TAB A – COVER SHEET

North Texas SHARE
Your Public Sector Solution Center

REQUEST FOR PROPOSALS
For
Cyber Security Consulting Services
RFP # 2021-043

Sealed proposals will be accepted until **2 PM CT, May 19, 2021** and then publicly opened and read aloud thereafter.

Stealth-ISS Group Inc.
Legal Name of Proposing Firm

Robert Davies — Contact Person
CEO — Title

866-500-0751 — Telephone Number
proposals@stealth-iss.com — E-Mail Address

4601 North Fairfax Drive, Suite 1200 — Street Address of Principal Place of Business
Arlington, Virginia — City/State
22203 — Zip

4601 North Fairfax Drive, Suite 1200 — Complete Mailing Address
Arlington, Virginia — City/State
22203 — Zip

Acknowledgment of Addenda: #1 ✔ #2 _____ #3 _____ #4 _____ #5 _____

By signing below, you hereby certify that the information contained in this proposal and any attachments is true and correct, and may be viewed as an accurate representation of proposed services to be provided by this organization. You agree that failure to submit all requested information may result in rejection of your company's proposal as non-responsive. You certify that no employee, board member, or agent of the North Central Texas Council of Governments has assisted in the preparation of this proposal. You acknowledge that you have read and understand the requirements and provisions of this solicitation and that the organization will comply with the regulations and other applicable local, state, and federal regulations and directives in the implementation of this contract. And furthermore that I certify that I am legally authorized to sign this offer and to submit it to the North Central Texas Council of Governments, on behalf of said offeror by authority of its governing body.

DocuSigned by:
Robert Davies
22E0EECA6FFF474...
Authorized Signature

Brief Statement of Understanding of Work to be Performed and Our Qualifications

The CEO of Stealth-ISS Group® Inc. ("Stealth Group" hereafter), Robert Davies, an authorized company official, is delighted for this opportunity to work with you.

We would like to take a moment to thank you for allowing us to collaborate with you and the SHARE members to help improve your cybersecurity maturity and reduce your risk profile. Our mission is to become your trusted partner, a true collaborator, and not "just another vendor." We look forward to long-lasting business and a mutually beneficial relationship with you.

The North Central Texas Council of Governments (NCTCOG) helps local governments within a 16-county metropolitan region surrounding the cities of Dallas and Fort Worth with planning for common needs, cooperating for mutual benefit, and coordinating for sound regional development. Cybersecurity, and in particular Incident Response (IR), is one of the critical areas where NCTCOG plans to support these local governments. As such, NCTCOG intends to make the contract resulting from this procurement available to other governmental entities through its SHARE cooperative purchasing program.

Your decision to improve your IR capabilities is prudent. Continued, high-profile cyber-attacks and an evolving regulatory landscape mean that public sector entities need to proactively implement capabilities to detect and respond to security incidents. It is becoming unmistakably clear that robust cybersecurity measures are an indispensable investment to combat the risks of ransomware, phishing attacks, and other threats facing your critical infrastructure. In 2020, malware increased by 358% and ransomware increased by 435% over the previous year[1]. Cyber-crime is big business – the crimes reported to FBI's Internet Crime Complaint Center (IC3) exceeded $3.5B in 2019.[2] Adversaries are increasingly targeting public entities to disrupt the lives of citizens and "earn" a huge payout. It is becoming unmistakably clear that proactive implementation of robust cybersecurity measures is an indispensable investment.

You will be served well by Stealth Group, a company whose sole focus is cybersecurity and helping organizations understand their current cyber risk profile and prepare for, or react to, high-risk threats. Established in 2002, Stealth Group is a total service cybersecurity and compliance consulting company that uses its deep domain knowledge to assess and remediate cybersecurity problems of vital importance to the Nation and internationally. Stealth Group is a Federally recognized Service-Disabled Veteran-Owned Small Business (SDVOSB) and Economically Disadvantaged Woman-Owned Small Business (EDWOSB) providing the full portfolio of Cybersecurity Consulting, Regulatory Compliance, Risk Management, and IT security engineering services. Commercially, Stealth Group rose to 167th on the Inc. 5000 fastest growing companies list in 2018, 387th in 2019, and placed in the VET50 list of fastest growing veteran-owned companies in both 2019 and 2020. Cyber Defense Awards recognized our president and founder, Dasha Deckwerth, as one of the top 100 Chief Information Security

[1] Forbes, "Alarming Cybersecurity Stats: What You Need to Know for 2021." March 2, 2021. forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/
[2] FBI, "*2019 Internet Crime Report* Released." February 11, 2020. fbi.gov/news/stories/2019-internet-crime-report-released-021120/

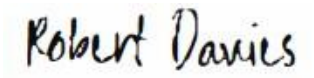
Officers of 2020. Dasha recently became one of the initial 25 candidates to be trained as a provisional assessor for the Department of Defense's new Cybersecurity Maturity Model Certification (CMMC) and Stealth Group has been nominated as a Candidate CMMC Third-Party Assessor Organizations (C3PAO) by the CMMC-AB to protect the DoD's Supply Chain.

Stealth Group does not offer a "one-size-fits-all" approach to cybersecurity, which is why we have won many awards and continue to grow, both in the state and local government and commercial spaces. When you hire Stealth Group, you benefit from a cybersecurity company whose focus is on quality outcomes for you, by way of completely tailored solutions for you, through full collaboration with you, and underpinned by a company culture built on accountability, quality, and integrity.

With over 19 years of demonstrated success in providing innovative cybersecurity solutions, Stealth Group has a wide range of past performance examples in terms of scope, size, scale, and complexity. Previous clients have included: the Departments of Transportation for the states of Texas, New York, and New Jersey; Citi Bank; McGraw-Hill; Deutsche Bank; Xerox/Conduent; Baha Mar Resort and Casino; the Olympic Broadcast Service for the 2016 and 2018 Olympic Games; and numerous other North Atlantic Treaty Organization (NATO) and commercial Fortune 100 clients.

Thank you again for allowing us this opportunity to earn your business; it is our absolute pleasure to work with you. We hope that through our approach and expertise, flexibility, and clear addition of massive value that you will be our next 'raving fan.'

Sincerely,



Robert Davies, CEO
robert.davies@stealth-iss.com

TABLE OF CONTENTS

TABLE OF EXHIBITS

GLOSSARY OF ABBREVIATIONS

Acronym	Definition
AB	Accreditation Board
ACL	Access Control List
AI	Artificial Intelligence
ASP	Application Service Providers
ATP	Advanced Threat Protection
AV	Anti-Virus
BA	Bachelor of Arts
CCCM	Certified Commercial Contracts Manager
CCO	Certified Confidentiality Officer/Business Espionage
CCS	Symantec Control Compliance Suite
CEO	Chief Executive Officer
CERT	Community Emergency Response Team
CFCM	Certified Federal Contract Manager
CGEIT	Certified in the Governance of Enterprise IT
CISO	Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CMMC	Cybersecurity Maturity Model Certification
COM	Component Object Model
CRISC	Certified in Risk and Information Systems Control
CSF	Cyber Security Framework
CSIRT	Cybersecurity Incident Response Team
DHCP	Dynamic Host Configuration Protocol
DLA	Defense Logistics Agency
DLP	Data Loss Prevention
DNS	Domain Name System
DR	Disaster Recovery
DSS	Data Security Standard
EDR	Endpoint Detection and Response
EDWOSB	Economically Disadvantaged Woman-Owned Small Business
EPP	Endpoint Protection Platform
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Modernization Act
FSSI	Federal Strategic Sourcing Initiative
GRC	Governance, Risk, and Compliance

