Discovery
- ◆ Controls Assessment
- ◆ Threat Assessment
- ◆ Risk Formulation
- ◆ Impact and Likelihood Assessment



Risk Assessments

Properly implemented vulnerability assessments produce a prioritized inventory of the threats faced by an organization. They enable the organization to develop effective plans to mitigate threats and roadmaps to a more secure future.

NIST publication 800-30 provides guidance for conducting vulnerability assessments. MGT has developed a methodology that embraces the 800-30 guidance and enhances it based on our extensive experience working with public sector institutions of all sizes and missions.

- ◆ **Identification of Threat Sources and Events**
Understand what threat sources are relevant and not, to the context of the organization, as well as what the associated threat event could be.
- ◆ **Identification of Vulnerabilities and Predisposing Conditions**
Understand administrative, managerial, procedural, and technical vulnerabilities within the organization that could be exploited through defined threat sources as well as the current predisposing conditions that could lead to a successful exploitation.
- ◆ **Determination of Likelihood of Occurrence**



Define the likelihood that the identified threat sources would execute certain threat events and the likelihood of these events being successful.

- ◆ **Determination of Magnitude of Impact**

Define the business impact to organizational assets, individuals, related organizations, and ultimately the nation, because of a vulnerability exploitation.

- ◆ **Final Determination of Organization Risk**

Determine the overall information security risks as a combination of the likelihood of threat exploitation of vulnerabilities and the impact of such exploitation, including any uncertainties associated with risk determinations.

ACTIONS / APPROACH

Our assessments are conducted with the use of both non-intrusive and robust commercial scanning tools and manual tests by our team of experts who will provide comprehensive infrastructure reports of active IP systems. When necessary, open-source tools are used to validate certain checks to remove any false positives.

MULTI-STAGE ATTACKS

Our assessment methodology incorporates the use of NIST 800-115, “Technical Guide to Information Security Testing and Assessment” which requires escalation procedures in which the assessment seeks to determine the likelihood that risk associated with single foothold in an environment will be compounded through lateral advance and chaining separate attack techniques in order to escalate privileges with the goal of compromising beyond the initial foothold.

During our assessments, we perform a threat vector assessment through manual and automated reconnaissance of the network. Through prioritizing the potential risks associated with misconfigurations, and known vulnerabilities identified through reconnaissance, we manually validate each threat vector with the goal of exploiting the misconfiguration or vulnerability to gain unauthenticated access to the target system.

We then execute various multi-staged attacks against the application, OS, and/or network stack in support of the compromised system to move laterally throughout the network and leveraging access tokens (credentials) against other systems. Throughout the development of our “Attack-Chain” we document the initial foothold, and subsequent techniques used to parlay our initial access into an escalated state. The use of multi-stage attacks to escalate privileges is key to understanding the risk and mitigating controls in place to minimize the likelihood threat vectors can be used to compromise the confidentiality, availability, or integrity of systems.

CHECKS AND BALANCES

Our assessment methodology is based on risk determination guidance contained within NIST 800-115. We understand that our assessors have limited time to identify and validate misconfigurations or vulnerabilities that exist within the environment. Given the threat identification process is a dynamic and continual process, there is no reasonable expectation that all threat vectors will be identified or exploited during our assessments.

In order to ensure that the most “likely” attacks are covered, our threat vectorization stage is performed to identify vulnerabilities and misconfigurations that present the most likely risk given the level of difficulty and prevalence of the issue within the constraints of the scope of the assessment. All weaknesses that are identified are assumed to be repeatable by malicious actors given the same level of expertise and time against the system.

METHODOLOGY AND APPROACH

Our methodology thus prioritizes the most serious “low-hanging fruit” for inclusion in testing to validate these weaknesses and ensure the organization is reducing threat surface proportionally (given resource constraints) during the remediation process. All weaknesses identified during our assessment are also weighed against and manually validated for their likely use in “multi-stage” attacks further in a potential the attack-chain. We give priority to misconfigurations and vulnerabilities that are known to be key leverage points for lateral advance and privilege escalation as these inherently carry more overall risk to the environment than other weaknesses that are systemic to an application, platform, or network.

ELIMINATION OF FALSE POSITIVES/NEGATIVES

Our methodology is based on guidance contained within NIST 800-115 as it relates to verification and validation of a potential weakness. The identification of a “potential” weakness during our reconnaissance and threat vectorization phase provide context to our chosen attack-paths and not create specific reportable weaknesses directly. In this way, our methodology inherently removes false-negatives and false-positives form the reporting phase due to our requirement to validate and re-perform exploitation of the misconfigurations or vulnerabilities to diagnose the potential level of lateral advance or privilege escalation associated with the weakness.

Our methodology also includes procedures for continual feedback and management awareness of assessment risks when the assessment’s scope is non-evasive. If during our threat vectorization phase, we identify a potential weakness that may create availability concerns or network operational harm if exploited, our team will raise client awareness of the issue and validate the concern through non-destructive measures (e.g., obtaining diagnostic information from the system, which cannot be observed from the assessor’s scope). This procedure further increases the level of integrity contained within the final reported weaknesses and ensures that potential false positives/negatives are minimized if not completely avoided.

Software Tools

Our choice of tools and techniques will enable us to identify and map network devices, to determine if the IT infrastructure services implement security measures sufficient to protect sensitive information. Our choice of scanning tools combined with the knowledge of our expert penetration testers and risk assessors will help to determine the level of security and evaluate how vulnerable the identified systems are to potential system attacks, penetration, and information loss due to external hacker threats or internal malicious/curious network usage.

We conduct our testing using recognized frameworks such as Open-Source Security Testing Methodology Manual (OSSTMM), Penetration Testing Execution Standard (PTES), and National Institute of Standards and Technology (NIST) 800-115. MGT has a large arsenal of custom scripts and automated tools which will be used during the penetration tests depending on the scope of the project and the attack vectors. Some of the tools recently used in penetration engagements include:

- ◆ Kali 2021.1(Various tools provided by distribution)
- ◆ ParrotOS (Various tools provided by distribution)
- ◆ Nessus Scanner
- ◆ Metasploit Pro
- ◆ TheDigger
- ◆ BurpsuitePro
- ◆ URL Fuzzer
- ◆ Zed Attack Proxy
- ◆ Wapiti
- ◆ WebScarab
- ◆ Wfuzz
- ◆ Pacu
- ◆ Cred Scanner
- ◆ Cloudjack

METHODOLOGY AND APPROACH

- ◆ Sub-domain Fuzzer
- ◆ Whois Registry search
- ◆ DNS Dumpster Reconnaissance
- ◆ WAAF Bypass
- ◆ S3 bucket Leak
- ◆ Nmap custom scripts
- ◆ Enum4Linux
- ◆ Smbclient
- ◆ Sipvicious
- ◆ Dirbuster
- ◆ OWASP ZAP 2.0
- ◆ Ratproxy
- ◆ W3af
- ◆ Grabber
- ◆ PowerSploit
- ◆ Enum4Linux
- ◆ Social Engineering Toolkit (SET)
- ◆ Aircrack-ng
- ◆ Airmon
- ◆ Kismet
- ◆ HTTRACK
- ◆ WinPeas
- ◆ PowerView
- ◆ PowerSploit
- ◆ BloodHound
- ◆ PSEXec
- ◆ Empire Project framework
- ◆ Pentesters framework
- ◆ Hashcat
- ◆ Nishang framework

Strategic Planning

vCISO Services

Add cyber security leadership and expertise to your executive team with MGT's Virtual Chief Information Security Officer (vCISO) services. MGT's vCISO services are specifically designed around the unique needs of governmental and other public sector entities. Our vCISO consultants are technology leaders and cybersecurity experts who are ready to join your executive team and bring our experience and broad perspective to your security decision making and implementation.

PARTNERING WITH MGT PROVIDES THE CITY WITH UNIQUE EXPERTISE:

Deward Neely, Chief Information Security Officer



Recognized by the *Indianapolis Business Journal* as **2021 Chief Technology Officer** of the year, Mr. Neely brings MGT's clients his experience as a CIO of Eleven Fifty Academy, one of the world's top software development and cybersecurity full-immersion training bootcamps.

At MGT, Mr. Neely provides CIO-as-a-service to our clients by building, managing, and implementing innovative solutions to meet your security, operational, compliance, and audit requirements. He is highly involved in his community and looks forward to helping your social impact through world-class technology solutions.

An MGT vCISO can be the ideal solution to bring coherence to your organization's security program as you work to elevate your "cyber security IQ" and harden your systems against threats. Many public sector organizations operate

with a complex mix of internal and third-party solutions but lack the key leadership to evaluate the security of those solutions and ensure they are protected by a robust cyber security framework. An MGT vCISO can step in and perform all the functions of a full-time executive at a fraction of the cost. Regardless of the maturity of your current cyber security program, your MGT vCISO is ready to roll up their sleeves and get to work. They will initiate and oversee assessment and testing of your assets, establish or refine a cyber security strategy, build, and maintain a Governance, Risk, and Compliance (GRC) program, oversee personnel, contractors, and vendors, and much more.

As one of the nation’s leading public-sector consulting firms and recognized cyber security leaders, MGT is uniquely positioned to provide the full range vCISO and related consulting services. The diverse skills and backgrounds of our consultant teams enable us to offer clients a level of in-depth support for their cyber security programs that other firms simply cannot match.



Service Level Agreements:

MGT will honor the SLA’s set by CGG in the RFP. However, once our Engineers understand the environment completely and get a better knowledge of the infrastructure, we will work with the I-Bank IT team and develop an SLA plan that is close to the I-Bank’s request.

Severity Level 1 - Major system, product, or component failure that impacts Service delivery and affects a major function of the business or affects a large number of Authorized Users. The business is unable to function until it is restored. Relative to the I-Bank’s infrastructure, a Severity Level 1 will remain a Severity Level 1 until final

Severity Level 2 - Major issue that impacts the I-Bank’s ability to complete daily work affecting multiple Authorized Users and affects Service dry. The business can perform the function with either a workaround or manual processes, but service is degraded.

Severity Level 3 - Issue has resulted in a limited loss of function. Work can be completed using alternative methods and there is minimal impact to Service delivery. The business can continue to function even though Services may be degraded.

Severity Level 4 - Minor issue or request which has no impact on Service delivery. Requires follow-up only.

Vulnerability Management

Vulnerability management is a continuous cybersecurity process that includes identifying, evaluating, treating, and reporting software and network vulnerabilities. Properly monitoring and responding to pressing, complex issues are essential components of vulnerability management and information security.

Software and network vulnerabilities are constantly at risk of being exploited by attackers with intentions to insert destructive malware, compromise system infrastructure, and steal sensitive user data. Furthermore, these malicious actors leverage both tried-and-true and constantly evolving methods for breaking through your perimeter.

Modern network technologies like cloud computing and containers have created an unprecedented spike in productivity. Many corporate jobs can now be done from the comfort of your living room or your local coffee shop and deploying a new application or data center takes a fraction of the time and cost it once did. The growing adoption of IaaS and virtualization, compounded by our growing reliance on fast and quick-built applications, creates unique security challenges; it is becoming increasingly difficult for security teams to know what is on their network, let alone defend it from attack.

Security teams must work closely with their IT and application development counterparts to understand the risk of these changing environments at every layer, and look at application, network, and user risk together rather than in silos.

Project Governance and Communication Plan

In every engagement large and small, MGT adheres to a rigorous project governance process and full communication that ensures the quality and timeliness of deliverables and the complete satisfaction of our clients with every aspect of the project. For any projects undertaken for the I-Bank, we will work closely with your IT department and project manager to manage scope and schedule and ensure delivery of services that meet your unique needs and chart a path forward that reflects the goals of your organization.



Key tenets of MGT’s project governance protocols are:

Project Initiation: All projects begin with an initiation phase. MGT facilitates a kick-off meeting with the client team that provides the opportunity for introductions, and a setting in which to confirm project expectations and deliverables. During the initiation phase, the MGT team finalizes the project work plan, schedules, and other documentation based on client input.

Work Plan and Schedule: The work plan and associated schedule are the guiding documents for the project. Together they capture the key objectives for the project, list the deliverables, and establish the timeframe for the various activities necessary to achieve those objectives. The MGT project director and the client team both use these documents to monitor progress and ensure that the project remains on track.

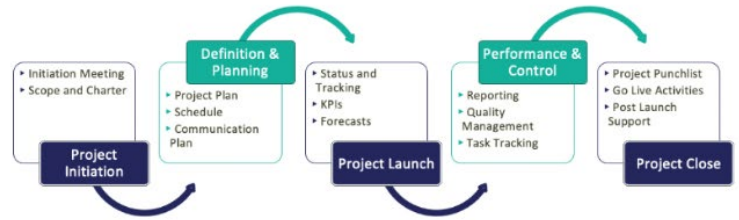
Quality Control: MGT follows industry standards and best practices to ensure all project activities are conducted appropriately, all devices and functionality are properly tested, and that all project deliverables are of the highest quality. Any project activities that require physical or virtual access to client facilities and IT infrastructure are closely managed to mitigate any risk of unintentional consequences such as loss of functionality or data breach.

Communication: Open communication and transparency are vital to the success of any project. Accordingly, MGT maintains a high and consistent level of communication throughout the course of the engagement. The communication plan is unique for every project and very much dependent on such factors as the duration of the project and the needs of the client. Early in the project, as part of the initiation phase, the MGT project director will work with the client team to establish the communications rhythm which typically includes routine status meetings, progress reporting and an open-door policy for ad-hoc communication to address project needs as they arise.

Knowledge Transfer: The MGT Technology Practice is distinguished in its commitment to complete knowledge transfer. Our goal in every technology implementation project is to leave the client team better informed than they were when we arrived. All data and other collateral materials gathered and developed during the project will be provided to the client team. At the conclusion of any development activities, we will, at the client’s discretion, meet with leadership to review the results step-by-step, and provide staff training and orientation so that team members are prepared to implement any recommended improvements in infrastructure or operations.

- ▶ Project Planning & Roadmaps
- ▶ Requirements Gathering
- ▶ Collaborate with Engineering and Operations Teams
- ▶ Project Status Reports to Leadership
- ▶ SPOC for OEM and Vendor collaboration
- ▶ BoM & SKU Management
- ▶ Change Management
- ▶ Documentation & Knowledge Assets
- ▶ Risk Management
- ▶ New Hardware, Technology Onboarding, Infrastructure Lifecycle Replacements (EOL/EOS)
- ▶ Project Go Live
- ▶ On-Going Management
- ▶ Lessons Learned Activities

**Project Management Approach & Focus:
Roles and Responsibilities**



MGT Project Management

In every engagement large and small, MGT adheres to a rigorous project management process that ensures the quality and timeliness of deliverables and the complete satisfaction of our clients with every aspect of the project.

Our unique methodologies are based on industry standard best practices enhanced by our vast implementation experience for schools, universities, government agencies, and private industry.

**We Have Successfully Completed More Than
13,000 Projects!**

Potential Challenges

The primary risk associated with this project is delay of deliverables, stemming from potential the I-Bank stakeholder engagement could be delayed if there is not adequate participation with I-Bank IT personnel. The I-Bank IT Project Officer and the MGT Project Director will work together as partners with full commitment to the project. As mentioned, this challenge can be mitigated with constant communication, proper planning, and back up strategies.