Acronym	Definition
GSA	General Services Administration
HACS	Highly Adaptive Cybersecurity Services
HCISSP	Health Care Security Professional
HIPAA	Health Insurance Portability and Accountability Act
HR	Human Resources
HVA	High Value Assets
IAM	Identity and Access Management
IEEE	Institute of Electrical and Electronics Engineers
IEM	Information Security Evaluation Methodology
INDOPACOM	United States Indo-Pacific Command
IOC	Indicators of Compromise
IP	Internet Protocol
IRP	Incident Response Plan
ISACA	Information Systems Audit and Control Association
ISF	Information Security Forum
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MBA	Master of Business Administration
MWE	Modeled Wage Estimates
NATO	North Atlantic Treaty Organization
NCMA	National Contract Management Association
NCTCOG	North Central Texas Council of Governments
NDA	Non-Disclosure Agreement
NERC	North American Electric Reliability Corporation
NGAV	Next-Generation Anti-Virus
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OBS	Olympic Broadcast Services
OCS	Olympic Channel Services
OS	Operating System
OSSA	Operating System Security Assessment
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
PCIP	Payment Card Industry Professional
PL/SQL	Procedural Language Extensions to the Structured Query Language

Acronym	Definition
PMI	Project Management Institute
PMP	Project Management Professional
POA&M	Plan of Action and Milestones
POS	Point-of-Sale
QSA	Qualified Security Assessor
RACI	Responsible, Accountable, Consulted, Informed
RFP	Request for Proposal
ROE	Rules of Engagement
SANS	SANS Institute – SysAdmin, Audit, Network and Security
SDVOSB	Service-Disabled Veteran-Owned Small Business
SEC	Securities and Exchange Commission
SIEM	Security Information and Event Management
SIN	Special Item Number
SLED	State, Local Government, and Education
SMA	Subject Matter Authority
SOC	Security Operations Center
SP	Special Publication
SQL	Structured Query Language
SSP	System Security Plan
TCP	Transmission Control Protocol
UEBA	User and Entity Behavior Analytics
URL	Universal Resource Locator
USACE	U.S. Army Corps of Engineers
VPN	Virtual Private Network
XML	Extensible Markup Language

TAB B – EXECUTIVE SUMMARY

NCTOG is seeking a third-party organization to support itself and its SHARE cooperative purchasing program members with the development of an Incident Response program, and other cybersecurity services. The primary and secondary objectives for this RFP are as follows:

- **Bid Item #1:** NCTCOG's primary intent is to receive proposals for the selection of a vendor to provide Cyber Security Consulting Services to be hosted on the SHARE Cooperative Purchasing Program. Under the SHARE program, any public entity or non-profit can use the SHARE contract and its selected vendor and pricing to pursue their own projects. This includes the ability to offer products and services nationwide.
- **Bid Item #2:** NCTCOG's secondary intent is to utilize the SHARE awarded contractor to facilitate the creation of an Incident Response capability and Recovery Plan for regional jurisdictions that maps out whom to call and what to do at various stages of incident for the NCTCOG Emergency Preparedness Department and the North Central Texas region.

Our Value Proposition

As a total service cybersecurity and compliance consulting company, there are a number of reasons why we believe we are best placed to work with you on this exciting and strategically important project:

End to End Security Service Provider – We are a one-stop-shop and provide end-to-end security services from advisory, through design and build, and into managed services with our partners. This means that we can help you at every stage of your security journey, from incident response planning, to program development, through actual Incident Response and investigations. It also means that our advice is steeped in realism and based in practical experience.

Incident Response Experience – Our staff have extensive experience with helping organizations develop their cybersecurity and Incident Response programs and respond during actual security events. Our past performance includes being the first line of Incident Response in support of the Winter Olympic Games in the Republic of Korea in 2018. The cyber-attack on the IOC infrastructure prior to the Games is public knowledge (which is why we can mention it here). Our Incident Responders onsite triaged, analyzed the log files, detected the anomalous activities and malware, and performed event correlation to identify threats and intrusions. We were able to assist the Global MSP by finding the most recent non-compromised backup and helped them restore the Games infrastructure such that the Games could continue and be broadcast. Full chain of custody rules were followed, and we worked closely with local, Federal and US security agencies to identify the perpetrator.

Award-Winning Experience – For over 19 years, our tailored cybersecurity solutions have accumulated 'raving fans' – repeat customers in addition to business recognition.

About Stealth Group

Unlike many cybersecurity companies, Stealth Group specializes in tailored cybersecurity solutions specific to our clients' requirements. Our wide variety of services and breadth and depth of our technical knowledge enable us to deliver a solution for every combination of cybersecurity pain points. To be able to deliver fully tailored solutions we see cybersecurity in eight dimensions, where other cybersecurity companies only tend to consider two or three:

1. Organizational Context – You and your business are unique and have a unique set of pain points, configuration, operation, and strategy. One size does not fit all.
2. Industry Vertical – Consideration of Governance, Risk, and Compliance (GRC) guides or mandates specific to your industry. We also consider ISO27K, Information Security Forum (ISF), and other frameworks for gaps that are relevant to your organization in your industry. Being compliant doesn't mean you are secure. Each industry vertical also has its own preferred technologies and way of doing things.
3. People, Process, Technology – We don't just do technology; all three components must be considered together. For example, people are your first line of defense and are often your weakest link. Technology alone will not meet your requirements.
4. Stealth Group Culture – Our culture supports our clients through accountability, integrity, quality, and collaboration. Our culture has only one goal – create raving fans of Stealth Group.
5. Stealth Group Tools and Services – We offer a huge array of industry-leading tools and best practice services, tailored and combined to serve your unique requirements. We review thousands of tools and services; we only choose those that are best of breed and that also deliver massive value.
6. Delivery and Remediation – From Assessment through Remediation, we cover the entire spectrum of cyber, including Cyber Operations, Penetration Testing, Vulnerability Scanning, Incident Response, Forensic Analysis, and Dark Web.
7. Risk vs. Cost – Recommendations are prioritized for you in terms of risk severity and the best remediation combination for the lowest cost.
8. The Future – GRC/Policy changes, Dark Web trends, Blockchain, Internet of Things (IoT), Microsegmentation, Artificial Intelligence (AI), Quantum Computing, Zero Trust – What is coming that you need to anticipate?

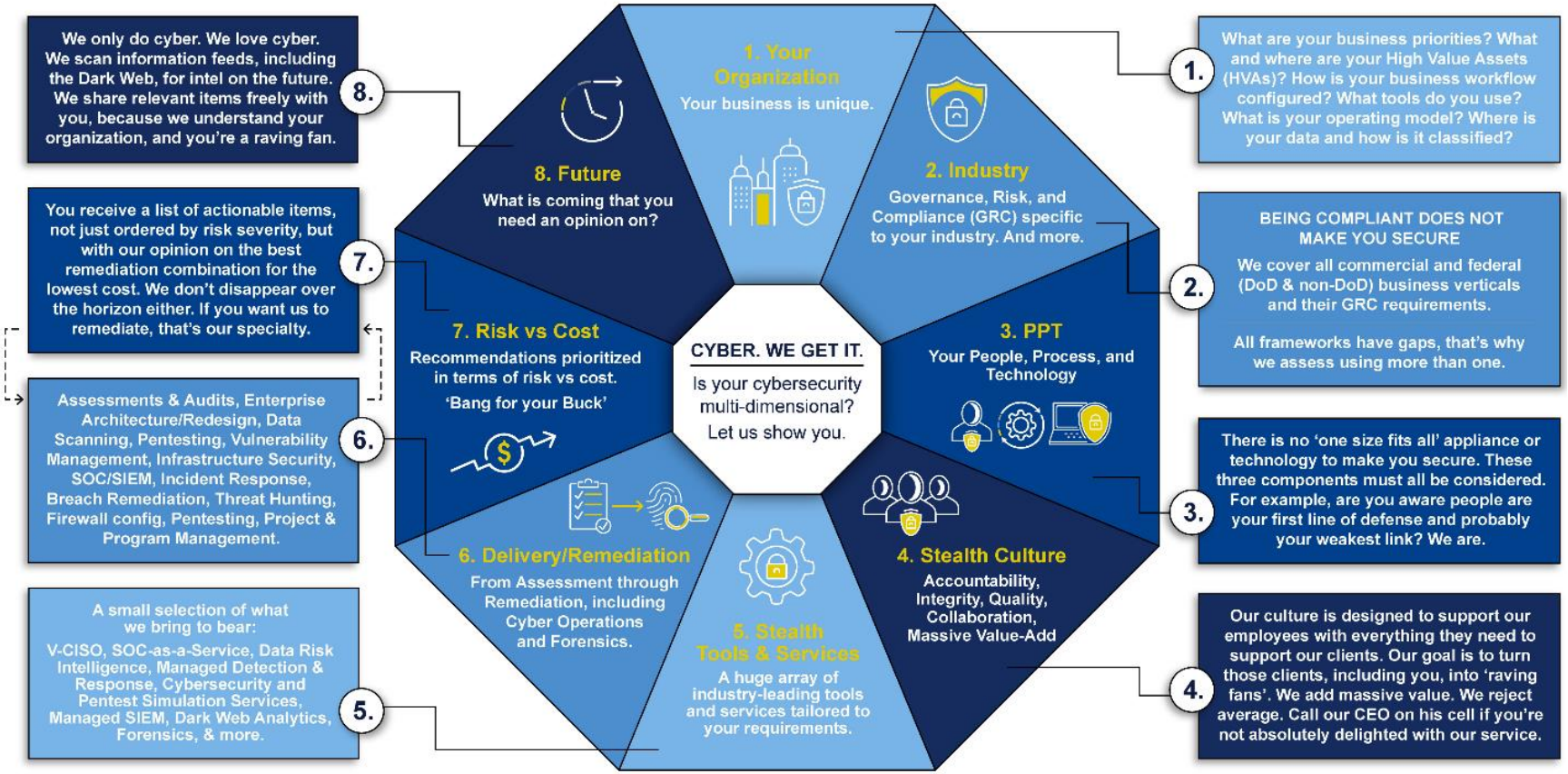


Exhibit 1: Eight Dimensions of Cybersecurity

TAB C – KEY PERSONNEL

We are fully confident that our team is second to none in our quest to meet and surpass your requirements, as we bring massive experience, and the right skills and certifications. Our cybersecurity-certified professionals are experienced in the Commercial, Federal, and State, Local Government, and Education (SLED) security processes, regulatory compliance, vulnerability assessments, penetration testing, and risk mitigation.

Stealth Group will reduce risk by providing a Corporate Governance Board (CGB) to the contract team. This team brings together a highly experienced and credentialed group of individuals who serve as 'the Voice of the Customer' to NCTCOG while effectively decreasing Stealth Group's reliance on NCTCOG oversight – at no additional cost to NCTCOG. The CGB supports the Project Manager (PM) and contract team by providing recommendations for improving performance, as well as guidance on best practices throughout the course of the contract. As NCTCOG and Stealth Group work together to strengthen SHARE members' security programs and cybersecurity defenses, the CGB acts almost as an external QA/auditor to ensure program success. The CGB will be led by Robert Davies, Stealth Group's CEO who was named the 2020 Cybersecurity CEO of the Year for Southern USA in the Global CEO Excellence Awards.

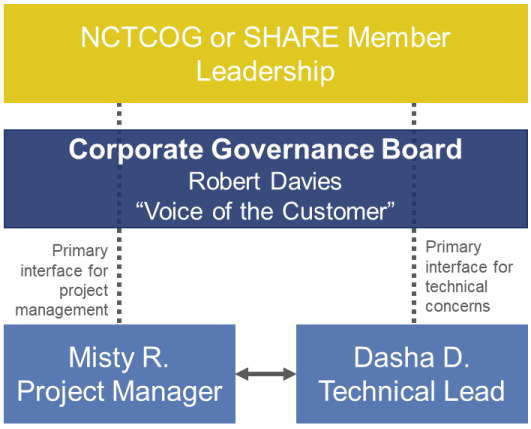


Exhibit 2: Stealth Group Organizational Structure

We have provided, in Appendix A, abbreviated resumes indicative of the quality of our staff members. If the listed candidate is unavailable at the time of the project start, staff similar or equal in experience, qualifications, and certifications will be selected for your review.

Stealth Group Capacity and Resources

Stealth Group has the experience, expertise, and capability to perform 100% of the required tasks and to provide the labor support necessary to meet all your requirements. We have

sufficient financial strength, resources, and capability to accomplish and finance the work in a satisfactory manner and will submit any necessary documentation upon request.

Our Human Resources (HR) Department has developed refined recruiting strategies and maintains substantial candidate databases for each labor category. A stable workforce is necessary for supporting the mission of our customers, and our past and present performance track records are a testament to our commitment to excellent performance.

Stealth Group's cybersecurity experts continually evaluate new technologies and attend industry conferences where technology advancements are discussed and scrutinized. We reward employees who advance their technical education and certifications with tuition reimbursement and monetary bonuses. We evaluate technology trends to ensure that our recommended mitigation techniques reflect the latest advancements in security technologies.

With continuous training of our staff as well as assignment to interesting and challenging projects, we maintain a very low attrition rate among all our staff (Backoffice and IT/Cyber and Engineering). We strive to give our staff a great working environment, with growth opportunities, direct customer interaction, and executive acknowledgement for all successful achievements. With this approach we maintain staff that are not only well integrated with our corporate culture but remain with our clients and the assigned projects most of the time for the entire duration of contracts. This guarantees consistency of delivery, understanding of the project/organization environment, and high satisfaction on your side. Our staff are proud to be working with Stealth Group and for our clients.

TAB D – TECHNICAL PROPOSAL

Bid Item 1 (SHARE Proposal)

We have extensive experience helping organizations build their incident response and cybersecurity programs. This includes helping organizations in the following areas:

- **Incident, Security, and Breach Response**
  - Reviewing existing Incident Response and Security Operations programs.
  - Identifying potential risks of internal and external attacks or data leakage that may cause an impact to your business, or loss of public confidence and trust.
  - Integrating all areas of the business into the incident response process (e.g., PR/Communications, Marketing, Regulatory, etc.) and all affected are aware of their roles and responsibilities when it comes to addressing an incident.
- **Cybersecurity Consulting Services**
  - Performing penetration testing, vulnerability assessments, and architecture reviews
  - Reviewing current posture on best business practices and relevant policy and procedures aligned with business, regulatory requirements, and industry standards.
  - Providing managed security services, including Security Operations Center-as-a-Service (SOCaaS), file integrity monitoring, and simulated penetration testing.
  - Advising organizations on cybersecurity program building and management via our virtual Chief Information Security Officer (vCISO) service.