Tentative Implementation Schedule for SIEM - Security Monitoring (50 Assets)

Tasks Scheduled	Week 1	Week 2	Week 3
Gather the Current Network Topology			
Gather the Asset Information in scope for SIEM deployment.			
Produce Architectural planning for deployment			
Classification of Log Collection types (Syslog, API, Agents, Remote Log Collection, etc.)			
Resource Planning (CPU, Memory, SSD Drives etc.) for ESXI Host Deployment			
Firewall Rules for all necessary communication among the Rapid7 components			
Build individual VM's for SIEM Components			
Download and Deploy the Rapid7 Collectors			
Register Rapid7 Collectors with Cloud			
Build a VM for Honeypots			
Deploy Honey Credentials and Honey Files			
Deploy Insight Agent to all servers and workstations			
Identify log sources from each type of devices (Qty 02 from each category including Firewalls, Routers, Switches, Servers etc.)			
Integrating all the required Log sources with Rapid7 Insight IDR			
Build and Customize the SOC Portal / Dashboards			
Adding the Log sources and validating the data on the backend			
Validate and customize the configuration			
Tweak the SOC Portal/Dashboards and go through User Acceptance Testing.			
24x7 environment monitoring			
Validate alerts and remove false positives from			
Custom alerts and 3rd party integrations			
Remediation & mitigation actions performed			
Trouble Shooting (If needed)			
Documentation			



Emergency Preparedness Plan

Below, we have provided a summary of our emergency response and continuity of operations plan.

MGT has a disaster preparedness and recovery plan to account for natural disaster and to safeguard against man-made incidents that could potentially impede our client's ability to operate at peak efficiency. We understand that emergencies have the potential to disrupt operations and jeopardize the safety of faculty, staff, and students.

MGT will strive to manage any facility emergency incidents rapidly and effectively, through clear leadership, effective management, and timely response. Management of emergencies and continuity operations at MGT will utilize best practices from the National Incident Management System (NIMS) and the National Disaster Recovery Framework.

Operational disruptions are continued in a remote capacity through our Security Operations Center (SOC) that exceed the on-site capabilities of the affected facility. Our SOC will monitor your network infrastructure, mitigate threats, and provide resolution to on-demand issues. We work closely with our client's leadership team to identify and coordinate continuity and recovery strategies and objectives that meet the needs of the organization.

Continuity of operations focuses on restoring essential services incorporating the following supportive principles:

- 1) Apply orders of succession and delegations of authority
- 2) Establish communication with supporting and supported organizations and stakeholders
- 3) Perform essential services in order of prioritization
- 4) Manage human capital
- 5) Acquire space and equipment as necessary for essential services
- 6) Establish means for accessing vital records, files, and databases
- 7) Prepare for the reconstitution of essential service

- Employee training (describe your organization's training plan, and how frequently your plan will be shared with employees).

We require mandatory, period security awareness training as well as providing new vendor on-boarding training for all security monitoring staff.

- Identify essential business functions and key employees (within your organization) necessary to carry them out.

Analyst	Years of Experience	Education	Required Skills/Certifications	Responsibilities
Associate Analyst	2 to 5 Years	BS/MS in Computers	Certified Security Analyst (CSA)	Responsible for alert triage and investigation of IDS/IPS events and logs and threat hunting
Analyst	3 to 6 Years	BS/MS in Computers	Certified Security Analyst (CSA) Certified Incident Handler / Threat Intelligence	Responsible for alert triage and investigation, threat hunting, alert tuning, and supporting Remote Incident Response
Senior Analyst	5 to 8 Years	BS/MS in Computers	Certified Security Analyst (CSA) Certified Incident Handler / Threat Intelligence / CISA	Responsible for alert tuning, threat hunting, leading Remote Incident Response engagements, and handles escalated investigations.
Pod Lead	8 + Years	BS/MS in Computers	Certified Security Analyst (CSA) Certified Incident Handler / Threat Intelligence CISA / CISSP	Manages the SOC teams. Responsible (along with the named Customer Advisor) for the MDR service delivered to their team's assigned customers.

- Contingency plans for:
 - How your organization will handle staffing issues when a portion of key employees are incapacitated due to illness:

MGT has over 250 personnel, including over 115 trained, certified, and experienced security personnel that are able to augment your staff if or when your employees are incapacitated due to illness. Due to our SOC we are also able to operate in a remote capability that allows for continued social distancing.

- **How employees in your organization will carry out the essential functions if contagion control measures prevent them from coming to the primary workplace.**

We will follow our continuity plan detailed above, as well as follow our Safety Plan in our Employee Handbook, as well as guidelines of the CDC. We will also work remotely and provide regular and proactive progress reports. We will also follow our Project Management and Communication protocols, described in our Proposal.

- **How your organization will communicate with staff and suppliers when primary communications systems are overloaded or otherwise fail, including key contacts, chain of communications (including suppliers), etc.**

MGT is committed to maintain full communication with NJIB.

NJIB Staff: Our communication with NJIB staff will be through email, phone, video conference capabilities, and other forms of communication.

Supplier: MGT is currently in partnership with over 40 suppliers in which we have established relationships and contacts to provide our customers with efficient process, updated hardware and software products, and maximum affordability. We have established a chain of communication with each vendor does not affect our client's business operations.

• **How and when your emergency plan will be tested, and if the plan will be tested by a third party:**

MGT's plan is continually revised by our cyber security expert team and is not reviewed by a third party.

Experience and References

MGT feels repeat business is the greatest testament to our commitment to customer service and client satisfaction. We encourage you to contact any of our references to learn of our professionalism, ability to meet timelines, and the expertise of our staff. Additional references which encompass this RFP's scope of work are available on request. The following references are MGT's most recent engagements relevant to the I-Bank's scope of work.

Managed Services Expertise

Howard County Public Schools

MANAGED SECURITY SERVICES (MSSP SERVICES)



Phillip Dixon - I.T Security Manager

10910 Clarksville Pike

Ellicott City, MD 21042

(410) 313-6600 | phillip_dixon@hcpss.org

Period of Performance: July 2020 – Present

Relevant Scope of Services: Howard County Public School System selected MGT as its 24/7 managed security partner. From our US based Security Operations Center, MGT provided monitoring and logging of network traffic, live data visualization

and analysis of all North/South & East/West traffic through the school system's two data centers, proactive threat hunting, firewall management, and vulnerability management.

City of Lawrenceville, City and Police Department

EXPERIENCE AND REFERENCES

MANAGED FIREWALL AND END POINT SERVICES PROJECT (MSSP SERVICES)



Kyle J Parker, Director - Information Technologies
70 S. Clayton Street
Lawrenceville, GA 30046
(678) 407-6406 | Kyle.Parker@LawrencevilleGA.Org
Period of Performance: December 2019 – Present

security gateway logging, monitoring, and management, threat detection and alerting, breach monitoring and alerting, incident response planning and execution, security intelligence and awareness, behavioral monitoring, intrusion detection and prevention (network & host-based), availability monitoring, malware detection/prevention, end point protection, and ransomware protection.

Tuskegee University

UNIVERSITY-WIDE MANAGED SECURITY SERVICES & DATA CENTER NETWORK REFRESH



Jamillah McCray – Contract Specialist Buyer
1200 West Montgomery Road
Tuskegee, AL 36088
(334) 724-4181 | jmccray@tuskegee.edu
Period of Performance: December 2020 – Present

Relevant Scope of Services: MGT has been selected by Tuskegee University as their technology partner to design and implement a data center network upgrade, replacing and upgrading the institution's entire network infrastructure. In addition to life-cycling components at EOL (end-of-life), the project will upgrade the Tuskegee University network topology from a layer-2 design to tiered layer-3/layer 2 environments and incorporate dual IPv4/IPv6 protocols.

- ◆ We are working with Tuskegee University to provide monthly Managed Security Services including:
- ◆ Level 1 network infrastructure and security support
- ◆ 24x7 management and monitoring of critical servers, firewalls and up to 500 devices
- ◆ Network vulnerability scanning on a quarterly basis
- ◆ Management of all network switches, routers and wi-fi across campus
- ◆ Managed VPN services for secure remote access

Cybersecurity Protection Services

Dallas Fort Worth Airport

ASSESSMENT AND VCISO SERVICES



Venu Sigamala - Information Security Manager
2400 Aviation Dr
DFW Airport, TX 75261
(972) 973 5478 | vsigamala@dfwairport.com
Period of Performance: 2019 – Present

Relevant Scope of Services: MGT provided comprehensive penetration testing for Dallas-Fort Worth Airport (DFW). MGT's testing probed the exploitable vulnerabilities of the airport's assets which include networks, Internet of Things devices and

Industrial Control Systems (ICS) /Supervisory Control and Data Acquisition (SCADA) systems. Testing methodologies and procedures conformed to the NIST Special Publication 800-115 and met the Audit Requirement of International Organization for Standardization (ISO) 27001 and Payment Card Industry Data Security Standard (PCI-DSS). DFW is the fourth busiest in the world by aircraft movements and the fourteenth busiest airport in the world by passenger traffic.

Silicon Valley Clean Energy

INFORMATION SECURITY AUDIT AND ASSESSMENT



Nik Zanotto - IT Director
333 W El Camino Real Ste 290
Sunnyvale, CA 94087
(844) 474-7823 | Nikolas.Zanotto@svcleanenergy.org
Period of Performance: April 2020 – June 2020

Relevant Scope of Services: MGT worked with the SVCE to design and execute a top to bottom audit of the agency's IT infrastructure, network, and data storage and to conduct a Focused Security Assessment of SVCE's information security

program. We performed penetration testing of the agency's assets, vulnerability assessments, a comprehensive review of current IT policies and procedures, and a focused assessment of the agency's cyber security program. We completed a report describing the activities performed, including results of all tests, the findings and risks identified, and prioritized recommendations and next steps to mitigate the risks and increase the security posture of SVCE.

Strategic Planning Services

Housing Authority of Savannah

STRATEGIC PLANNING



Earline Wesley Davis - Executive Director
1407 Wheaton Street
Savannah, Georgia 31404
(912) 235-5800 | davis@savannahpha.com
Period of Performance: October 2017 –October 2018

Relevant Scope of Services: The Savannah Housing Authority (SHA) retained MGT to assist in the development of the SHA’s five-year strategic plan. Throughout the strategic planning process, MGT worked closely with SHA’s leadership, staff, and

Board of Commissioners to reach consensus on vision, mission, values, strategic priorities, and goals and objectives. MGT conducted an environmental scan and comprehensive SWOT analysis including the collection of both quantitative and qualitative data from both internal and external stakeholders of the SHA. The data gathered during these processes served as the framework for developing mission, vision, and values that served as the framework for the new strategic plan. MGT also developed implementation strategies and a framework for monitoring strategic plan implementation.

Appendix A: Resumes

Please see our Team's professional resumes on the following pages of this section.



Studies

Biology - University of Alabama at Birmingham (UAB)

Information Security and Assurance
- Kennesaw State University

Certifications/Affiliations

- Certified Information Systems Security Professional (CISSP)
- Security+ Certified Professional
- Microsoft Certified Professional (MCP)

Alton M. Kizziah Jr.

Executive Vice President and GM
MGT Technology Solutions

Summary

Technology and Information Security Executive with over 20 years experience designing, building and managing global scale security operations centers.

What I Bring to the Engagement:

Executive level oversight with background in operations, sales, and delivery. Ability to develop strategy aligned with critical business outcomes with an eye to the details. Decades of experience in managed security services.

Accomplishments

- ◆ Built, from the ground up, multiple Cyber Fusion Centers and SOCs with locations in Europe, APAC, and the United States with hundreds of staff responsible for thousands of global customers analyzing more than 10 billion security events per day.
- ◆ Recognition from industry analysts like Gartner, Forrester, and others.
- ◆ Set strategic initiatives and drive key results on a global scale for multinational corporations.
- ◆ Veteran, US Army.
- ◆ Diversity and Inclusion champion.



Work Experience

Chief Strategy Officer and Senior Vice President of Global Managed Security- Kudelski Security

April 2016 – Feb 2022

- Chief Strategy Officer. Owner of the company growth strategy and responsible to drive business expansion. Created and implemented plan to build business units in new locations. Oversee the expansion to broader EMEA (France, Benelux, DACH, Italy) and the UK. Drive and oversee the roll out of an Alliances program globally.
- Senior Vice President of the Managed Security Business Unit Globally. Built, from the ground up, a global Cyber Fusion Center with locations in Switzerland and the United States. Responsible for all aspects of the Managed Security business including budgeting, sales, go to market, operations, strategy, research, devops, and threat intelligence. Achieved recognition from Gartner by inclusion in the 2017-2021 Managed Detection and Response Market Guide as well as notable vendor in the 2019 Magic Quadrant for Global MSSPs, from Forrester by inclusion in the 2018 Emerging MSSP Wave as a Leader and 2020 Mid-Size MSSP Wave again as a leader, and from IDC in the 2019 Emerging MSSP North America as a Major Player.

Vice President Security, Forsythe

March 2015 – April 2016

- General Manager of the National Security Business Unit in the Central Region. Responsible for \$100 Million in yearly revenues, forecasting and deal management, pipeline development, marketing strategy and event participation, field on-boarding and enablement, partner relationship development, customer relationship building and account development, coaching individual contributors toward successful execution of duties, and active participation in key services related projects and initiatives.

Vice President and GM, Managed Security Services Business Unit – FishNet Security

May 2014 – March 2015

- General Manager responsible for a \$20 Million P&L, the strategic direction, operations, sales, budgeting, forecasting, staffing, go to market strategy, and overall health/maturity of the MSS line of business, key to growing FishNet revenue 30% in 2014. Oversaw MSS growth of 160% year over year and capturing 68 new logos in 2014. Managed 2 SOC locations, 90 Staff, and reduced customer attrition by 50% while staff retention improved dramatically. Created set of key performance indicators and tracking metrics on customer satisfaction, productivity, monthly recurring revenue, and attrition. Lead through Merger and Acquisition activities as subject matter expert for MSSP.

Senior Director of Managed Security Services, Security Business Unit – Trustwave Inc.

June 2010 – May 2014

- Designed, built and managed 3 new Security Operations Centers Globally. Responsible for space planning, staffing, training, and developed the first Global Follow the Sun support model. Managed Global SOC of 100 staff responsible for 7000+ global customers 24x7 and that analyzes 10 billion events per day. Exceeded all SLA goals and maintained high customer satisfaction.

Chief Information Security Officer – Newedge Group, LLC

April 2009 – June 2010

- Developed and implemented IT Security Standards and Procedures. Measured and reported compliance to Newedge IT Security Policy's to the IT Executive and Technology Risk Management Committees. Developed IT Security metrics and reporting for the parent banks.

Lead Information Security Engineer – OfficeMax Inc.

September 2008 – April 2009

- Responsible for identifying solutions, product/vendor evaluation, selection and procurement, development, migration, deployment and oversight including perimeter defense, firewall management, endpoint security, intrusion detection and prevention, encryption, VPN, data leakage protection and data integrity across platforms and applications.

Solution Integration Manager – IBM Corporation/Internet Security Systems

May 2006 – September 2008

- Responsible for leading multiple project teams integrating and delivering high value, complex MSS solutions to customers. Responsible for managing scope, cost, schedule, and contract deliverables. Consulted and guided customers through professional services security engagements as part of the ISS X-Force.

Senior Information Security Analyst/Engineer– Rare Hospitality International

July 2002 – May 2006

- Instrumental in developing and implementing Business Continuity and Disaster Recovery (BCP & DRP) Plans for corporate site in Atlanta, Georgia and worked as the Project Leader for all Information Security projects and a trusted advisor on other IT projects.



Sridhar Ratnam

Director of Cyber Security Solutions

MGT Consulting

Proposed Role: Director of Cyber Security Solutions

Summary

Mr. Sridhar Ratnam has more than 30 years of Enterprise IT infrastructure architecture, engineering, operations, and consulting experience including managing large and multiple data centers; Cloud strategy and infrastructure management. Mr. Ratnam has a strong background as leader at developing, optimizing, transforming, and scaling next generation of network and cloud strategy, enterprise networking standards, architecture, design, engineering and enterprise infrastructure transformations.