We will work closely with the SHARE members to help them identify their cybersecurity needs, tailor our services to fit them, and guide them through the program development process. Specific to incident response, we will accomplish this through the following activities:

- **Whiteboarding sessions**: We will hold sessions with your Incident Response stakeholders to identify any concerns or issues they have with the response process. This will help us identify any roadblocks to a successful Incident Response program, dependencies and compliance obligations, and any stakeholders who may have been previously overlooked.
- **Responsibility matrix**: We will help you develop a RACI (Responsible, Accountable, Consulted, and Informed) matrix defining roles within the Incident Response Process (IRP).
- **Communications matrix**: We will help you document escalation requirements within the IRP tied to a communication matrix detailing who to contact and when in the process they should be contacted. This will cover both internal staff and external entities (e.g., law enforcement; Federal, State, and Local entities; Emergency Services; the Texas Division of Emergency Management; and third-party forensics firms)

- **Tabletop exercises**: After drafting the IRP (See Bid Item 2 below for details on this approach), we will lead a tabletop exercise with your incident response team (ideally everybody with a role in the RACI matrix) to walk through the documented processes. The tabletop exercise will cover high-risk incident scenarios that could impact the confidentiality, integrity, and availability of your network and data. This exercise will help your team learn their responsibilities and identify areas for improvement.

Bid Item 2 (Incident Response Plan)

The secondary intent of the North Central Texas Council of Governments' RFP is to utilize the SHARE awarded contractor to facilitate the creation of an Incident Response / Recovery Plan, a consolidated list of standards, and a maturity model for regional jurisdictions that maps out whom to call and what to do at various levels of incident for the North Central Texas Council of Governments Emergency Preparedness Department and the North Central Texas region. All project deliverables related to the secondary intent of this RFP will be completed by September 30, 2021.

Incident Response Plan

In case of a security breach, a standby team needs to be rapidly available with the following capabilities:

- Expert IR experience
- Awareness of and/or details of your business processing environment
- The right tools to investigate the incident
- Contact details for key stakeholders
- Processes and activities must meet the expectations of legal authorities

This is why it is critical to have a documented Incident Response Plan (IRP) that is readily available to applicable personnel, tested, and regularly updated. We will help you develop the IRP and build your response maturity to help you prepare for an incident.

We will help develop an IRP that aligns with the guidance outlined in the NIST SP 800-61, *Computer Security Incident Handling Guide*, US-CERT Federal Incident Notification Guidelines, and your existing processes. Incident response is divided into four phases as shown below.

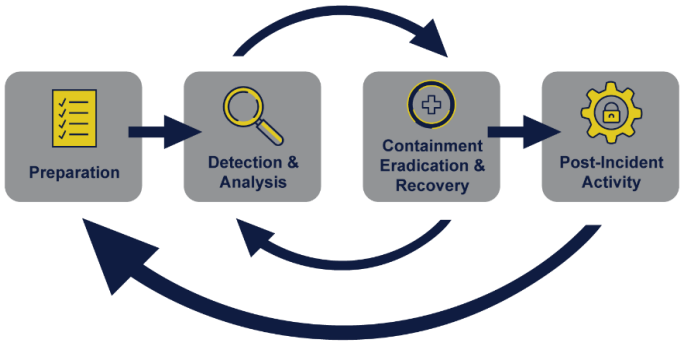


Exhibit 3: Phases of Incident Response

Preparation

Preparation includes defining a governance structure for Incident Response, including response team roles and responsibilities. Preparation will also involve documenting the following:

- Contact information for internal and external stakeholders
- Pre-existing retainers for third party incident response support
- Mechanisms for staff and customers to report suspected incidents, including anonymously
- A method to track incidents
- Communication methods for the incident response team

Preparation also includes ensuring that incident analysis hardware and software requirements are documented and the necessary assets are procured (e.g., a jump kit/server).

A key element of preparation is the prevention of incidents. We can help you identify your ability to prevent incidents through additional services, such as maturity assessments and security testing detailed elsewhere in this proposal.

Detection and Analysis

We will help you develop processes to detect incidents. This will include identifying current detection capabilities and any gaps that should be addressed to ensure comprehensive coverage. Detection capabilities may include, but are not limited to:

- Personnel to review logs and other mechanisms for identifying precursors and indicators of compromise
- Systems for analyzing events, trends, and patterns of behavior
- Intrusion detection and prevention devices
- User reporting of anomalous activity

The IRP will document the processes for regularly reviewing detection mechanisms and steps to take following indication of a potential incident.

Analysis steps within the IRP will encompass identifying the impact of the security event on:

- The confidentiality, integrity, and availability of data and systems
- The immediacy of its effect on critical business functions
- The scope of the incident in terms of risk, affected users, assets, and locations

This will result in a categorization based on severity, which dictates the steps to be taken for containment, eradication, and recovery.

Containment, Eradication, and Recovery

We will help you develop containment processes within the IRP. This can include the development of playbooks to address high-risk incidents, such as ransomware.

Eradication efforts will be documented within the IRP, such as removal of malware and user accounts, vulnerability remediation, and identification of other hosts that may have been affected within the organization.

Recovery efforts for incidents will involve the restoration of affected systems to normal operation. This is dependent upon the type of incident experienced but may include actions such as restoring systems from backups, rebuilding systems from an agency approved baseline, replacing compromised files with clean versions, installing patches, changing passwords, and increasing network perimeter and host-based security.

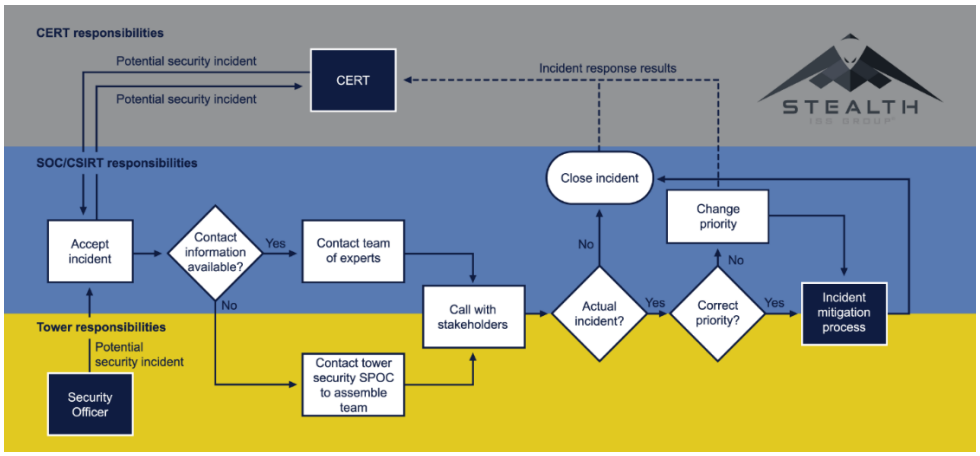


Exhibit 4: Example Security Incident Response Flow

Post-Incident Activity

We will help you develop processes to continually test, analyze, and update response procedures, incorporating lessons learned and technological advancements through monitoring and control efforts to yield the desired outcome or seek corrective action. In this way, you can establish a set of tested processes and procedures to quickly contain and eradicate realized incidents.