Relevant Skills

IT Infrastructure Operations Strategy and Leadership

- ◆ Solid technical background and deep-rooted experience in critical Infrastructure architecture, design, system, and performance management including managing large enterprise WAN and data center infrastructure, security appliances, perimeter security
- ◆ Provided 24/7 escalation support for Tier3/4 levels for worldwide and critical operations (SNOW)
- ◆ ITIL Processes Implementation: Problem, Support, Incident and Change Management
- ◆ Lead and managed development of innovation and provided strategic directions in enterprise network infrastructure - from conceptual data network design to delivery, especially in areas IaaS, PaaS, SaaS, Cloud Migration and Network Analytics
- ◆ Lead transformational projects in the area of data center and cloud infrastructure.
- ◆ Built and lead 20+ network/security engineering team to deliver Voice, Video, Data, Wi-Fi and WAN technology solutions enterprise wide.
- ◆ Alignment with customers and business stakeholders, outside partners and service delivery organizations through major technology transitions

Achievements

AWS and GCP Cloud Migration
2018-2020

About 5000+ workloads (VMs)
moved between AWS and GCP

RFP management and selection
process for cloud services

Refactoring Applications and
Data Base for Deployment to
Cloud Services

Network Transformation
Strategy (SDDC/SDN/SDWAN)
and Roadmap (2017/2018)

IHG Next Generation
Infrastructure Strategy (2014-
2016): Design, engineering,
implementation of two new
data centers (east coast and
west coast)

Enterprise Video Conferencing
(2016) extensive collaborative
engineering

Designed MPLS network for
primary connectivity for over
5000 hotels (2010-2013)

Post 9/11 Network Recovery
Project for New York Port
Authority (Disaster Recovery).

Certifications

AWS Certified Cloud Practitioner

Certified Information System Security Professional (CISSP)

Cisco Certified Network Professional (CCNP)

Several Industry certifications such as MCSE, CNE4, Sniffer Certified Expert, Etc.

Six Sigma Lean (White Belt)

Awards and Recognition

Winner of CIO's "Techcelerate Award", 2018

Winner of CIO's "Excellence in Delivery" Award 2017

Winner of CIO's Technology Award for the year 2014

Relevant Professional Experience

- ◆ MGT/CiraInfoTech | Director of Cyber Security Solutions | 2020 – Present
- ◆ IHG, Inc. | Director of Global Infrastructure Engineering | 2014-2020
- ◆ Americas Hotel IT Ops, IHG, Inc | Senior Technology Advisor | 2007-2014
- ◆ Unisys Corporation | Consultant Integration Architect | 2000-2007
- ◆ Bank of America | Senior Network Architect | 1998-2000
- ◆ US Dept. of State Public Affairs (USIS) Data Center, New Delhi, India | Operations Manager | 1992-1998
- ◆ US Dept. of State Public Affairs (USIS) Data Center, New Delhi, India | Systems Analyst | 1986-1992PK12



Education

Master of Computer Applications,
Bachelor of Science

MAHESH GARIKOTA

Head of Cyber Security Solutions

MGT Consulting

Proposed Role: Head of Engineering and Solutions

Summary

MGT's Head of Engineering and Senior Vice President of Cyber & Network Solutions is Mr. Mahesh Garikota. He is a widely experienced senior security professional with expert proficiency in developing and implementing innovative managed security solutions for public sector clients and a range of private industries that includes banking, insurance, manufacturing, and energy. Mr. Garikota brings over 20 years' experience in network and security engineering at the enterprise level with design, implementation, and support of network infrastructure.

Relevant Skills

- ◆ Lead Network Security Architect and Head of IT Operations with over 20 years' experience in Network and Security Engineering at enterprise level with design, implementation, and support of network infrastructure.
- ◆ Build and implement SIEM Solutions for customers at enterprise level with thousands of assets.
- ◆ Provide Managed Detection and Response Services to SLED customers 24x7 managing team of Security Analysts.
- ◆ Demonstrated abilities of delivery in large enterprise networks and security design, integration and implementation services covering perimeter, DMZ, NG firewall, Load Balancing, Proxy, Network Detection and response, End Point Security, IOR (Indicators of compromise), VAPT, Advanced Threat detection, Cloud Security including AWS, AZURE and google.
- ◆ Subject Matter Expert for enterprise security and GRC (Governance, Risk and Compliance).
- ◆ Experience performing Compliance audits such as PCI DSS, ISO 27001, HIPAA, SOC2/Type2 etc.
- ◆ Design and implement PCI security zone as well as install and configure firewalls at the Perimeter & DMZ
- ◆ Highly motivated and Internationally experienced senior technology professional with expert proficiency in developing and implementing innovative technical solutions for a variety of industries, including banking, insurance, manufacturing, health care, and oil refiner



Relevant Professional Experience

- ◆ MSP Division (Multiple End Clients) | Lead Architect and SOC Delivery Head | Oct 2018 – Present
- ◆ Major Banking Clients including. Key Bank and Capital One | Subject Matter Expert Network Security/SOC | Nov 09 – Sep 18
- ◆ Enterprise Data Center Network Support (TRW, GE, Hitachi etc.) | Sr. Network Security Engineer | Mar 05 – Nov 09
- ◆ Savvis Data Center Support (American Airlines) | Firewall Engineer | Jun 04 – Feb 05



Technical Experience

NGFW Technologies:

- ◆ Planning, Design, Implementation and Troubleshooting of Checkpoint, Palo Alto Networks, Cisco ASA, Juniper and Fortinet Firewalls in the large Enterprise scale networks.
- ◆ Working with Enterprise firewall management platforms including PANORAMA to manage Palo Alto Firewalls, Checkpoint Provider-1/MDS environment with multiple CMA's for Policy Provisioning, Forti Manager for Fortinet's, and FMC (Firepower Management Console) for Cisco devices

Cyber Security:

- ◆ Lead Managed Detection and Response (MDR) team to effectively detect, and respond to incidents
- ◆ Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation
- ◆ Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)
- ◆ Experience working with NDR tools as well as SIEM tools such as LogRhythm, Rapid7 InsightIDR, Splunk etc.
- ◆ Familiarity with industry standards such as PCI DSS, HIPAA, CIS Critical Controls, NIST, OWASP (TOP20).
- ◆ Detect and respond to alerts from end point detection response tools.
- ◆ Establish vulnerability management program using systematic scanning, risk evaluation, and coordination to remediate or mitigate identified vulnerabilities.
- ◆ Provide escalation support and document resolutions for improvement
- ◆ Work with the Account Management team as a Security SME to advise clients on applicable security solution technology, practices, managed services, and available solution programs.
- ◆ Provide weekly and monthly reports on Security Incident Response team activities
- ◆ Coordinate and provide expert technical support to resolve cyber defense incidents. Coordinate with intelligence analysts to correlate threat assessment data
- ◆ Experience deploying and configuring Blue Coat Proxy SG series appliances and manage using Bluecoat Director.
- ◆ Build and troubleshoot Site to Site (B2B) IPsec VPN and work with various business partners.
- ◆ Implementation and support of Remote Access VPN solutions with Multi Factor Authentication.
- ◆ Understanding of DMZ and build the segregation across application layers (Web / App and Data Base)
- ◆ Zoning of Firewalls based on Production, QV, Preproduction, DR and Development
- ◆ Building Disaster Recovery and Business Continuity Planning and Data Center Migration to Cloud.

Routing and Switching:

- ◆ Planning, designing, Installing and Configuring of Cisco Routers (ASA 1000, 7600, 7200, 3900, 2900, 2800) & Cisco L2 & L3 Switches (Nexus 9K, 7K, 5K, 2K and IOS 6500, 4500, 3750 series,).
- ◆ Configuring and implementing Routed and Routing protocols including: OSPF, EIGRP and BGP.
- ◆ Designing & implementing Cisco 3-tier LAN Network Architecture (Core, Distribution and Access).
- ◆ Configuring Spanning Tree, Rapid Spanning Tree, MST, VLAN, VTP.
- ◆ Redistribution of routing protocols, Route-maps (Policy Based Routing), access list and NAT.
- ◆ Implementation of HSRP, VRRP protocol on routers. VRF on Routers and build GRE Tunnels between Cisco routers.
- ◆ ITIL, Agile Scrum, Waterfall Methodology, Infrastructure Services Served on the Title III; Orientation and Peer Support Advisory committees and the Honors Council



Avinash Vellori, PMP, CISSP

Sr. Technical Program Manager

MGT Consulting

Proposed Role: Technical Program Manager

Summary

Avinash Vellori is a technology program manager with detail oriented, results driven security expertise. Mr. Vellori has a proven record of accomplishment in driving solutions, projects for cross-functional programs from definition, design, and implementation to launch, and building effective relationships with clients and team members along the way. Extensive experience in managing priorities, resourcing, schedules, and communication throughout full project lifecycle. Unsurpassed customer service, dedication, positive team-oriented attitude with proven leadership and success in highly visible roles for various sized project implementations.

Skills I Bring to This Engagement:

- ◆ IT Infrastructure, information security/assurance, security compliance auditing, Network and Security Engineering with over 10 years of experience in private, public and legal industry environments.
- ◆ Experienced in driving teams - Engineering, Implementation, Configuration and support of multimillions dollars, and high visible team projects. Includes McAfee ESM, Splunk SIEM, SourceFire, BRO IDS, Snort, Cisco, Fortinet, Juniper etc.
- ◆ Demonstrated abilities in enterprise wide network and security administration, Cloud services (IaaS, PaaS, SaaS) with market leading vendors like Microsoft Azure, Amazon Web Services, SAP Virtuestem with integration
- ◆ Auditing security compliance, FedRAMP, NIST SPECIAL PUBLICATIONS 800-53 (Rev. 4) guidelines to security governance teams.
- ◆ Unsurpassed customer service, dedicated, positive, team-oriented attitude with proven leadership and success in highly visible roles for various sized project implementations.

Education

Bachelor's in Technology –
Computer Sciences &
Information Technology

Masters – Computers &
Information Sciences

Certifications

CISSP (Certified Information
Systems Security Professional)

AWS SA (Amazon Web Services
Solution Architect)

CCNA (Cisco Certified Network
Associate)

CCSA (Cisco Certified Security
Associate)

SIXSIGMA GREENBELT

Juniper JunOS)

Security Clearances

US Security Clearance: Active

Position Risk Level - High Risk BI
Secret (Level II)

Awards and Recognition

Best employee of Wipro 2008 – with a signed certificate from Sr. VP

Best support supervisor in Wipro HP Project – with a signed certificate from AVP.

NITC Best employee of the quarter 2014 – with a signed certificate from the CIO.

Relevant Professional Experience

- ◆ United States Department of Agriculture (USDA) | Security Solutions Architect/Program Manager | 2018 - Present
- ◆ National Information Technology Center (NITC) | Sr. Network Security Engineer/Cloud Architect | 2012 - 2018
- ◆ McGraw Hill Global Data Center | Network Security Engineer | 2009 - 2010
- ◆ Wipro Technologies | Network Security Engineer | 2008 - 2009
- ◆ Hewlett Packard | Network Analyst | 2007 – 2008

Technical Experience

Hardware: Sourcefire, Fortigate, Checkpoint NGX R65, R70 and R71 PowerEdge2950 on Nokia Hardware using IPSO 1220 and SPLAT as well as IP Appliances IP 690, IP 695, IP 697 Juniper Netscreen 6500, 6000, 4500 SSL SA VPN, Netscreen ISG 1000, Netscreen 5400. Juniper SSG Firewalls, Juniper SRX 3600, Juniper SA 6500 Cisco ASA Firewalls including ASA 5585, 5550, 5540 and Cisco Core, distribution and access layer network devices including 7200, 3800, 3600, 2800, series routers, Cisco Catalyst switches including 6513, 6509, 4948, 3750G, 3560G, 3548, 2960G. Tuffin, Juniper Pulse PSO 6500.

Operating System: Sourcefire 5.4.X Fortigate FOS-5.x or later, Checkpoint R65, R70, R71, R75. Juniper Screen OS 6.X, NSM 2007, 2010, 2011, 2012 CentOS, JunOS 11+VS, ASA 7.X, 8.X, Nokia Voyager IPSO 4.x, 6.x, CSM 4.X, ASDMMS Windows 7, Vista, XP, Server 2000, 2003, 2008 Mac OS-X, Linux-Red Hat.

Network Topologies: TCP/IP and OSI Communication Layer, DS3, MPLS, Frame Relay, ATM, LAN and WAN routing protocols, including RIP, EIGRP, OSPF, BGP network service protocols and standards Active Directory LDAP, Radius, Tacacs, DNS, DHCP, NTP, SNMP V3 etc. as well as network redundancy protocols including VRRP, HSRP (Hot Standby Routing Protocol) 802.1q trunking

Security Topologies : Layer 2 (transparent mode) layer 3 (Routed mode), DMZ configurations, Access lists, Application inspection, NAT, reverse path verification etc. IDS (Intrusion detection system) and IPS alert management, Vulnerability Scan, IPSec Remote/Site to Site VPN connections using strong encryption.

Powershell, JSON, Shell, Python (beginner level)



Sudhir Musirigari

SOC Manager

MGT Consulting

Proposed Role: SOC Manager

Summary

Impact-oriented professional with exceptional problem-solving skills, strong analytical and communication skills; successfully managed programs and client-relationships working with executives at Fortune 500 companies with a passion for using analytical capabilities and insights to drive strategic recommendations to influence decisions & actions that drive improved customer experience. Consistently leads teams that convert ideas into efforts that produce innovative and bottom line results.

The journey started as a Network and Security engineer, which allowed me to acquire a broad range of technical skills at a breakneck pace. Improving the security posture of different products, services, applications and platforms has been my passion all along.

Gradually progressed towards Security Program Management, collaborated with cross-functional teams to operationalize and scale programs related to security, privacy, regulatory and compliance with 'Secure by Design' principle.

Relevant Skills

- ◆ Design; Implement; and Operate IDR, EDR, NDR solutions, Vulnerability Management solutions, SIEM tools.
- ◆ Experience in creating Project Charters, Project Status reports, RACI matrix, Project Delivery reports.
- ◆ Worked as an Operational Project Manager handling Operational readiness reviews, Handover tick sheets, Key operational procedure documents for a Multinational Investment Bank.
- ◆ Understand IT infrastructure silos including network, Security, Server, Applications Firewalls, Cloud etc.
- ◆ Manage IT projects and proficient with the use of project documentation and tasking tools (i.e., JIRA, MS Project, Mavenlink, etc.)
- ◆ Skilled in the areas of managing teams and client engagements, forecasting and budgeting, risk management, regulatory compliance, business process analysis, relationship management, team building and leadership, as well as project management.
- ◆ Installation, Configuration of Next Generation Firewalls Palo Alto, Check Point, Cisco, and Fortinet.
- ◆ Design, Implement, and troubleshoot Next Generation Threat Prevention solutions like IDS/IPS, Application filtering, URL filtering, Anti-virus, Anti-Bot.

Education

- Bachelor's in Electronics and Communication Engineering
- Master's in Electrical Engineering

Certifications/Affiliations

- Cisco Certified Network Associate Security (CCNA Security)
- Cisco Certified Network Associate R&S (CCNA R&S)
- Check Point Certified Security Expert (CCSE)

Achievements

- Completion of 'Advanced Threat Prevention R80,20' course from Check Point professional Services
- As an Operational Project Manager for a Multinational Investment Bank supported Network Operations in Operational readiness for 5 critical and major audit required Network Security projects.

Awards and Recognition

- Awarded as Most Valuable Performer (MVP) in 2021 within Technology Solution Group (TSG) at MGT



Relevant Professional Experience

- Deutsche Bank | Network Operation Engineer | Aug 2019 – Dec 2021
- Deutsche Bank | Operational Project Manager | Aug 2018 – July 2019
- Royal Bank of Scotland | Network Security Engineer | Sep 2015 – July 2018



Technical Skills

Technology Platforms:

- Firewall Platforms including Check Point, Cisco, Palo Alto Networks and Fortinet with DMZ Architecture
- Firewall Management Platforms including Forti Manager, MDS / Smart Center, FMC, Panorama
- Cisco based Routing and Switching platforms including Nexus
- McAfee Proxy, F5 Load Balancers, Check Point IDS/IPS, WAF, End-point security solutions, site2site VPN
- Managed Detection and Response - Rapid7 Insight IDR, Splunk, IBM Qradar
- Vulnerability Scanner and Vulnerability Management System - Nessus, Manage Engine, Rapid7 Insight IVM
- Patch Management - Manage Engine
- AWS / AZURE / GCP Cloud Platforms



Ashok Pilla

NOC Leader and Security Engineer
MGT Consulting
Proposed Role: NOC Manager

Summary

Network and Security Engineer with 10+ years of experience includes design, installation, configuration and supporting of network & security Products. Significant experience on industry leading Network and Security appliances including Fortinet, Cisco ASA, Checkpoint, Palo Alto, Fortinet and Juniper Firewalls as well as Cisco based Routing and Switching. Hands on experience with VPN implementation including Site to Site, IPsec based Remote access, Intrusion Detection and prevention appliances including Cisco AIP-SSM, IDSM, Source Fire. Experience on F5 load balancers. Knowledge in Network monitoring and vulnerability assessment tools like Solarwinds, Qualys and Nessus. Unsurpassed customer service, dedicated, positive, team-oriented attitude with proven leadership and success in highly visible roles for various sized project implementations.

Relevant Professional Experience

- ◆ Cira Infotech Inc (Various Customers) | Sr. Security & Lead Engineer | Oct 2019 – Present
- ◆ Fresenius Medical Care | Network and Security Consultant | April 2019 – September 2019
- ◆ Cira Infotech Inc (Various Customers) | Sr. Security & Lead Engineer | Oct 2017 – March 2019
- ◆ Tupperware/Di Data | Sr. Security Engineer | July 2016 – Sep 2017
- ◆ CapitalOne | Sr. Security Engineer | Feb 2015 – June 2016
- ◆ Verizon Global Professional Services | Design Engineer | April 2014 to Jan 2015
- ◆ Savvis Data Center Services | Security Design Engineer | May 2008 to March 2014

Education

Bachelor's in Electrical Engineering

Master's in Information Technology (Network and Security).

Certifications and Training

Checkpoint Certified Security Expert CCSE (Gaia)

Checkpoint Certified vSEC Administrator

Checkpoint Certified Sandblast Administrator

Palo Alto Certified Network Security Engineer (PCNSE)

Cisco Certified Network Associate Security (CCNA Security)





Technical Experience

Hardware Platforms:

- ◆ Fortinet gate 7030E, 3960E, 1500D, 200E running 5.x and 6.x software versions
- ◆ Fortigate firewalls managed through FortiManager and FortiAnalyzer at Enterprise level.
- ◆ Palo Alto firewalls including PA 3000, 4000, 5000, 7000 series firewalls and small scale devices like PA-500. M-500 Management console
- ◆ Cisco ASA Firewalls including ASA 5585, 5550, 5540, 5545x, 5525x, 5512x, 5516x, 5510 and PIX 535 Firewalls. FMC 2500 and Virtual Edition of FMC
- ◆ Juniper Netscreen 5400 and 5200, SRX 3600, 3400, 650 and 240 Series Firewalls running
- ◆ Cisco Networking Hardware: Nexus 5K, 7K, 7600, 7200, 3800, 3600, 2800 Series Routers and Cisco 6500, 4900, 4500, 3750, 3560, 2900 series switches.
- ◆ Ruckus Networking Hardware: ICX model switches.
- ◆ Experience in configuring Extreme network switches and routers.

LAN/WAN:

- ◆ OSI Layer, TCP/IP, WAN Routing Protocols RIP V2, EIGRP, OSPF, BGP. Layer 2 WAN Protocols MPLS, Frame Relay. High Availability configurations including HSRP, VRRP and Spanning Tree Protocols STP, RSTP, MST. Dot1q Trunk.
- ◆ Network Management Protocols including SNMP, SYSLOG. Sniffer tools like Wire Shark, Packet Capture.

Security:

- ◆ Wire Shark / Sniffer capture for packet level analysis. (TCPDUMP and packet capture)
- ◆ OPsec Client based access for Firewall Optimization tools such as Tufin, AlgoSec etc.
- ◆ Security Implementations including multiple Zones (DMZ, Third-party, ASZ etc.)
- ◆ Advanced NAT including Identity, Static, Policy static etc

Additional Skills

- ◆ Troubleshooting of Point to Point WAN Circuits, Frame Relay, ATM, and MPLS.
- ◆ VLAN configurations, 802.1q trunking, and spanning tree, VTP, IP Subnetting, VLSM. NAT, IPSec based VPN, IPSec VPN Tunnels, VOIP,
- ◆ DNS, DHCP, Active Directory, IIS, Syslog, OPsec, NMAP, SNMP v2 & v3, load balancing and high availability.
- ◆ Packet level troubleshooting using sniffer tools like Ethereal, Packet capture tools using ASA Firewall CLI, ASDM and CSM (Cisco Security Manager)
- ◆ Basic knowledge and experience in Pearl scripting for API and network automation
- ◆ Documentation Tools: Rational Requisite Pro, MS Word, Excel, PowerPoint, MS Project, Visio and Rational Rose, MS Access.



Education

Bachelor of Computer Science,
Jawaharlal Nehru Technological
Univ., India

Masters in Computer Science,
California, USA

Certifications and Training

Cisco Certified Network Associate
(Routing & Switching and
Security) (CCNA)

Check Point Certified Security
Expert (CCSE)

Check Point Certified CloudGuard
IaaS Public Cloud Administrator
(CCVSA)

Palo Alto Networks Certified
Network Security Engineer
(PCNSE)

Fortinet Network Security Expert
5 (NSE5)

Vishal Maheshwaram

Network and Security Engineer

MGT Consulting

Proposed Role: Security Operations Center
Analyst

Summary

Network Security engineer with 5+ years of experience implementing, migrating IT Network Security technologies like Firewalls, Routers, Switches, IDS/IPS, VPNs and performing Vulnerability Assessment of Network Infrastructure.

Relevant Professional Experience

- ◆ Cira Infotech Inc (Various Customers) | Network & Security Engineer | Present
- ◆ DXC Technology | Network and Security Engineer | 2017 – 2020
- ◆ Hewlett Packard | Network and Security Engineer | 2015 – 2017

Clients

- ◆ City of Lawrenceville GA,
- ◆ Spelman College
- ◆ Piedmont Cancer Institute Comanche County Memorial Hospital
- ◆ Atlantis National Services
- ◆ First Bank Richmond
- ◆ Tuskegee University
- ◆ Hewlett Packard Inc
- ◆ Hewlett Packard Enterprise
- ◆ DXC Technology
- ◆ Microfocus
- ◆ Brunswick Corporation
- ◆ Rhode Island Airport Corporation
- ◆ Silicon Valley Clean Energy



Technical Experience

Engineering

- ◆ Technical hands-on experience in Network & Security products like Firewalls, LAN, WAN, Routing & Switching, Endpoint security, SIEM products
- ◆ Understanding of various industry leading IT Network Security products and features
- ◆ Experience working with Checkpoint, Fortinet, Palo Alto, Cisco and Trend Micro Products
- ◆ Perform Vulnerability Assessment on the Network Infrastructure and provide a detailed overview to Leadership and Engineers.

Achievements

- ◆ Lead Engineer –Get all Network and Security devices at HPE VPC spread across 22 data centers worldwide qualify to host PCI Data.
- ◆ Install and configure 100+ firewalls in span of 6 months for HP Inc and HPE Split.
- ◆ Fortinet SME – Mergers, Acquisitions, Divestiture and Outsourcing (MADO) project for DXC Technology in terms of Network Security implementations across APJ, EMEA and AMS datacenters.
- ◆ Perform Network IP Addressing schema refresh across AMS, APJ and EMA DC's for sold Class A public subnets
- ◆ Lead Engineer at DXC Technology to build Leveraged Service Zone at 4 different geographical locations shared across HP Inc, HPE and DXC



Education

Bachelor's Degree : 05/2019

Christian Brothers University -
Memphis, TN

Double Major:

Computer Science with Electrical
Engineering concentration

Cybersecurity and Digital
Forensics

Graduated Magna Cum Laude
(3.71 M, 3.53 C)

Certifications

CHFI - Computer Hacking Forensic
Investigator, EC-Council, April '21

CEH(v10) –Certified Ethical
Hacker, EC-Council, May '18

InsightIDR –Certified Specialist

Technical Skills

Python, Java, C, C++, Bash,
JavaScript, Swift, C#, MySQL, VB,
D3

Unix, Linux and Windows

Experience with IOS/Android app
development Unity 3d, Android
Studio, XCode



Sriya Rao

Network Operations Security Engineer
MGT Consulting

Proposed Role: NOC Engineer

Summary

An experienced Network Security Operations Center (NOC) Engineer with multiple years of direct managed security technical knowledge. His technical experience includes design, installation, configuration and supporting of network & security products. Significant experience on industry leading Network and Security appliances including Security Operations Center (SOC) Managed Detection and Response services and products, SIEM integration, and Firewall endpoint analysis (PaloAlto, Checkpoint, Fortinet, Cisco Meraki). Knowledge in penetration testing and vulnerability assessment tools, like Solarwinds, Qualys and Nessus. Unsurpassed customer service, dedicated, positive, team-oriented attitude with proven leadership and success in highly visible roles for various sized project implementations.



Relevant Technical Experience

SOAR Dashboard (Python, JavaScript)

Built a dynamic web application for integrating all the Security tools alerts in one place using RESTful APIs in python.

Spam Tracer (Python)

Built a Burp-Suite Plugin that extracts signatures of Malicious Popup Ad by reverse engineering the proxy history captured by Burp.

Phish Response (Visual Basic)

Built an outlook plugin/add-in used for automatically extracting phishing email senders & URLs and later blocking them.

Scour IOS/Android App (Java, Swift)

Built a mobile application which helps in regenerating a malicious popup ad for reverse engineering purpose.

Spyder (Python)

Built a Web scraping Tool for populating all the external domain URLs in a graphical display.



Work Experience

Penetration Tester, Cira Infotech (Alpharetta, Georgia)

January 2021 - Present

- ◆ Network and Web Application pen-testing
- ◆ Security and Vulnerability Assessments
- ◆ Network Forensics - Deep Packet Traffic Analysis (Wireshark)
- ◆ Most Kali Tools - Primarily BurpSuite; Forensic Tools - Autopsy and FTKImager
- ◆ IoT Pen-testing and Digital Forensics
- ◆ Reverse Engineering and Malware Analysis

Information Security Engineer, Cira Infotech

May 2020 - Present

- ◆ Security Operations Center- MDRteam, Rapid7-SIEM
- ◆ Firewalls and endpoints analysis – PaloAlto, Checkpoint, Fortinet, Cisco Meraki
- ◆ Incident Response and Forensic Analysis

Information Security Analyst, St. Jude's Children Hospital – ALSAC (Memphis, TN)

2019 - 2020

- ◆ Security Operations Center- MDRteam, Rapid7-SIEM
- ◆ Built security tools for automation
- ◆ Analyzed emails and URLs for Phishing Content - Proofpoint
- ◆ Static and Dynamic code analysis – Checkmarx, Burpsuite
- ◆ Worked with Endpoint Protection (ENP) - McAfee EPO and ENS Trained
- ◆ Incident Response - Rapid7 IDR and LogRhythm
- ◆ Penetration testing and vulnerability assessments – Kali Linux and Parrot
- ◆ Third party vendor Risk Assessments – AllgressGRC

Course Instructor, Udemy

September 2019 – November 2019

- ◆ Via Dream Vision IT LLC, Instructed Course: IT Security Gumbo – Exploitation with Kali

Cyber Security Analyst (Malware) Intern/ Software Engineer Intern, Devcon-AdTech Security (Memphis, TN)

2018- 2019

Cybersecurity Analyst (Malware) Intern:

- ◆ Reverse engineering exploits and decoding obfuscated Scripts
- ◆ Performed cybersecurity investigations and technical analysis of malware/malvertising attacks
- ◆ Pen-tested mobile and web applications; Worked with DevOps

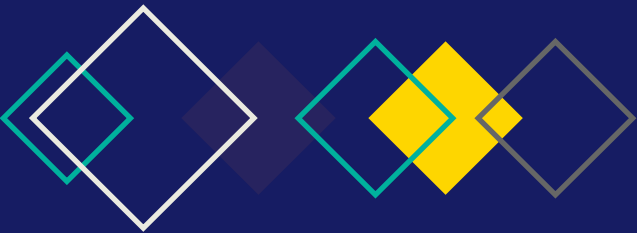
Software Engineer (Security) Intern

- ◆ Worked with machine learning experts to automate detection and track exploits by building multiple security tools and mobile applications that increased productivity by 50% and eliminated manual work

Cybersecurity Consultant Intern, Sawyers & Jacobs, LLC (Memphis, TN)

2017 -2018

- ◆ Created mobile app for cybersecurity risk assessment and profile using Java and
- ◆ Performed vulnerability scans of client networks
- ◆ Worked on an email whaling project



Education

M.S. Computer Engineering.

B. Tech – Electronics and Communication Engineering)

Certifications and Training

LogRhythm Platform Administrator.

LogRhythm Security Analyst.

EXTRAHOP User Certification.

Checkpoint Certified Security Expert.

Cisco Certified Network Associate

Palo Alto Networks Certified Network Security Administrator.

Palo Accredited Configuration Engineer



Siva Kallam

SOC Manager and Senior Cyber Security Engineer

MGT Consulting

Proposed Role: SOC Lead

Summary

A certified security engineer having 10 years' experience in mission-critical enterprise Data Center environments with extensive exposure to clustered firewalls, Cisco based Routing and Switching, , IPS devices, SIEM, PCI ASV Scans, proxies. Mr Kallam is proficient in design, implementation, management and troubleshooting of SIEM Solution, Incident Detection and Response (IDR), Network Detection and Response (NDR), End Point Detection and Response (EDR) as well as Next Generation Palo Alto Firewalls, Check Point Security Gateways (including GAIA), RAPID 7 PCI ASV Scans, Dell SecureWorks IPS, Cisco ASA firewalls and Fortinet. He has experience implementing SIEM Solution from Ground and manage all the components of SIEM and has been actively responsible for Managed Detection and Response (MDR) team to effectively prepare, detect, and respond to incidents.

Skills Mr. Kallam Brings to This Engagement

- ◆ Perform analysis of log files from a variety of sources (e.g., network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security
- ◆ Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation
- ◆ Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs)
- ◆ Worked on Enterprise scale Management platforms such as Panorama on Palo Alto, Checkpoint, Fortinet Forti Manager and Cisco Security Manager CSM for Cisco ASA, FMC.