Additional Cybersecurity Services

SOC-as-a-Service (SOCaaS)

Typically, each endpoint in an organization's environment is monitored by a costly security operations team dedicated to detecting and responding to cyber threats. Providing 24x7x365 support requires a minimum of five trained employees – the base salary for one Junior SOC Analyst is approximately $50,000[3] and one Senior SOC Analyst averages approximately $92,500 [4]. Even disregarding additional overhead costs and time to train, deploy and manage these resources, funding the salaries of even the smallest security operations team is a costly endeavor.

Stealth Group's SOC-as-a-Service (SOCaaS) offering enhances your existing team's capabilities and saves money on resources by unifying environmental visibility, attack protection, and response orchestration together into a single interface. This eliminates the need for multi-product security stacks, as well as dependency on high-level security skills. Regardless of your security team's size and skill, this software would help to prevent, protect, and enable recovery from malicious threats and attacks on your infrastructure and applications on a 24x7x365 basis.

Stealth Group's SOCaaS combines the technologies, processes, and people in a comprehensive service offering that addresses all attack surfaces. This consolidated protection service will provide you with full network coverage for users, files, hosts, and networks. Our service includes a wide set of remediation tools to fully recover from attacks by correlating users, files, network traffic and hosts activities with complete set of threat prevention and detection tools joined by pre-set and custom auto-remediation policies for post-compromise activity.

Stealth Group will coordinate with you to mutually define performance metrics, escalation procedures, response times, and contact lists as well as participate in weekly, monthly, and quarterly meetings as required.

Your protected environments will be mapped to host, file, user, and network entities, and the SOCaaS software will natively integrate prevention and detection technologies that cover attack vectors which target them, avoiding the partial threat coverage inherent to Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), and network analytic tools.

Total Environment Visibility
An organization's attack surface is much wider than its endpoints. We continuously monitor all

[3] Payscale. "Average Junior SOC Analyst Salary." Last updated November 4, 2020. https://www.payscale.com/research/US/Job=Junior_SOC_Analyst/Hourly_Rate
[4] Payscale. "Average Senior SOC Analyst Salary." Last updated February 6, 2021. https://www.payscale.com/research/US/Job=Senior_SOC_Analyst/Salary

users' logging in and out, internal and external traffic, and process execution on hosts to provide real-time contextual visibility into the entire environment's activities.

360° Prevention and Detection
We continuously and natively integrate the full-scope of technologies to prevent and detect attack vectors that target users, files, the network, and hosts: Anti-Virus (AV), Next-Generation Anti-Virus (NGAV), EDR, network analytics, User and Entity Behavior Monitoring (UEBA) and deception technology, building a robust security protection stack across all attack stages.

Deception
Advanced attackers can evade detection. To confront this, our team enables its users to plant decoy files, log-in credentials, and network connections across their environment, luring such attackers to reveal their presence by attempting to use or access these decoys.

Automated Remediation
We provide the widest set available of remediation actions for compromised hosts and users, malicious files and network communication. Our SOC-as-a-Service team has the ability to block attacks at multiple post-compromise stages such as privilege escalation, credential theft, lateral movement and others.

Stealth Group provides pre-built default remediation rules, but these rules can be easily modified to reflect your internal balance between security and operational continuity. These custom rules can take place using either:

- Built-in remediation actions: matching a set of actions to the respective file, network, user, and host entities following the alert's validation.
- Custom script: uploading a script that communicates with other devices (firewall, proxy, etc.) to expand remediation scope across the environment.

Context-based Alert Operation
In the case of malicious activity without a matching pre-built remediation, we provide the full user, file, network and host context for rapid insight into the attack's impact and scope. The resolving process concludes with manually applying a remediation action on the compromised entity that can be saved as policy to automate response in future occurrences.

IT Hygiene Reports
While addressing active threats is a sole domain of the security team, there are various IT hygiene procedures which can greatly enhance IT management efficiency and dramatically reduce your attack surface. Stealth Group's SOCaaS includes various hygiene reports, which creates a continuous health check for your Data Network.

IT Hygiene Report types include:

- System vulnerability assessment
- Application vulnerability assessment
- App blacklisting

- Asset management
- File integrity policies
- Password change

Easy Deployment & Maintenance
Our service is based on server-agent architecture. The server can be either on-prem, IaaS or hybrid, per customer preference and either a dissolvable executable or a lightweight agent that rapidly deploys 50Ks of hosts a single day.

Stealth Group's 24X7 Security Team
Our SOCaaS complements its security services with automated threat protection technology. Our 24/7 team of threat analysts and security researchers proactively hunts for threats among our customers, as well as responds to customer escalations, assisting with file analysis, incident response and deep investigations.

Intuitive Dashboard
Our service includes a user-friendly dashboard which provides a high-level overview of the current security status of the environment. It utilizes various graphics to display the current number of open alerts, files that have been analyzed, hosts that have been scanned, and allows pivoting to various other areas of the console based on this information. The main graphics on the dashboard describe:

Open Alerts –Metrics about current open alerts, including the number of files, users, hosts, and network traffic items associated with these open alerts. Hovering the cursor over the Total Alerts ring will display how many open alerts there are of each severity. Clicking on the object symbols pivots to the Alerts page, filtered by File Alerts, User Alerts, Network Alerts, and Host Alerts.

Exhibit 5: Open Alerts

Threat Radar – Overall risk level (center) and high-risk objects (files, users, hosts, and network traffic). Individual risk scores for objects will be displayed as dots on the radar. Objects with open alerts will be shown as solid dots and can be clicked on to view details.

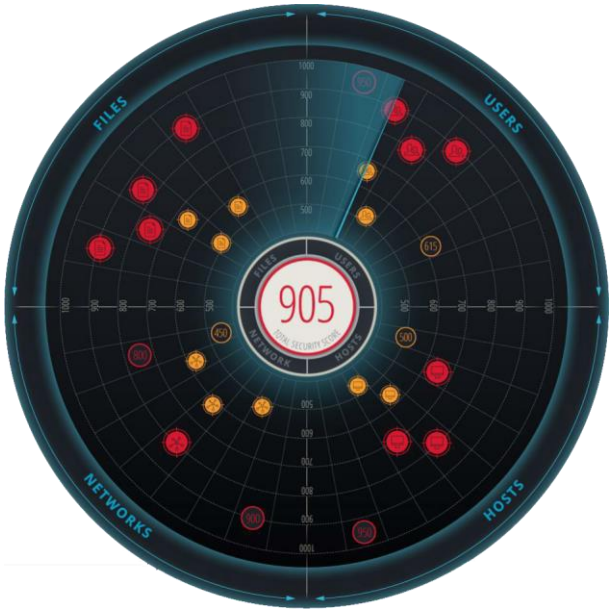


Exhibit 6: Threat Radar Shows Total Security Score

Files Analyzed – Metrics about files that have been analyzed by the system to date. The percentage of "whitelisted" files indicates the number of files which have been analyzed and deemed safe through security intelligence. The remaining percentage will be reviewed by the Stealth Group 24/7 Security Team.