- ◆ Build VPN for B2B Communications and remote access VPN including SSL VPN.
- ◆ Configuring F5 load balancers to enable load sharing and load balancing among web servers.
- ◆ Experience with forward and reverse proxy using Blue Coat appliances in explicit mode.
- ◆ Identify and troubleshoot network connectivity issues through firewall using Command line utilities such as Tcpdump, FW-Monitor and review with Wireshark.
- ◆ Configuring and implementing Routed and Routing protocols including: OSPF, EIGRP and BGP.
- ◆ Experienced in implementing / maintaining compliance with security and IT standards such as ISO 27001, and SOC2 Type2 as well as PCI with remediation.
- ◆ Strong troubleshooting and communication skills with proficiency in grasping new technical concepts quickly and utilising the same in a productive manner.
- ◆ Ability to create HTTP/URL/DNS Regular Expressions to stop low level attack traffics
- ◆ Experience with Tufin for firewall policy clean up and remediation

Professional Experience

- ◆ Multiple SLED Accounts | Senior Information Security Analyst | May 2018- Present
- ◆ Spelman College, Atlanta | Network Security Consultant | May 2016 – Dec 2017
- ◆ Verizon, North Carolina | Network Security Engineer | Jan 2015 – Apr 2016
- ◆ TATA Communications | Network Security Engineer | Jan 2013 – July 2014

Technical Skills

Firewalls/IDS	Palo Alto firewalls including PA 5k, 3K and 2k appliances and Managed through PANORAMA M100 series. Check Point 15k, 13k, 12k, 5k, 4k appliances running Gaia, FortiGate's 200E, 3700D, 3600C, 1000C, 300C, 500D, 90D, and Cisco ASA 5585X, 5555X, 5540, 5525 Firewalls with FIREPOWER services.
Scanning Vendors	RAPID 7 COALFIRE for ASV Scanning, RAPID 7 INSIGHT VM for internal.
SIEM	Rapid7 InsightIDR, LogRhythm and Splunk.
Threat Intelligence	Recorded Future, Proofpoint, Dell SecureWorks, Palo Alto and Cisco Umbrella.
Load Balancers	F5 LTM and GTM products.
Protocols	TAXII, IPSEC, BGP, EIGRP and OSPF.
Operating Systems	Palo Alto PAN OS 9.x, 8.x, 7.x, 6.x, Panorama 8.x, 7.x. LogRhythm Version 7.2.5, 7.2.7, 7.4.4 and 7.4.9. Checkpoint GAIA versions including R80.10, R77.30, R77.20, R77.10.
Authentication	2FA (2 factor Authentication using RSA), Radius, TACAS, LDAP.
Routers	Cisco ASR/ISR Series 7204/7206VXR/3825/3745
Switches	Cisco Nexus 9k, 7k, 5k, 2k as well as Catalyst 6500, 4500, 3750

Appendix B: ISO Certificate



PERRY JOHNSON REGISTRARS, INC.

Certificate of Registration

*Perry Johnson Registrars, Inc., has audited
the Information Security Management System of:*

Cira Info Tech Inc
5755 North Point Parkway, Suite 82, Alpharetta, GA 30022 United States

*(Hereinafter called the Organization) and hereby declares that
Organization is in conformance with:*

ISO/IEC 27001:2013

This Registration is in respect to the following scope:

The IT Managed Services and Security Operations Center Support

(Statement of Applicability Version 2.0 Dated January 2018)

*This Registration is granted subject to the system rules governing the Registration referred to above, and the
Organization hereby covenants with the Assessment body duty to observe and comply with the said rules.*



Terry Boboige

Terry Boboige, President

Perry Johnson Registrars, Inc. (PJR)
755 West Big Beaver Road, Suite 1340
Troy, Michigan 48084
(248) 358-3388

The use of the UKAS accreditation symbol is in respect to the activities covered by the Accreditation Certificate Number 0105.

The validity of this certificate is dependent upon ongoing surveillance.

Effective Date:
January 9, 2020

Expiration Date:
January 4, 2023

Certificate No.:
C2020-00285

Appendix C: Financial Statements

Please see our financial statements on the following pages of this section.

**MGT of America, LLC
and Subsidiaries**

September 30, 2020 and 2019

**Consolidated Financial Statements and
Independent Auditor's Report**



Table of Contents

Independent Auditor's Report.....	3-4
Consolidated Balance Sheets as of September 30, 2020 and 2019.....	5
Consolidated Statements of Operations for the fiscal years ended September 30, 2020 and 2019.....	6
Consolidated Statements of Changes in Members' Equity for the fiscal years ended September 30, 2020 and 2019.....	7
Consolidated Statements of Cash Flows for the fiscal years ended September 30, 2020 and 2019.....	8
Notes to Consolidated Financial Statements.....	9-17

INDEPENDENT AUDITOR'S REPORT

To the Members
MGT of America, LLC and Subsidiaries
Tampa, Florida

We have audited the accompanying consolidated financial statements of MGT of America, LLC and Subsidiaries ("Company"), which comprise the consolidated balance sheets as of September 30, 2020 and 2019, and the related consolidated statements of operations, consolidated statements of changes in members' equity, and consolidated statements of cash flows for the years then ended, and the related notes to the consolidated financial statements.

Management's Responsibility for the Consolidated Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with accounting principles generally accepted in the United States of America; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of the consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditor's Responsibility

Our responsibility is to express an opinion on these consolidated financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating overall presentation of the consolidated financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Experienced, resourceful and passionate about your needs

INDEPENDENT AUDITOR'S REPORT (Continued)

Opinion

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of MGT of America, LLC and Subsidiaries as of September 30, 2020 and 2019, and the results of their consolidated operations and their consolidated cash flows for the years then ended in accordance with accounting principles generally accepted in the United States of America.

LS + Company

Is and company

St. Petersburg, FL
January 28, 2021

MGT of America, LLC and Subsidiaries
Consolidated Balance Sheets
As of September 30, 2020 and 2019

	2020	2019
Assets		
Current Assets:		
Cash and cash equivalents	\$ 4,225,845	\$ 537,580
Accounts receivable, net	3,647,068	3,731,593
Due from related parties	-	107,148
Unbilled receivables	5,043,159	4,191,165
Deferred contract costs	77,681	665,960
Prepaid expenses	247,084	114,954
Total current assets	13,240,837	9,348,399
Property and equipment, net	533,914	617,681
Goodwill	4,830,435	4,830,435
Intangibles, net	217,903	253,753
Deposits	19,895	30,672
Total other assets	5,602,147	5,732,542
Total assets	\$ 18,842,984	\$ 15,080,941
Liabilities and members' equity		
Current liabilities:		
Accounts payable	\$ 909,744	\$ 548,946
Accrued liabilities	3,632,548	2,010,562
Lines of credit	-	3,041,968
Deferred revenue	267,869	588,501
Term Loan, current portion	-	322,111
PPP Loan, current portion	252,565	-
Related party notes payable, current portion	-	140,662
Total current liabilities	5,062,726	6,652,751
Long-term liabilities:		
Term loan, less current portion	-	567,404
PPP loan, less current portion	2,013,507	-
Related party notes payable, less current portion	-	1,481,068
Total long term liabilities	2,013,507	2,048,472
Total liabilities	7,076,233	8,701,223
Members' equity:	11,766,751	6,379,718
Total liabilities and members' equity	\$ 18,842,984	\$ 15,080,941

Read accompanying Independent Auditor's Report and Notes to Consolidated Financial Statements.

MGT of America, LLC and Subsidiaries
Consolidated Statements of Operations
For the Fiscal Years September 30, 2020 and 2019

	<u>2020</u>	<u>2019</u>
Revenue	\$ 29,168,923	\$ 25,789,731
Salaries and benefits	19,005,063	16,219,455
Contract labor	5,059,350	2,793,294
Travel	944,128	1,773,996
	<u>25,008,541</u>	<u>20,786,745</u>
Gross profit	<u>4,160,382</u>	<u>5,002,986</u>
General and administrative expenses		
Operating expenses	4,013,990	2,316,607
Occupancy	520,934	445,285
Interest	425,276	320,297
Depreciation and amortization	261,794	244,703
Total general and administrative expenses	<u>5,221,994</u>	<u>3,326,892</u>
Other income	19,192	174,237
Net income (loss)	<u>\$ (1,042,420)</u>	<u>\$ 1,850,331</u>

Read accompanying Independent Auditor's Report and Notes to Consolidated Financial Statements.

MGT of America, LLC and Subsidiaries
Consolidated Statement of Members' Equity
For the Fiscal Years Ended September 30, 2020 and 2019

	Total	Common Units	Preferred Units
September 30, 2018	\$ 4,342,727	\$ 3,851,172	\$ 491,555
Net income before taxes	1,850,331	1,850,331	-
Priority charges	-	(117,063)	117,063
Common units vested	218,280	218,280	-
Distributions	(31,620)	(31,620)	-
September 30, 2019	\$ 6,379,718	\$ 5,771,100	\$ 608,618
Net loss before taxes	(1,042,420)	(1,042,420)	-
Priority charges	-	(67,955)	67,955
Common units vested	316,427	316,427	-
Common units issued	10,327,789	10,327,789	-
Units redeemed	(4,214,763)	(3,538,190)	(676,573)
	<u>\$ 11,766,751</u>	<u>\$ 11,766,751</u>	<u>\$ -</u>

Read accompanying Independent Auditor's Report and Notes to Consolidated Financial Statements.

MGT of America, LLC and Subsidiaries
Consolidated Statement of Cash Flows
For the Fiscal Years Ended September 30, 2020 and 2019

	2020	2019
Cash flow from operating activities		
Net loss	\$ (1,042,420)	\$ 1,850,331
Adjustments to reconcile net loss to net cash provided by (used in) operating activities:		
Depreciation and amortization	261,794	244,703
Change in allowance for bad debts	92,875	140,692
Employee units vested	316,427	218,280
Change in operating assets and liabilities		
Accounts receivable, net	(22,127)	21,516
Due from related parties	120,721	(75,090)
Unbilled receivables	(851,995)	(2,219,936)
Deferred contract costs	588,279	(665,960)
Prepaid expenses	(132,130)	80,089
Deposits	10,777	234,849
Accounts payable	360,798	113,545
Accrued liabilities	1,622,192	159,222
Deferred revenue	(320,634)	588,501
Net cash from operating activities	1,004,557	690,742
Cash flow from investing activities		
Purchase of property and equipment	(142,177)	(323,394)
Issuance of units	10,327,789	-
Distributions to members	-	(31,620)
Net cash from (used) by investing activities	10,185,612	(355,014)
Cash flow from financing activities		
Proceeds from PPP Loan	2,266,072	-
Borrowings under VNB line of credit, net	-	(1,122,830)
Redemption of common units	(4,214,763)	-
Principal payments on term loan	(3,931,484)	670,581
Principal payment on related party notes payable	(1,621,730)	(200,714)
Net cash from (used) by financing activities	(7,501,905)	(652,963)
Decrease in cash and cash equivalents	3,688,264	(317,235)
Cash and cash equivalents, beginning of period	537,580	854,815
Cash and cash equivalents, end of period	\$ 4,225,845	\$ 537,580

Read accompanying Independent Auditor's Report and Notes to Consolidated Financial Statements.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

1. Description of Business

MGT of America, LLC (MGT) along with its principal subsidiaries (MGT of America Consulting, LLC and Strategos Public Affairs, LLC) (collectively called “the Company”) is a nationwide professional services firm that delivers a diverse range of consulting services to public and public related agencies in the following lines of service: financial services, educational transformation, PK-12, higher education, facilities, disparity, human resources, and cyber security.

2. Basis of Presentation and Consolidation

The accompanying audited consolidated financial statements of the Company have been prepared in accordance with accounting principles generally accepted in the United States of America (“U.S. GAAP”) and reflect the financial statement presentation and disclosure requirements thereunder. The consolidated financial statements include the accounts of MGT along with its subsidiaries as noted above. All significant intercompany transactions have been eliminated in consolidation.

Certain prior balances have been reclassified to conform with current year presentation. These reclassifications had no effect on previously reported net income or total equity.

3. Summary of Significant Accounting Policies Under US GAAP

Use of Estimates

The preparation of consolidated financial statements in conformity with US GAAP requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying disclosures. Actual results could differ from those estimates.

Cash and Cash Equivalents

The Company considers all highly liquid investments with a maturity of three months or less when purchased to be cash equivalents. Cash and cash equivalents include cash or deposits with financial institutions and deposits in highly liquid money market securities. Deposits with financial institutions are insured by the Federal Deposit Insurance Corporation (FDIC) up to \$250,000 per depositor. Bank deposits at times may exceed federally insured limits. Amounts over the FDIC insurance limit as of September 30, 2020 and 2019 were approximately \$3,870,000 and \$317,000, respectively.

Accounts Receivable, Net

The Company carries its accounts receivable at face value less an allowance for doubtful accounts. The allowance for doubtful accounts is established to cover probable and reasonably estimable losses. The Company evaluates its accounts receivable and establishes an allowance for doubtful accounts based on historical experience, aging analyses, specifically identified troubled receivable balances that are past due and other currently available information, including macroeconomic factors. Uncollectible receivables are charged to bad debt expense when that determination is made. Bad debt expense for the year ended

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

3. Summary of Significant Accounting Policies Under US GAAP - Continued

September 30, 2020 and 2019 was \$79,000 and \$146,000, respectively. Allowance for doubtful accounts was \$75,000 and \$168,000 for the fiscal years ended September 30, 2020 and 2019.

Property and Equipment, Net

Property and equipment are carried at cost, net of accumulated depreciation and amortization. Maintenance repairs and minor improvements are expensed as incurred. Depreciation is computed using the straight-line method of depreciation over the estimated useful lives of the assets, as follows:

Technology equipment and software	3 to 5 years
Furniture and fixtures	15 years
Leasehold improvements	Term of lease

Goodwill and Intangible Assets

Goodwill consists of the excess of purchase price over the fair value of identifiable net assets of companies acquired. In accordance with the Accounting Standards Codification (“ASC”) 350 “Intangibles-Goodwill and Other”, the carrying amount of goodwill and intangible assets is to be reviewed at least annually for impairment, and losses in value, if any, will be charged to operations in the period of impairment. Accounting Standards Update 2011-8 permits an entity to evaluate qualitative factors to assess whether impairment is more likely than not to have occurred. The test for impairment was completed for the years ended September 30, 2020 and 2019. Goodwill was determined to not be impaired for the fiscal years ended September 30, 2020 and 2019.

In June 2019, partners of Fiscal Choice joined the Company. They were given one-year employment agreements with earn out targets of \$100,000 if performance metrics were met. In August 2017, the Company acquired the assets of Anderson Strickler (AS), a management consultancy firm for \$50,000 at closing and \$286,000 payable over the next three years based on AS achieving certain earn out targets. Earn out targets were not met for the first payoff of \$50,000 due in August 2018 except for the guarantee of \$25,000. The remaining targets to achieve the additional payouts in 2019 were not met and goodwill was adjusted by \$211,000 to reflect that these payoffs would not occur.

Intangible assets are recorded at their estimated fair value at the date of acquisition. Intangible assets are amortized using the straight-line method over 15 years. Intangible assets are reviewed for impairment whenever events or changes in circumstances indicate the carrying value may not be recoverable. Assets that are deemed to be potentially impaired are evaluated for recoverability based upon management’s estimates of future discounted cash flows. If the carrying value exceeds the recoverable amount of the asset, the deficiency is recorded as an impairment loss. No fixed or intangible assets impairment charges were recorded for the fiscal years ended September 30, 2020 and 2019.

Fair Value Measurements

The Company’s financial instruments primarily consist of cash, accounts receivable, accounts payable, and debt. The fair value of cash, accounts receivable, and accounts payable approximate carrying value

Read accompanying Independent Auditor’s Report.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

since they are relatively short-term in nature. The carrying value of debt approximates fair value due either to length of maturity or existence of interest rates that approximate the prevailing market rates.

Income Taxes and Priority Charges

The Company operates as a partnership for U.S. federal and state income tax purposes with a calendar year end. Generally, the tax liability related to income earned represents obligations of the individual members and has not been reflected in the consolidated financial statements. In February 2020, the Company amended and restated its Operating Agreement (see Note 10). Under the Company's previous operating agreement, preferred members earn a 4% dividend on capital invested payable at the discretion of management with board approval. This obligation is not charged against earnings but shown as priority charge in the Statement of Changes in Members' equity.

The Company accounts for uncertain tax positions, if any in accordance with FASB Accounting Standards Codification 740. In accordance with these professional standards, the Company recognizes tax positions only to the extent management believes it is "more likely than not" that its tax positions will be sustained upon IRS examination. Management believes it has no uncertain tax positions that qualify for either recognition or disclosure in the consolidated financial statements for the years ended September 30, 2020 and 2019. The Company believes that its income tax filings positions will be sustained upon examination and does not anticipate any adjustments that would result in material adverse effect on the Company's consolidated balance sheet, consolidated statement of operations or consolidated cash flows. Accordingly, the Company has not recorded any accruals for interest and penalties for uncertain income tax positions at September 30, 2020.

The Company's income tax returns are subject to examination by taxing authorities since its formation. At September 30, 2020 the following tax years are subject to examination

<u>Jurisdiction</u>	<u>Open Years for Filed Returns</u>
Federal	December 31, 2017, 2018 and 2019
Various State	December 31, 2017, 2018 and 2019

Revenue Recognition

Revenues include all amounts billable to clients. Revenues are principally recognized as services are rendered by employees of the Company and subcontractors working under the authority of the Company. The impact of performance variances to engagement revenues recognized to date, from changes in expected revenues, are recorded in the period in which these changes become known. Unbilled accounts receivable represents revenues for services rendered and expenses incurred that have not yet been billed. Billings in excess of services rendered are recorded as deferred revenues until the applicable revenue recognition criteria are met. The Company also derives revenues from engagements with incentive-based contracts and other contracts that condition fees on the ability to deliver certain defined goals. Revenues from such engagements are not recognized until a defined goal or milestone is met.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

3. Summary of Significant Accounting policies under US GAAP - Continued

Credit Risks

The Company provides professional services to many geographically diverse customers primarily across the public sector. The Company performs ongoing credit evaluations of its clients and generally does not require collateral. Accounts receivable are reviewed on a periodic basis and an allowance for doubtful accounts is recorded where such amounts are determined to be uncollectible. Due to the large number of client accounts and the type of client base, management does not believe that a significant exposure from a concentration of credit risk exists.

4. Property and Equipment, net

Property and equipment, net consists of the following as of September 30:

	2020	2019
Computers and Software	\$ 542,827	\$ 213,066
Furniture and equipment	353,081	353,081
Leasehold improvements	36,171	36,171
Assets under constuction	168,444	361,017
	1,100,523	963,335
less accumulated depreciation	(566,609)	(345,654)
	\$ 533,914	\$ 617,681

Depreciation expense for the fiscal years ended September 30, 2020 and 2019 was approximately \$221,000 and \$203,000, respectively.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

5. Intangible Assets, net

Intangible assets consist of the following:

	2020	2019	Estimated life (years)
Non-complete agreements	\$ 771,277	\$ 771,277	15
Customer relationships	1,088,000	1,088,000	15
	<u>1,859,277</u>	<u>1,859,277</u>	
less accumulated amortization	<u>(1,641,374)</u>	<u>(1,605,524)</u>	
	<u>\$ 217,903</u>	<u>\$ 253,753</u>	

Amortization expense was approximately \$41,000 and \$42,000 for the years ended September 30, 2020 and 2019, respectively. Estimated future amortization is estimated to be approximately \$40,800 for each of the next five years.

6. Debt

The outstanding balances owed on the Line of Credit as of September 30, 2020 and 2019 were \$0 and \$3,041,968. In February 2020, the Company repaid its lines of credit totaling \$5,150,000 with interest rates of prime plus one percent. The lines of credit are collateralized by all assets of the Company. At September 30, 2020 and 2019, the Company is compliant with all covenants.

In April 2020 the Company received a loan from Valley National Bank in the amount of \$2,266,072 under the Paycheck Protection Program established by the Coronavirus Aid, Relief, and Economic Security (CARES) Act. The loan is subject to a note dated April 16, 2020 and may be forgiven to the extent proceeds of the loan are used for eligible expenditures such as payroll and other expenses described in the CARES Act. No determination has been made as to whether the Company will be eligible for forgiveness, in whole or in part. The loan bears interest at a rate of 1% and is payable in monthly installments of principal and interest over 24 months, with payments commencing in August 2021, after the deferral period. The loan may be repaid at any time with no prepayment penalty.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

6. Debt - Continued

	2020	2019
Term loan due in monthly installment of \$31,486 in 2019 including interest at 5.5% through January 2023, secured by the assets of the Company and guaranteed by a member of the Company.	\$ -	\$ 1,146,179
Term loan due in monthly installments of \$4,500 in 2019 including interest at 5% through October 2019. Secured by all assets of Strategos Public Affairs, LLC	-	4,497
PPP loan due in monthly installments of \$127,215 including interest of 1% through 2022	2,266,072	
	2,266,072	1,150,676
Less current installments of long-term debt	(252,565)	(322,111)
Long-term debt, excluding current installments	2,013,507	828,565
Capitalized loan costs	-	(261,161)
Long-term debt	\$ 2,013,507	\$ 567,404

7. Lease Obligations

The Company leases various operating facilities in Florida, Michigan and California with non-cancelable lease terms through 2025. The leases require payments of taxes and certain other expenses. Office rent expense was approximately \$511,000 and \$445,000 in 2020 and 2019 respectively. The following is a schedule of future minimum rental commitments required under non-cancelable leases that have a minimum initial or remaining non-cancelable lease terms in excess of one year as of September 30, 2020:

September 30,	
2021	\$ 259,000
2022	166,000
2023	39,000
	\$ 464,000

In 2019, computer equipment under lease was purchased for \$243,000 by the Company and recorded as fixed assets. No capital leases exist as of September 30, 2020.

Read accompanying Independent Auditor's Report.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

8. Retirement Plan

The Company has adopted a 401(k)-profit sharing plan. Eligible employees may contribute elective pre-tax deferrals subject to Internal Revenue Service limitations. The Company matches contributions up to 3% of an employee's compensation. Employer contributions vest over a six year period. Total employer contributions for the year ended September 30, 2020 and 2019 were approximately \$207,000 and \$427,000, respectively.

9. Related Party Transactions

In June 2018, the former founders exchanged their preferred interests for long term notes with an original principal balance of \$1,206,000, payable in 96 monthly principal payments of \$12,706 plus interest of 4.25%. In 2014, CPI, a company majority owned by former stockholders of MGT of America, Inc., entered into a loan agreement with an original principal balance of \$1,000,000 with the Company to fund ongoing operations payable monthly through July 15, 2025 plus interest of 6.25%.

Related party notes consist of the following:

	2020	2019
Related party debt due in monthly payments of \$12,706 plus interest of 4.25%	\$ -	\$ 1,026,101
Related party debt due in monthly payments of \$9,288 plus interest of 6.25% Secured by accounts receivable of the Company	-	585,629
Due to member	-	10,000
	\$ -	\$ 1,621,730
Less current installments of long-term debt	-	(140,662)
Long-term debt, excluding current installments	\$ -	\$ 1,481,068

In February 2020, all related party long term notes were repaid in full.

Read accompanying Independent Auditor's Report.

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

9. Related Party Transactions – Continued

For the fiscal years ending September 30, 2020 and 2019, the Company incurred rent expense of approximately \$217,000 and \$198,000; legal and other costs of \$9,000 and \$0; travel costs of \$80,000 and \$98,000, respectively, to entities that are owned by members.

10. Investment by Trivest MGT Investor LLC

In February 2020, the Company issued and sold 478,667.27 Class A Common units, equivalent to 41.9% of the Company's total equity at the transaction date, to Trivest MGT Investor LLC ("Trivest Member") for cash of \$10,600,000. Trivest Member's ownership percentage was subsequently reduced to 37.1% based upon the Company's achievement of agreed upon financial milestones. Concurrent with the transaction, the Company amended and restated its Operating Agreement (the "A&R Operating Agreement"). The Company incurred approximately \$327,000 in transaction expenses in connection with the transaction.

Among other provisions, the A&R Operating Agreement grants the Trivest Member certain preemptive and redemptive rights. The preemptive rights require notice to the Trivest Member no less than 30 days prior to a transaction where securities or instruments are issued, sold or granted by the Company or any of its subsidiaries.

The redemptive rights require, with written notice, the Company to redeem the Trivest Member's Class A common units in the event that certain events do not occur within five years of the A&R Operating Agreement's effective date.

11. Commitments and Contingencies

The Company is involved in litigation arising in the ordinary course of business. Some of the actions and proceedings have been brought on behalf of various claimants and certain of these claimants seek damages of unspecified amounts. While the ultimate outcome of litigation matters cannot be predicted with certainty, it is the current opinion of management that the resolution of such litigation is not likely to have a material adverse effect on the consolidated financial statements.

12. Voting Rights

In February 2020, the Company amended and restated its Operating Agreement as discussed above. The Company had two classes of common units - Class A common units which have total voting rights while Class C common units have limited voting rights and could be redeemed subject to cash availability and board approval. There were 997,387 and 551,622 vested Class A units and 1,142,137 and 713,710 Class A units issued as of September 30, 2020 and 2019, respectively. Class C common units vested and issued

MGT of America, LLC and Subsidiaries
Footnotes to Consolidated Financial Statements
For the Fiscal Years September 30, 2020 and 2019

12. Voting Rights -- Continued

were 22,934 as of September 30, 2019. On June 9, 2019, Class C units of 9,708 were redeemed as part of the related party transaction described in Note 9. On November 22, 2019, Class C units of 12,975 were redeemed and the remaining 9,959 Class C units were redeemed on December 16, 2019.

Preferred units included three types – Preferred A, Preferred B and Preferred C. Preferred A units have no voting rights. They were issued at \$1,000 per unit and were redeemable at any time at the discretion of the Board. They accrued dividends at Prime plus 3% per annum, cumulative and payable with preference over common units. All 687 units issued and outstanding except 59 were redeemed during June 2019 for notes payable – see note 9. Preferred B units have no voting rights. They were issued at \$12 per unit and could be redeemed at any time at the discretion of the Board. They accrue dividends at 5% of Agreed Value, cumulative, payable monthly, with preference over common units. All 65,384 units were redeemed during June 2019 for notes payable. See note 9. Preferred Class C units have limited voting rights and accrue dividends at 4% to be paid at the discretion of the Board with preference over common units. There were 515,205 units outstanding as of September 30, 2019. The outstanding 515,205 Preferred C units were fully redeemed in February 2020. The outstanding 59 Preferred A units were fully redeemed in May 2020.

13. Subsequent Events

On October 1, 2020, the Company acquired CIRA Infotech, Inc. (CIRA), a provider of IT infrastructure managed services and support, for a purchase price of \$6,005,823. The Company drew \$4,500,000 from the available line of credit to fund the transaction.

On November 2, 2020, the Company entered into a credit agreement with CIBC Bank USA. The agreement provides for a Term Loan of \$6,000,000, a delayed draw Term Loan of \$1,200,000, and a revolving line of credit up to \$5,000,000. Proceeds from the term loan were used to fully repay the line of credit referred to above, which was closed.

On December 10, 2020, the Company purchased the assets of Eric Hall & Associates, LLC at a purchase price of \$1,050,000. The seller engages in the business of providing services with respect to human resources, fiscal and budget support and facility services to K-12 schools, school districts and county offices of education in California.

Management has evaluated subsequent events through January 28, 2021, the date on which the consolidated financial statements were available to be issued. No further subsequent events were identified that would require adjustment to, or disclosure in, the consolidated financial statements.

Appendix D: Required Forms

- Identify, if any, proprietary (in-house) technology software the firm intends to leverage to aid in the MSSP offering.
 - Identify security information and event management (SIEM) technology and software (sensory applications, event logging, correlation, and notification, etc.) your firm leverages to provide 24/7/365 MSSP services to the I-Bank.
- j. Provide a statement on whether the company is currently involved with any material litigation, arbitration, or bankruptcy proceedings, or has been within the past three years directly or indirectly.
 - k. Identify any existing or potential conflicts of interest, as well as your representation of parties or other relationships that might be considered a conflict of interest, that may affect or involve transactions for the I-Bank.
 - l. A copy of a valid New Jersey Business Registration must be submitted by the selected firm. If not already registered with the New Jersey Division of Revenue, registration can be completed online at the Division of Revenue website:
<https://www.state.nj.us/treasury/revenue/busregcert.shtml>

VI. Attachments

a. Forms and Other Requirements

The following documents must be completed, included, and submitted with the bid proposal. All forms listed below can be downloaded from the Department of Treasury website:

<http://www.state.nj.us/treasury/purchase/forms.shtml>

The required forms are also attached as **Attachment B – State Requirement Forms.**

1. Ownership Disclosure Form (N.J.S.A. 52:25-24.2)
2. New Jersey Business Registration Certificate. Please provide a copy of your firm's business registration certification (or interim registration) (N.J.S.A. 52:32-44). If the firm is not already registered with the New Jersey Division of Revenue, the form should be completed online at the Division of Revenue website: <https://www.state.nj.us/treasury/revenue/busregcert.shtml>
3. Disclosure of Investigations and Other Actions Involving Bidder Form
4. Disclosure of Investment Activities in Iran (N.J.S.A. 52:32-58)
5. Affirmative Action Employee Report
6. Two-Year Chapter 51/Executive Order No. 117 (Corzine) - Vendor Certification and Disclosure of Political Contributions ("E.O. No. 117")
7. Source Disclosure Form (N.J.S.A. 52:34-13.2; E.O. No. 129 McGreevey)

b. Specific Statutory Requirements

Chapter 51 and Executive Order No. 117. Pursuant to Public Law 2005, Chapter 51 ("Chapter 51") and Executive Order No. 117 (Corzine 2008) ("E.O. No. 117"), State departments, agencies and authorities are precluded from awarding contracts exceeding \$17,500 to vendors who make certain political contributions on and after October 15, 2004, to avoid any appearance that the selection of contracts is based on the contractors' political contributions. Chapter 51 also requires the disclosure of all contributions to any political organization organized under 26 U.S.C. 527 that also meets the definition of a "Continuing Political Committee" within the meaning of N.J.S.A. 19:44A-3(n) and N.J.A.C. 19:25-1.7.

Failure to submit the certification and disclosure form(s) shall be cause for rejection of your institution's proposal. Please consult the website listed below for information and forms relating to Chapter 51 and E.O. No. 117.

<https://www.nj.gov/treasury/purchase/forms/eo134/CH51-FAQ.pdf>

The firm selected pursuant to this RFP shall be required to maintain compliance with Chapter 51 and E.O. No. 117 throughout the term of its engagement.

Chapter 271. Pursuant to Public Law 2005, Chapter 271 ("Chapter 271"), the firm is required to disclose its (and its principals') political contributions within the immediately preceding twelve (12) month period prior to entering into a contract. No prospective firm will be precluded from entering a contract with the State by virtue of the information provided in the Chapter 271 disclosure provided the form is fully and accurately completed. Prior to award of this engagement, the financial institution selected pursuant to this RFP shall be required to submit Chapter 271 disclosures, although completion and submission of the form is not required to be included in your proposal. For a copy of the Chapter 271 disclosure form please refer to: <http://www.state.nj.us/treasury/purchase/forms/CertandDisc2706.pdf>.