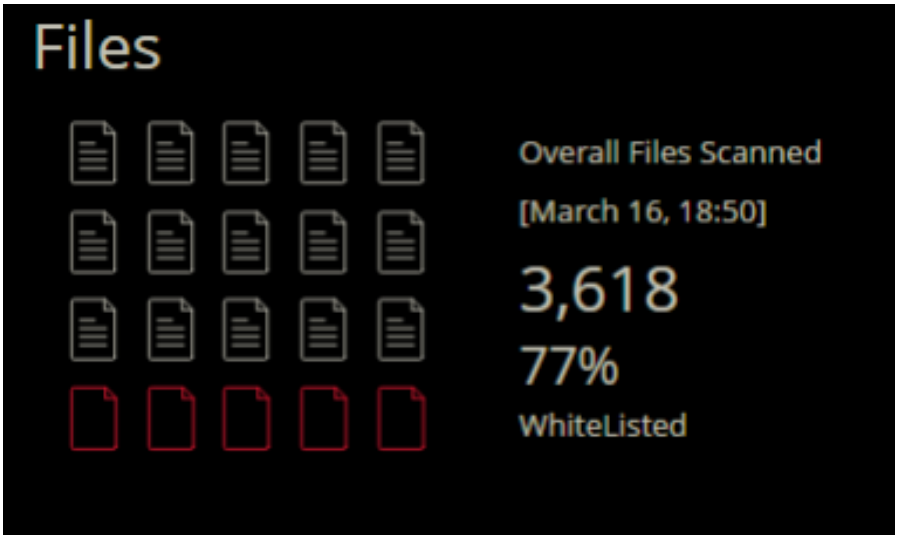


Exhibit 7: Files Analyzed and Deemed "Safe"

Alerts by Date – Graphical timeline of generated alerts over the past 10 days. Hovering the graph will display the number of alerts generated on each day.

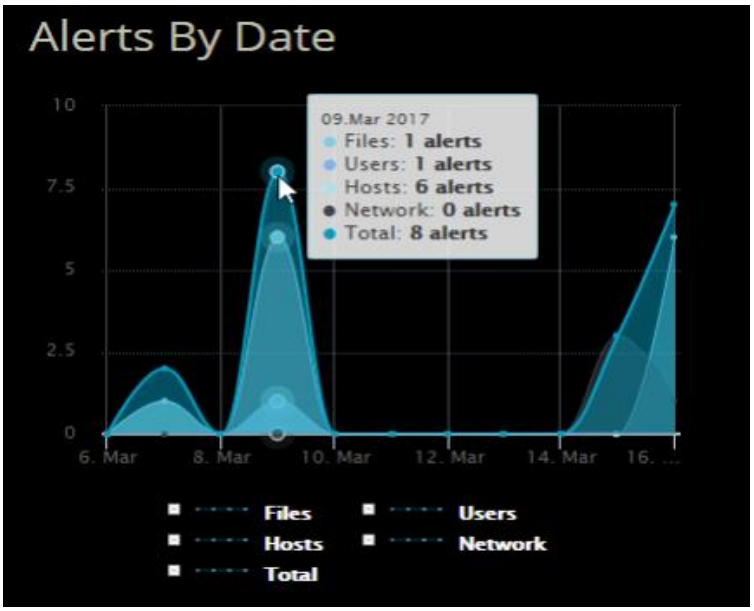


Exhibit 8: Timeline of Recent Alerts

Hosts Scanned – Metrics on hosts that have been scanned in the past day, week, and month.

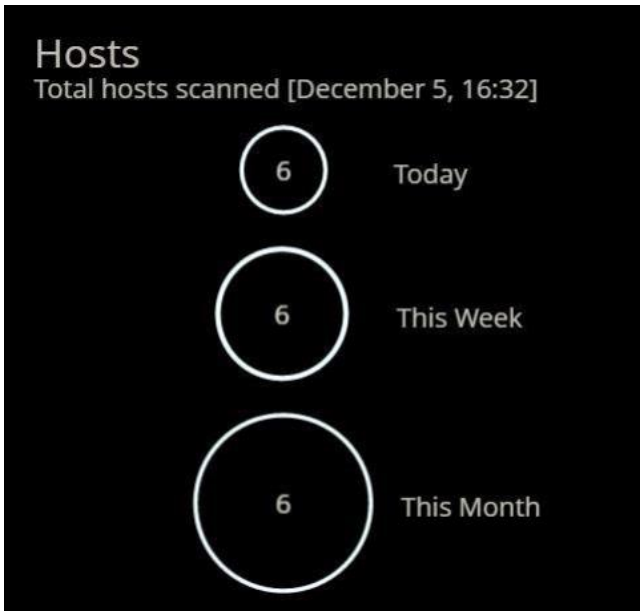


Exhibit 9: Quick View into Number of Recently Scanned Hosts

Incident Analysis and Forensics

Stealth Group Cybersecurity Engineers perform data forensics using various commercial and open-source applications to differentiate between malicious and benign activities, following best practice escalation procedures as established by the customer. Our engineers are knowledgeable and experienced with tools such as Encase, Kali Linux Suite, Lastline, PTK, SANS, Volatility, Digital Forensics Framework, and Wireshark. We examine intrusions meticulously to identify the attack vector, malware used, deployment techniques, and assess the type and amount of data exfiltrated.

In the event of a potential breach, we perform a thorough Incident Analysis including in-depth forensic analysis to provide information spillage response which includes identifying the specific information involved in the information system contamination or potential breach; alerting personnel of the information spill using a method of communication not associated with the spill; isolating the contaminated information system or system component; eradicating the information from the contaminated information system or component; and identifying other information systems or system components that may have been subsequently contaminated.

Incidents that impact resources and/or business operations, or negatively affects customer experience usually results in a S1/S2 incident (see table below). The forensics team usually gets involved after Level 1 and/or 2 once the SOC or monitoring team have assessed the situation and decided that it requires further and more detailed investigation. Or, they were not able to resolve the system and/or it is a P1 incident (as classified per SOC incident policy classification).

Usually after a compromise (breach or data leakage has been identified), when Service Level Agreements (SLAs) are broken, customer impact has occurred, an illegal action has been identified or regulatory requirements have been broken (HIPAA, PCI, etc.) the internal legal team will need to be involved and official report will need to be filed with the authorities (if applicable). In some cases, clients may have internal policies and processes that govern this and those would be the ones followed. If they are less stringent and do not meet the above requirements, our suggestions would be to adjust those communication guidelines towards the Legal team accordingly.

Our Incident Response teams are usually involved with the Internal Communications teams and IT as early as during SOC Level 1 investigation to identify and collect information to check if there is a false positive.

We will assume the lead role in incident handling response for potentially high-impact or high-priority security breaches. We perform incident response services using command and control functions as outlined in NIST SP 800-61 Rev. 2 *Computer Security Incident Handling Guide* which includes the incident response life cycle phases of preparation, detection and analysis, containment, eradication, recovery, and post-incident activity.

Normally, all incidents are handled as if a compromise had occurred. All data is handled using appropriate tools and chain of custody is rigorously maintained such that forensic data is admissible in court if needed. Post incident activities, to include lessons learned, are integrated into daily IT operations, security management, policies, and procedures. Action Items forthcoming from this incident (e.g., remediation action and lessons learned) are tracked and reported until closed.

File Integrity Monitoring Service

Being able to quickly detect and respond to unauthorized changes in your IT environment is a critical component of Incident Response. For example, detecting encryption of a critical file could give you an earlier warning of a ransomware attack. To ensure that your business operations are always available and performing as expected, it's vital to adopt a comprehensive security, integrity, and compliance solution.