If selected pursuant to this RFP, please also be advised of your firm's responsibility to file an annual disclosure statement on political contributions with the NJ Election Law Enforcement Commission ("ELEC") pursuant to N.J.S.A. 19:44A-20.13 (L. 2005, c. 271, section 3) if your firm receives contracts in excess of \$50,000 from a public entity during a calendar year. It is your financial institution's responsibility to determine if filing is necessary. Failure to so file can result in the imposition of financial penalties by ELEC. Additional information about this requirement is available from ELEC at (888) 313-3532 or www.elec.state.nj.us.

c. Source Disclosure Form (N.J.S.A. 52:34-13.2; E.O. No. 129 McGreevey)

Chapter 92 and Executive Order No. 129. Pursuant to Public Law 2005, Chapter 92 and Executive Order No. 129 (McGreevey 2002), all services performed pursuant to this engagement shall be performed within the United States of America.

d. Emergency Preparedness

To support continuity of operations during an emergency, including a pandemic, I-Bank needs a strategy for maintaining operations for an extended period of time. One part of this strategy is to ensure that essential contracts that provide critical business services to I-Bank have planned for such an emergency and put contingencies in place to provide needed goods and services.

1. Describe how you anticipate such a crisis will impact your operations.
2. Describe your emergency response continuity of operations plan. Please attach a copy of your plan, or at a minimum, summarize how your plan addresses the following aspects of pandemic preparedness:
 - Employee training (describe your organization's training plan, and how frequently your plan will be shared with employees).
 - Identify essential business functions and key employees (within your organization) necessary

NEW JERSEY INFRASTRUCTURE BANK OWNERSHIP DISCLOSURE FORM

Bid Solicitation Number: Information Technology Managed
Security Services Provider **Vendor Bidder:** MGT of America Consulting, LLC

PART 1: PLEASE COMPLETE THE QUESTIONS BELOW BY CHECKING EITHER THE "YES" OR "NO" BOX.

ALL PARTIES ENTERING INTO A CONTRACT WITH THE AUTHORITY ARE REQUIRED TO COMPLETE THIS FORM PURSUANT TO N.J.S.A.

52:25-24.2 **PLEASE NOTE: IF THE VENDOR BIDDER IS A NON-PROFIT, THIS FORM IS NOT REQUIRED.
PLEASE COMPLETE THE SEPARATE DISCLOSURE OF INVESTIGATIONS FORM.**

- | | YES | NO |
|--|-------------------------------------|-------------------------------------|
| 1. Are there any individuals, corporations, partnerships, or limited liability companies owning a 10% or greater interest in the Vendor Bidder? | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| IF THE ANSWER TO QUESTION 1 IS NO, PLEASE SIGN AND DATE THE FORM.
YOU DO NOT HAVE TO COMPLETE ANY MORE QUESTIONS ON THIS FORM.
IF THE ANSWER TO QUESTION 1 IS YES, PLEASE ANSWER QUESTIONS 2-4 BELOW. | | |
| 2. Of those parties owning a 10% or greater interest in the Vendor Bidder, are any of those parties individuals ? | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3. Of those parties owning a 10% or greater interest in the Vendor Bidder, are any of those parties corporations, partnerships, or limited liability companies ? | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| 4. If your answer to Question 3 is "YES", are there any parties owning a 10% or greater interest in the corporation, partnership or limited liability company referenced in Question 3? | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

IF ANY OF THE ANSWERS TO QUESTIONS 2-4 ARE YES, PLEASE PROVIDE THE REQUESTED INFORMATION IN PART 2 BELOW.

PART 2: PLEASE PROVIDE FURTHER INFORMATION RELATED TO QUESTIONS 2-4 ANSWERED AS "YES".

If you answered "YES" for question 2, 3 or 4, you **must** disclose identifying information related to the individuals, corporations, partnerships, and/or limited liability companies owning a 10% or greater interest in the Vendor Bidder. Further, if one or more of these entities is itself a corporation, partnership, or limited liability company, you must also disclose all parties that own a 10% or greater interest in that corporation, partnership, or limited liability company. This information is required by statute.

TO COMPLETE PART 2, PLEASE PROVIDE THE REQUESTED INFORMATION PERTAINING TO EITHER INDIVIDUALS, CORPORATIONS, PARTNERSHIPS, OR LIMITED LIABILITY COMPANIES HAVING A 10% OR GREATER INTEREST IN THE VENDOR BIDDER. IF YOU NEED TO MAKE ADDITIONAL ENTRIES, CLICK THE "ADD AN ENTRY" BUTTON IN THE APPROPRIATE ENTITY BOX.

Individuals	
Name: _____ Date of Birth: _____	<input type="button" value="Delete Entry"/>
Home Address: _____	
City _____ State _____ Zip Code _____	
Are there additional entities holding a 10% or greater ownership interest in the Vendor Bidder and its parent corporation, partnership or limited liability company? <input type="checkbox"/> Yes or <input type="checkbox"/> No	
<input type="button" value="Add An Additional Individual Entry"/>	

Partnerships/Corporations/Limited Liability Companies

Entity Name: MGT of America Consulting, LLC

Partner Name: MGT of America, LLC is the parent company
that owns the 100%

Business Address: 4320 West Kennedy Boulevard

City Tampa State FL Zip Code 33609

Are there **additional** entities holding a **10% or greater** ownership interest in the Vendor Bidder and its parent corporation, partnership or limited liability company?

Yes or No

Delete Entry

Add An Additional Partnership/Corporation/
Limited Liability Company Entry

In the alternative, to comply with this section, a bidder with any direct or indirect parent entity which is publicly traded may submit the name and address of each publicly traded entity and the name and address of each person that holds a 10 percent or greater beneficial interest in the publicly traded entity as of the last annual filing with the federal Securities and Exchange Commission or the foreign equivalent, and, if there is any person that holds a 10 percent or greater beneficial interest, also shall submit links to the websites containing the last annual filings with the federal Securities and Exchange Commission or the foreign equivalent and the relevant page numbers of the filings that contain the information on each person that holds a 10 percent or greater beneficial interest. N.J.S.A. 52:25-24.2

Certification: I hereby certify that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I certify that I am authorized to execute this form on behalf of the Vendor Bidder; and acknowledge that the New Jersey Infrastructure Bank is relying on the information contained herein and that the Vendor Bidder is under a continuing obligation from the date of this certification through the completion of any contracts with the I-Bank to notify the I-Bank in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the I-Bank, permitting the I-Bank to declare any contract(s) resulting from this certification void and unenforceable.

Signature: 

Date: 02/15/2022

Print Name and Title: Patrick J. Dyer, Vice President

FEIN/SSN: 81-0890071

**STATE OF NEW JERSEY
DEPARTMENT OF THE TREASURY
DIVISION OF REVENUE AND ENTERPRISE SERVICES
SHORT FORM STANDING**

**MGT OF AMERICA CONSULTING, LLC
0600436247**

I, the Treasurer of the State of New Jersey, do hereby certify that the above-named Florida Foreign Limited Liability Company was registered by this office on November 03, 2016.

As of the date of this certificate, said business continues as an active business in good standing in the State of New Jersey, and its Annual Reports are current.

I further certify that the registered agent and office are:

*C T CORPORATION SYSTEM
820 BEAR TAVERN ROAD
WEST TRENTON, NJ 08628*



*IN TESTIMONY WHEREOF, I have
hereunto set my hand and affixed
my Official Seal at Trenton, this
15th day of November, 2021*

A handwritten signature in black ink, appearing to read 'Elizabeth Maher Muoio'.

*Elizabeth Maher Muoio
State Treasurer*

Certificate Number : 6125293592

Verify this certificate online at

https://www1.state.nj.us/TYTR_StandingCert/JSP/Verify_Cert.jsp



NEW JERSEY INFRASTRUCTURE BANK

**3131 PRINCETONPIKE PIKE
BUILDING 4, SUITE 216
LAWRENCEVILLE, NEW JERSEY 08648-2201**

DISCLOSURE OF INVESTIGATIONS AND OTHER ACTIONS INVOLVING THE VENDOR FORM

BID SOLICITATION #: _____ **VENDOR:** _____

PART 1

PLEASE LIST ALL OFFICERS/DIRECTORS OF THE VENDOR BELOW.

IN PART 2 OF THIS FORM, YOU WILL BE REQUIRED TO ANSWER QUESTIONS REGARDING THESE INDIVIDUALS.

OFFICERS/DIRECTORS

NAME	_____
TITLE	_____
ADDRESS 1	_____
ADDRESS 2	_____
CITY	_____ STATE _____ ZIP _____

NAME	_____
TITLE	_____
ADDRESS 1	_____
ADDRESS 2	_____
CITY	_____ STATE _____ ZIP _____

NAME	_____
TITLE	_____
ADDRESS 1	_____
ADDRESS 2	_____
CITY	_____ STATE _____ ZIP _____

Attach Additional Sheets If Necessary.

PART 2

PLEASE COMPLETE THE QUESTIONS BELOW BY CHECKING EITHER "YES" OR "NO".

PLEASE REFER TO THE PERSONS LISTED ABOVE AND/OR THE PERSONS AND/OR ENTITIES LISTED ON THE OWNERSHIP DISCLOSURE FORM WHEN ANSWERING THESE QUESTIONS.

- | | YES | NO |
|---|-----|----|
| 1. Has any person or entity listed on this form or its attachments ever been arrested, charged, indicted, or convicted in a criminal or disorderly persons matter by the State of New Jersey (or political subdivision thereof), or by any other state or the U.S. Government? | | |
| 2. Has any person or entity listed on this form or its attachments ever been suspended, debarred or otherwise declared ineligible by any government agency from bidding or contracting to provide services, labor, materials or supplies? | | |
| 3. Are there currently any pending criminal matters or debarment proceedings in which the firm and/or its officers and/or managers are involved? | | |
| 4. Has any person or entity listed on this form or its attachments been denied any license, permit or similar authorization required to engage in the work applied for herein, or has any such license, permit or similar authorization been revoked by any agency of federal, state or local government? | | |
| 5. Has any person or entity listed on this form or its attachments been involved as an adverse party to a public sector client in any civil litigation or administrative proceeding in the past five (5) years? | | |

IF ANY OF THE ANSWERS TO QUESTIONS 1-5 ARE "YES", PLEASE PROVIDE THE REQUESTED INFORMATION IN PART 3. IF ALL OF THE ANSWERS TO QUESTIONS 1-5 ARE "NO", NO FURTHER ACTION IS NEEDED; PLEASE SIGN AND DATE THE FORM.

PART 3
PROVIDING ADDITIONAL INFORMATION

If you answered "YES" to any of questions 1 - 5 above, you must provide a detailed description of any investigation or litigation, including, but not limited to, administrative complaints or other administrative proceedings involving public sector clients during the past five (5) years. The description must include the nature and status of the investigation, and for any litigation, the caption of the action, a brief description of the action, the date of inception, current status, and if applicable, the disposition.

PERSON OR ENTITY NAME	_____		
CONTACT NAME	_____	PHONE NUMBER	_____
CASE CAPTION	_____		
INCEPTION OF THE INVESTIGATION	_____	CURRENT STATUS	_____
SUMMARY OF INVESTIGATION	_____		

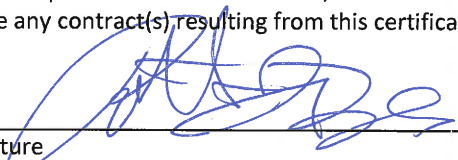
PERSON OR ENTITY NAME	_____		
CONTACT NAME	_____	PHONE NUMBER	_____
CASE CAPTION	_____		
INCEPTION OF THE INVESTIGATION	_____	CURRENT STATUS	_____
SUMMARY OF INVESTIGATION	_____		

PERSON OR ENTITY NAME	_____		
CONTACT NAME	_____	PHONE NUMBER	_____
CASE CAPTION	_____		
INCEPTION OF THE INVESTIGATION	_____	CURRENT STATUS	_____
SUMMARY OF INVESTIGATION	_____		

Attach Additional Sheets If Necessary.

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I may be subject to criminal prosecution under the law, and it will constitute a material breach of my contract(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.



 Signature
 Patrick J. Dyer, Vice President

 Print Name and Title

02/15/2022

 Date

**NEW JERSEY INFRASTRUCTURE BANK
DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN**

Quote Number: Information Technology Managed Security Services Provider Bidder/Offeror: MGT of America Consulting, LLC

**PART 1: CERTIFICATION
BIDDERS MUST COMPLETE PART 1 BY CHECKING EITHER BOX.
FAILURE TO CHECK ONE OF THE BOXES WILL RENDER THE PROPOSAL NON-RESPONSIVE.**

Pursuant to Public Law 2012, c. 25, any person or entity that submits a bid or proposal or otherwise proposes to enter into or renew a contract must complete the certification below to attest, under penalty of perjury, that neither the person or entity, nor any of its parents, subsidiaries, or affiliates, is identified on the Department of Treasury's Chapter 25 list as a person or entity engaging in investment activities in Iran. The Chapter 25 list is found on the Division's website at <http://www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf>. Bidders must review this list prior to completing the below certification. **Failure to complete the certification will render a bidder's proposal non-responsive.** If the Director finds a person or entity to be in violation of law, s/he shall take action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party

PLEASE CHECK THE APPROPRIATE BOX:

I certify, pursuant to Public Law 2012, c. 25, that neither the bidder listed above nor any of the bidder's parents, subsidiaries, or affiliates is listed on the N.J. Department of the Treasury's list of entities determined to be engaged in prohibited activities in Iran pursuant to P.L. 2012, c. 25 ("Chapter 25 List"). I further certify that I am the person listed above, or I am an officer or representative of the entity listed above and am authorized to make this certification on its behalf. **I will skip Part 2 and sign and complete the Certification below.**

OR

I am unable to certify as above because the bidder and/or one or more of its parents, subsidiaries, or affiliates is listed on the Department's Chapter 25 list. I will provide a detailed, accurate and precise description of the activities in Part 2 below and sign and complete the Certification below. Failure to provide such will result in the proposal being rendered as non-responsive and appropriate penalties, fines and/or sanctions will be assessed as provided by law.

PART 2: PLEASE PROVIDE FURTHER INFORMATION RELATED TO INVESTMENT ACTIVITIES IN IRAN

You must provide a detailed, accurate and precise description of the activities of the bidding person/entity, or one of its parents, subsidiaries or affiliates, engaging in the investment activities in Iran outlined above by completing the boxes below.

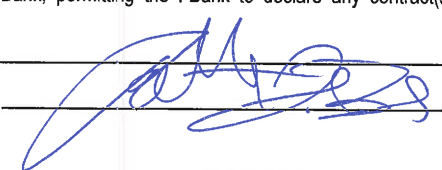
EACH BOX WILL PROMPT YOU TO PROVIDE INFORMATION RELATIVE TO THE ABOVE QUESTIONS. PLEASE PROVIDE THOROUGH ANSWERS TO EACH QUESTION. IF YOU NEED TO MAKE ADDITIONAL ENTRIES, CLICK THE "ADD AN ADDITIONAL ACTIVITIES ENTRY" BUTTON.

Name _____	Relationship to Bidder/Offeror _____
Description of Activities _____	

Duration of Engagement _____	Anticipated Cessation Date _____
Bidder/Offeror Contact Name _____	Contact Phone Number _____

ADD AN ADDITIONAL ACTIVITIES ENTRY

Certification: I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder; that the New Jersey Infrastructure Bank is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the I-Bank to notify the I-Bank in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the I-Bank, permitting the I-Bank to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (Print): Patrick J. Dyer Signature: 

Title: Vice President Date: 02/15/2022

STATE OF NEW JERSEY
Division of Purchase & Property
Contract Compliance Audit Unit
EEO Monitoring Program

EMPLOYEE INFORMATION REPORT

IMPORTANT-READ INSTRUCTIONS CAREFULLY BEFORE COMPLETING FORM. FAILURE TO PROPERLY COMPLETE THE ENTIRE FORM AND TO SUBMIT THE REQUIRED \$150.00 FEE MAY DELAY ISSUANCE OF YOUR CERTIFICATE. DO NOT SUBMIT EEO-1 REPORT FOR SECTION B, ITEM 11. For Instructions on completing the form, go to: http://www.state.nj.us/treasury/contract_compliance/pdf/aa302ins.pdf

SECTION A - COMPANY IDENTIFICATION

1. FID. NO. OR SOCIAL SECURITY FEIN #:81-0890071	2. TYPE OF BUSINESS <input type="checkbox"/> 1. MFG <input checked="" type="checkbox"/> 2. SERVICE <input type="checkbox"/> 3. WHOLESALE <input type="checkbox"/> 4. RETAIL <input type="checkbox"/> 5. OTHER	3. TOTAL NO. EMPLOYEES IN THE ENTIRE COMPANY 250
4. COMPANY NAME MGT of America Consulting, LLC		
5. STREET 4320 West Kennedy Boulevard	CITY Tampa	COUNTY Hillsborough
STATE FL	ZIP CODE 33609	
6. NAME OF PARENT OR AFFILIATED COMPANY (IF NONE, SO INDICATE) MGT of America, LLC		
7. CHECK ONE: IS THE COMPANY: <input type="checkbox"/> SINGLE-ESTABLISHMENT EMPLOYER <input checked="" type="checkbox"/> MULTI-ESTABLISHMENT EMPLOYER		
8. IF MULTI-ESTABLISHMENT EMPLOYER, STATE THE NUMBER OF ESTABLISHMENTS IN NJ 0		
9. TOTAL NUMBER OF EMPLOYEES AT ESTABLISHMENT WHICH HAS BEEN AWARDED THE CONTRACT 0		
10. PUBLIC AGENCY AWARDDING CONTRACT		
Official Use Only	DATE RECEIVED	ASSIGNED CERTIFICATION NUMBER

SECTION B - EMPLOYMENT DATA

11. Report all permanent, temporary and part-time employees ON YOUR OWN PAYROLL. Enter the appropriate figures on all lines and in all columns. Where there are no employees in a particular category, enter a zero. Include ALL employees, not just those in minority/non-minority categories, in columns 1, 2, & 3. *DO NOT SUBMIT AN EEO-1 REPORT.*

JOB CATEGORIES	ALL EMPLOYEES			PERMANENT MINORITY/NON-MINORITY EMPLOYEE BREAKDOWN										
	COL. 1 TOTAL (Cols. 2 & 3)	COL. 2 MALE	COL. 3 FEMALE	***** MALE *****					***** FEMALE *****					
				BLACK	HISPANIC	AMER. INDIAN	ASIAN	NON MIN.	BLACK	HISPANIC	AMER. INDIAN	ASIAN	NON MIN.	
Officials/ Managers	25	10	15	2	6	0	2			2	3	1	9	
Professionals	104	72	32	1	3	0	68			8	7	0	17	
Technicians														
Sales Workers														
Office & Clerical	1	0	1	0	0	0	0			1	0	0	0	
Craftworkers (Skilled)														
Operatives (Semi-skilled)														
Laborers (Unskilled)														
Service Workers														
TOTAL	130	82	48	3	9	0	70			11	10	1	26	
Total employment From previous Report (if any)	33	20	13	3	9	0	1			10	7	0	3	
Temporary & Part-Time Employees	The data below shall NOT be included in the figures for the appropriate categories above.													

12. HOW WAS INFORMATION AS TO RACE OR ETHNIC GROUP IN SECTION B OBTAINED? <input type="checkbox"/> 1. Visual Survey <input checked="" type="checkbox"/> 2. Employment Record <input type="checkbox"/> 3. Other (Specify)	14. IS THIS THE FIRST Employee Information Report Submitted? 1. YES <input checked="" type="checkbox"/> 2. NO <input type="checkbox"/>	15. IF NO, DATE LAST REPORT SUBMITTED MO. DAY YEAR
13. DATES OF PAYROLL PERIOD USED From: _____ To: _____		

SECTION C - SIGNATURE AND IDENTIFICATION

16. NAME OF PERSON COMPLETING FORM (Print or Type) Patrick J. Dyer	SIGNATURE 	TITLE Vice President	DATE MO DAY YEAR 02 15 202
17. ADDRESS NO. & STREET 4320 West Kennedy Boulevard	CITY Tampa	COUNTY Hillsborough	STATE Florida
ZIP CODE 33609	PHONE (AREA CODE, NO., EXTENSION) 888 - 302 - 0899		



Two-Year Chapter 51/Executive Order 117 Vendor Certification and Disclosure of Political Contributions

FOR STATE USE ONLY

Solicitation, RFP, or Contract No. _____ Award Amount _____

Description of Services _____

State Agency Name _____ Contact Person _____

Phone Number _____ Contact Email _____

Check if the Contract / Agreement is Being Funded Using FHWA Funds

Please check if requesting recertification

Part 1: Business Entity Information

Full Legal Business Name MGT of America Consulting, LLC
(Including trade name if applicable)

Address 4320 West Kennedy Boulevard

City Tampa State FL Zip 33609 Phone 888.302.0899

Vendor Email Proposals@mgtconsulting.com Vendor FEIN (SS# if sole proprietor/natural person) 81-0890071

Check off the business type and list below the required information for the type of business selected. MUST BE COMPLETED IN FULL

- Corporation: LIST ALL OFFICERS and any 10% and greater shareholder (If the corporation only has one officer, please write
- Professional Corporation: LIST ALL OFFICERS and ALL SHAREHOLDERS "sole officer" after the officer's name.)
- Partnership: LIST ALL PARTNERS with any equity interest
- Limited Liability Company: LIST ALL MEMBERS with any equity interest
- Sole Proprietor

Note: "Officers" means President, Vice President with senior management responsibility, Secretary, Treasurer, Chief Executive Officer or Chief Financial Officer of a corporation, or any person routinely performing such functions for a corporation.

Also Note: "N/A will not be accepted as a valid response. Where applicable, indicate "None."

All Officers of a Corporation or PC

10% and greater shareholders of a corporation or all shareholders of a PC

All Equity partners of a Partnership

All Equity members of a LLC

A, Trey Traviesa ,Chairman and CEO

Fred Seamon, Executive Vice President

Carla Luke, Chief Financial Officer

Robert Holloway, Senior Vice President

Patrick J. Dyer, Vice President

If you need additional space for listing of Officers, Shareholders, Partners or Members, please attach separate page.

Part 2: Disclosure of Contributions by the business entity or any person or entity whose contributions are attributable to the business entity.

1. Report below all contributions solicited or made during the 4 years immediately preceding the commencement of negotiations or submission of a proposal to any:

Political organization organized under Section 527 of the Internal Revenue Code and which also meets the definition of a continuing political committee as defined in N.J.S.A. 19:44A-3(n)

2. Report below all contributions solicited or made during the 5 ½ years immediately preceding the commencement of negotiations or submission of a proposal to any:

Candidate Committee for or Election Fund of any Gubernatorial or Lieutenant Gubernatorial candidate
State Political Party Committee
County Political Party Committee

3. Report below all contributions solicited or made during the 18 months immediately preceding the commencement of negotiations or submission of a proposal to any:

Municipal Political Party Committee
Legislative Leadership Committee

Full Legal Name of Recipient _____
Address of Recipient _____
Date of Contribution _____ Amount of Contribution _____
Type of Contribution (i.e. currency, check, loan, in-kind) _____
Contributor Name _____
Relationship of Contributor to the Vendor _____
If this form is not being completed electronically, please attach additional contributions on separate page. Click the "Add a Contribution" tab to enter additional contributions.
<input type="button" value="Remove Contribution"/>
<input type="button" value="Add a Contribution"/>

Check this box only if no political contributions have been solicited or made by the business entity or any person or entity whose contributions are attributable to the business entity.

Part 3: Certification (Check one box only)

- (A) I am certifying on behalf of the business entity and all individuals and/or entities whose contributions are attributable to the business entity as listed on Page 1 under **Part 1: Vendor Information**.
- (B) I am certifying on behalf of the business entity and all individuals and/or entities whose contributions are attributable to the business entity as listed on Page 1 under **Part 1: Vendor Information**, except for the individuals and/or entities who are submitting separate Certification and Disclosure forms which are included with this submittal.
- (C) I am certifying on behalf of the business entity only; any remaining persons or entities whose contributions are attributable to the business entity (as listed on Page 1) have completed separate Certification and Disclosure forms which are included with this submittal.
- (D) I am certifying as an individual or entity whose contributions are attributable to the business entity.

I hereby certify as follows:

1. I have read the Information and Instructions accompanying this form prior to completing the certification on behalf of the business entity.
2. All reportable contributions made by or attributable to the business entity have been listed above.

3. **The business entity has not knowingly solicited or made any contribution of money, pledge of contribution, including in-kind contributions, that would bar the award of a contract to the business entity unless otherwise disclosed above:**
- a) Within the 18 months immediately preceding the commencement of negotiations or submission of a proposal for the contract or agreement to:
 - (i) A candidate committee or election fund of any candidate for the public office of Governor or Lieutenant Governor or to a campaign committee or election fund of holder of public office of Governor or Lieutenant Governor; OR
 - (ii) Any State, County or Municipal political party committee; OR
 - (iii) Any Legislative Leadership committee.
 - b) During the term of office of the current Governor or Lieutenant Governor to:
 - (i) A candidate committee or election fund of a holder of the public office of Governor or Lieutenant Governor; OR
 - (ii) Any State or County political party committee of the political party that nominated the sitting Governor or Lieutenant Governor in the last gubernatorial election.
 - c) Within the 18 months immediately preceding the last day of the sitting Governor or Lieutenant Governor's first term of office to:
 - (i) A candidate committee or election fund of the incumbent Governor or Lieutenant Governor; OR
 - (ii) Any State or County political party committee of the political party that nominated the sitting Governor or Lieutenant Governor in the last gubernatorial election.

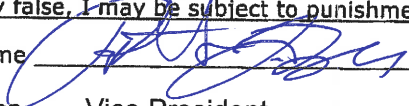
4. During the term of the contract/agreement the business entity has a continuing responsibility to report, by submitting a new Certification and Disclosure form, any contribution it solicits or makes to:

- (a) Any candidate committee or election fund of any candidate or holder of the public office of Governor or Lieutenant Governor; OR
- (b) Any State, County or Municipal political party committee; OR
- (c) Any Legislative Leadership committee.

The business entity further acknowledges that contributions solicited or made during the term of the contract/agreement may be determined to be a material breach of the contract/agreement.

5. During the two-year certification period the business entity will report any changes in its ownership structure (including the appointment of an officer within a corporation) by submitting a new Certification and Disclosure form indicating the new owner(s) and reporting said owner(s) contributions.

I certify that the foregoing statements in Parts 1, 2 and 3 are true. I am aware that if any of the statements are willfully false, I may be subject to punishment.

Signed Name  Print Name Patrick J. Dyer
 Title/Position Vice President Date 02/15/2022

Procedure for Submitting Form(s)

The contracting State Agency should submit this form to the Chapter 51 Review Unit when it has been required as part of a contracting process. The contracting State Agency should submit a copy of the completed and signed form(s), to the Chapter 51 Unit and retain the original for their records.

The business entity should return this form to the contracting State Agency. The business entity can submit this form directly to the Chapter 51 Review Unit only when it -

- Is approaching its two-year certification expiration date and wishes to renew certification;
- Had a change in its ownership structure; OR
- Made any contributions during the period in which its last two-year certification was in effect, or during the term of a contract with a State Agency.

Forms should be submitted either electronically to: cd134@treas.nj.gov, or regular mail at: Chapter 51 Review Unit, P.O. Box 230, 33 West State Street, Trenton, NJ 08625.

NEW JERSEY INFRASTRUCTURE BANK SOURCE DISCLOSURE FORM

Information Technology Managed

SOLICITATION #: Security Services Provider

BIDDER/PROPOSER: MGT of America Consulting, LLC

The Contractor submits this Certification in response to the solicitation issued by the New Jersey Infrastructure Bank (the "I-Bank"), in accordance with the requirements of N.J.S.A. 52:34-13.2.

Instructions:

List every location where services will be performed by the Contractor and all Subcontractors.

If any of the services cannot be performed within the United States, the Contractor shall state, with specificity, the reasons why the services cannot be performed in the United States.

Contractor/Subcontractor Name	Performance Location by Country	Description of Services	Reason Services Cannot Be Performed in U.S.
	Not Applicable. Service will perform within the United States.		

The Contractor shall provide justification that the services cannot be performed in the United States by a contractor. The Director will review this justification and if deemed sufficient, the Director may seek the Treasurer's approval.

Any changes to the information set forth in this Certification during the term of any contract awarded under the referenced solicitation or extension thereof will be immediately reported by the Vendor to the I-Bank.

I understand that, after award of a contract to the Contractor, it is determined that the Contractor has shifted services declared above to be provided within the United States to sources outside the United States, prior to a written determination by the I-Bank that circumstances require the shift of services or that the failure to shift the services would result in economic hardship to the I-Bank, the Contractor shall be deemed in breach of contract, which contract will be subject to termination for cause pursuant to the Terms of the Contract.

I further understand that this Certification is submitted on behalf of the Contractor in order to induce the I-Bank to accept a proposal, with knowledge that the I-Bank is relying upon the truth of the statements contained herein.

Certification: I, being duly sworn upon my oath, hereby represent that the foregoing information and any attachments thereto to the best of my knowledge are true and complete. I acknowledge: that I am authorized to execute this certification on behalf of the bidder; that the New Jersey Infrastructure Bank is relying on the information contained herein and that I am under a continuing obligation from the date of this certification through the completion of any contracts with the I-Bank to notify the I-Bank in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification, and if I do so, I am subject to criminal prosecution under the law and that it will constitute a material breach of my agreement(s) with the I-Bank, permitting the I-Bank to declare any contract(s) resulting from this certification void and unenforceable.

Full Name (print): Patrick J. Dyer

Signature: 

Title: Vice President

Date: 02/15/2022



CERTIFICATION FOR EXECUTIVE ORDER NO. 271 - COVID-19 VACCINE

STATE OF NEW JERSEY
NEW JERSEY INFRASTRUCTURE BANK
3131 PRINCETON PIKE, BLDG.4 STE. 216, LAWRENCEVILLE, NJ 08648

Pursuant to [Governor Murphy's Executive Order No. 271](#) (EO 271) which was signed and went into effect on October 20, 2021, a covered contractor, must have a policy in place:

- (1) that requires all covered workers to provide adequate proof, in accordance with [EO 271](#), to the covered contractor that the covered worker has been fully vaccinated; or
- (2) that requires that unvaccinated covered workers submit to COVID-19 screening testing at minimum one to two times weekly until such time as the covered worker is fully vaccinated; and
- (3) that the covered contractor has a policy for tracking COVID-19 screening test results as required by [EO 271](#) and must report the results to local public health departments.

The requirements of [EO 271](#) apply to all covered contractors and subcontractors, at any tier, providing services, construction, demolition, remediation, removal of hazardous substances, alteration, custom fabrication, repair work, or maintenance work, or a leasehold interest in real property through which covered workers have access to State property.

By signing below, contractor certifies that it shall comply with the requirements [Governor Murphy's Executive Order No. 271](#) if awarded a contract.

02/15/2022

Signature of Contractor's Authorized Representative

Date

Patrick J. Dyer, Vice President

Print Name and Title of Contractor's Authorized Representative

MGT of America Consulting, LLC

Print Contractor's Name