Our Managed Continuous Security & Compliance with File Integrity Monitoring Security Service is a powerful compliance, information assurance, and security solution for your business. We provide you with a comprehensive set of security, auditing, and compliance solutions to ensure the integrity of your entire IT Infrastructure. This solution has the following capabilities:

Detect Changes to Critical Files: With our File Integrity Monitoring services, we can detect changes to critical files including system, application, and configuration files and monitor registry, installed software, and local users/groups. We can detect zero-day attacks and unauthorized changes in real-time, while simultaneously complying with regulations such as PCI DSS, HIPAA, NERC, and FISMA.

Our solution can be implemented to protect your systems as follows:

Servers	We protect you against unauthorized change to vital applications and servers (physical, virtual, or cloud-based), including operating system settings, system files, directories, data files, file attributes and Windows® Registry settings.
Workstations	We protect you against unauthorized changes to workstation/desktops with specific functionalities or those running critical applications. We monitor all of the same items for servers, but scaled to meet the needs of the smaller machine using minimal system and network resources.
Databases	We protect you against unauthorized changes to critical database schemas including changes to security and access settings which have the potential to allow critical data to be breached.
Network Devices	We protect you against unauthorized and destructive changes to your network infrastructure, including firewalls, routers, and switches, as well as accidental misconfigurations that can lead to your IT infrastructure being compromised.
Active Directory / LDAP	We protect you against changes to your directory services including objects, attributes, and schema.
Point of Sale (POS)	We protect you against changes to POS systems that can allow payment card data to be breached or cripple these business-critical IT assets.

VMware/ESXi	We protect you against changes to VMware ESX and ESXi host configurations that can lead to a compromise of a large number of "guest" virtual operating systems.

Maintain a Secure State: We protect you against external attacks that slip by your firewall or intrusion detection system. This is accomplished through comprehensive visibility into your environment, providing the ability to identify and respond to internal threats originating from inside the network or even the occasional accident by IT personnel.

Plan Any Change with Integrated Ticketing: We automate the detection and documentation of all changes within the IT infrastructure. This simplified process for creating and dynamically updating authoritative baselines saves time and resources.

Automatically Identify Changes Due to Patches and Updates: Our managed services give you the ability to automatically identify changes due to patches and updates.

vCISO

Stealth Group's vCISO will provide the independent, senior-level cybersecurity expertise necessary to help you make critical decisions to reduce your risk. Stealth Group will assign a vCISO, **working remotely**, as a Senior Security Consultant for this contract. The vCISO will act as the main security Point of Contact (POC) for any security related questions, recommendations, assessments, and/or strategic consulting for your organization. The person selected will have **extensive technical and security hands-on experience** and understand business and operational factors to **align security and compliance requirements with operations**. The consultant will minimize risks while enabling and supporting the end-users and clients in their daily tasks, without causing any disruption or delays to business.

The vCISO will assist your organization by recommending the **best approach** to eliminating, thwarting, or offsetting risks, and will recommend appropriate security systems, protocols, and countermeasures to be implemented. These recommendations will enable your organization to apply **industry best practices** and develop future state ("to be") architecture, which will make you **less vulnerable** to unwarranted risks or hacks.

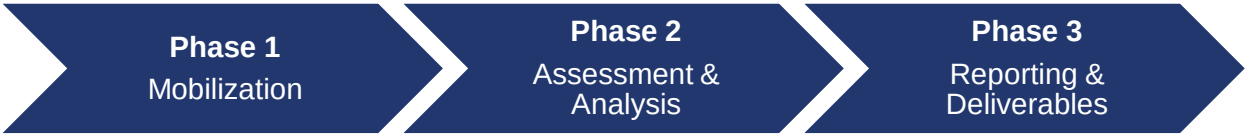
The tasks will include, but are not limited to:

- **Security operations:** Supporting real-time analysis of immediate threats and triage when something goes wrong.
- **Cyber risk and cyber intelligence:** Keeping abreast of developing security threats, and helping you understand potential security problems that might arise from acquisitions or other big business moves.
- **Data loss and fraud prevention:** Making sure internal staff doesn't misuse or steal data.
- **Investigations and forensics:** Determining what went wrong in a breach, dealing with those responsible if they are internal, and planning ahead to avoid repeats of the same crisis.
- **Security architecture:** Guide planning, procurement, and deployment of security hardware and software, making sure IT and network infrastructure is designed with best security practices in mind.
- **Identity and access management:** Ensuring that only authorized users have access to restricted data and systems, including creation, adjustment and/or verification of existing standards and compliance requirements.
- **Governance:** Making sure all the above initiatives run smoothly and are aligned with compliance and standard requirements, as well as internal and external audits activities.

The vCISO will produce and deliver regular status reports that summarize the status of tasks and activities that have been performed during the reporting period. The report will also identify any risks or issues detailing the **impact, mitigation, or avoidance** of such risks.

Maturity Assessment

We can conduct a maturity assessment to identify your organization's current ability to Identify, Protect against, Detect, Respond to, and Recover from a cybersecurity incident. The maturity assessment will take place in the following phases:



We recommend that the governance is finalized during the Mobilization Phase and documented in the Project Initiation Document. Given the nature and duration of the project we also recommend the following approach:

- Regular update meetings with your Project Manager and/or key stakeholders during Phases I and II to review progress against the plan, review and manage risks and resolve any issues that may have arisen. The purpose of this meeting will be very tactical and short-term in its outlook. This will include review of the next activities, and lessons learned.
- Once the final report is completed and the presentation given, we propose a formal project close-down meeting to ensure assignment completion is formally documented, appropriate handover (where relevant) takes place, all outstanding activities are concluded, all questions have been answered, and next steps for you are defined.
- If any high or major risks are identified throughout the assessment, these will be reported to your Project Manager and/or Security Officer immediately with a recommendation for remediation.

You will be guided by you through the security assessment and remediation discussion to guarantee a collaboration between our teams and provide hands on learning and information sharing.

Phase 1 – Mobilization

The Mobilization Phase's primary purpose is to ensure that the project starts from a solid foundation. Our objective is to be transparent and to establish/agree how Stealth Group and your organization will collaborate regarding ways of working, reporting mechanisms, governance structures, roles and responsibilities of the key project stakeholders and processes for risk and issue management.

We will need you to assign a project manager to this initiative who can help us navigate your organization effectively. We will require a project kick-off meeting at the earliest opportunity with key stakeholders. This meeting will be used to discuss and agree upon our approach and to answer any questions required to get started. We will document our agreements and shared understandings in the form of a short Project Initiation Document which will be the scope cornerstone of this effort.

Our normal way of working during Phase 1 is to work alongside our clients, either physically or virtually – at least for the initial information gathering phase. This ensures we build strong and effective working relationships, share ideas and thoughts readily, and work collaboratively to overcome challenges and obstacles.

From experience we know the biggest single challenge to a project like this is the availability of key stakeholders and our ability to get time in people's calendars in a timeframe that fits in with the overall project plan. One of the key activities within the mobilization phase will be to identify and agree with you who the key stakeholders are. We recognize that there are at least six key communities to this project:

- Security and Compliance Team
- Local Security Officer
- Risk Officer
- IT Systems Owners and IT team (applications and infrastructure)
- HR team
- Legal Team

We plan to speak to designated representatives of each community at the start of the project to help us understand how your business operates and to help us identify common challenges.

As we move into the Detailed Technical Assessment activity then there is likely to be a requirement to engage directly with Subject Matter Experts (SMEs) and Business Managers from outside of the Security and Compliance team to gain an important perspective on Security from the functions that Security and Compliance are designed to support.

Whenever we conduct a formal interview, we will write up notes from the meeting and make them available. We are likely to request supporting documentation, screenshots, or demonstration of the processes, technology, or configuration details.

Phase 2 – Assessment and Analysis

The primary objective of Phase 2 is to collate and analyze the information delivered in order to enable us to assess your current security performance, assess it against industry best practice, and start to draw up a prioritized list of actions.

Over time and experience, Stealth Group has developed a common-sense methodology to assess cybersecurity maturity aligned to the three pillars of consulting: People, Process, and Technology. We work with you and challenge your thinking around crucially important strategic questions such as:

- What Information assets does your organization possess?
- How valuable are those assets in business terms? What is the impact on your business if any of those assets suffer harm in terms of their Confidentiality, Integrity or Availability?

- What threats (accidental and environmental as well as adversarial) does your organization face? How capable are those threats and what are their motivations?
- Do you have the resource availability and technology to address identified issues?
- Are governance structures in place to ensure security is integrated into day-to-day business?

The purpose of taking this approach is that it provides not just the information you need to be informed about your security posture, but also a business context and justification for making improvements to individual security controls. It provides a means of determining which aspects of your security need addressing more urgently than others. Our hypothesis is that without having this structure in place you may be placing undue emphasis on certain aspects of security which may not give you the best return on your investment. Security is all about identifying and managing risk and applying finite budgets in the most effective and efficient manner – rather than having a very long list of action items that may or may not do anything to manage the overall risk to your business.

Phase 3 – Reporting and Deliverables

Phase 3 is a short final phase of the project during which the draft gap analysis and prioritization document are delivered to your Leadership Team. Stealth Group will highlight the maturity gaps and provide an overview of any major concerns and outline steps to address any vulnerabilities or weaknesses. The focus here is on not only providing remediation based on risk and probability but also aligning it with the current and near future business operations you have in place. By evaluating compliance with regulations and enterprise directives, Stealth Group will help your leadership find the best, most efficient budget friendly approach to remediate existing gaps to your objectives.

Stealth Group will analyze the gaps from a technical perspective and provide guidance and provide a prioritization based on risk. However, implementing and agreeing on the execution of the suggested remediation will be up to the asset owners and the business owners. The planned remediating actions should be executed in line with the agreed timeframes and business operations.

In addition to the gap analysis, Stealth Group will also work with you to create a System Security Plan and a Plan of Actions & Milestones.

Creation of System Security Plan (SSP) – The purpose of the SSP is to provide an overview of the security requirements of the enterprise ‘system’. An Unclassified SSP is not a single document. It is a collection of documents that tell the story of the security requirements of the system and describe the controls in place or planned, responsibilities and expected behavior of all individuals who access the system including administrators. The SSP serves as a repository of documentation of the structured process of planning adequate, cost-effective security protection for the system. It reflects input from various managers with responsibilities concerning the system, including information owners, the system operators, and the system security manager.

Creation of Plan of Actions & Milestones (POA&M) – A POA&M is different from the SSP in that its focus is to fill the gaps and between where the enterprise is now and their desired maturity. It is recommended at this point to document the remediation project plan and help establish timelines and resource requirements to meet desired maturity.

At the end of Phase 3, all documentation will be delivered to your Leadership Team. After you have had time to digest the contents, we will meet with you to take your feedback with a view to finalizing the document and delivering our final presentation.

We will also be able to provide you a proposal for the tools and services to address many of the remediation items identified during the gap assessment. This is because we consider our engagements to be a partnership with our clients and we collaborate to ensure customized solutions are tailored to meet your unique requirements.

Penetration Testing

Stealth Group's Penetration Testing Capabilities include:

- Network Mapping
- Vulnerability Scanning
- Penetration Testing – Internal and External
- Social Engineering, including dumpster diving and USB stick drops
- Phishing Assessment
- Wireless Assessment
- Web Application Assessment
- OS Security Assessment (OSSA)
- Database Assessment, especially for in-house developed applications
- Automated and manual application code analysis and code review following the OWASP framework during the entire Software Development Life Cycle
- Simulated penetration testing via a SaaS-based breach and attack simulation platform that you can run daily, weekly, or whenever you need them

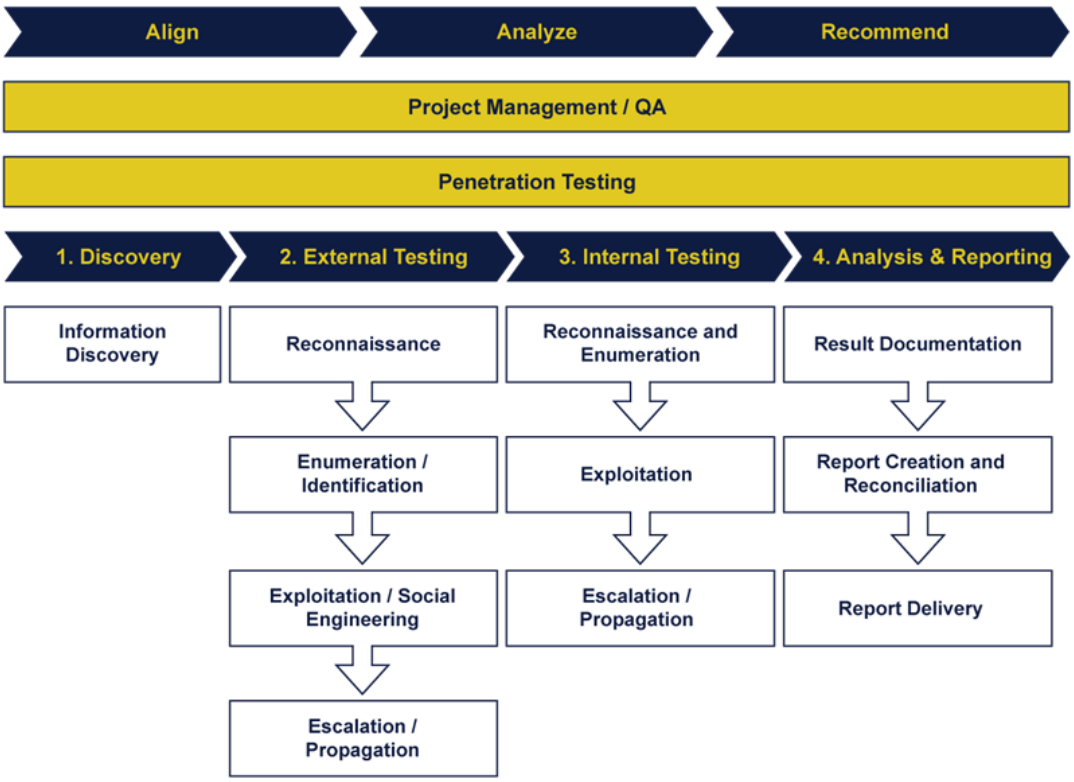


Exhibit 10: Penetration Testing Process

To determine the effectiveness of your security systems and their ability to withstand malicious exploits, Stealth Group performs various types of non-intrusive penetration testing. The goal is to mimic real-world attacks and attempt to compromise networks and operating systems to identify potential vulnerabilities in your systems. Testing uncovers the risk exposure for systems and demonstrates how vulnerabilities could be exploited to gain access to your systems.

Prior to a penetration testing engagement, Stealth Group experts coordinate with you to establish Rules of Engagement (ROEs) and document and schedule the testing. The extent and nature of the testing are always clearly delineated and agreed upon before commencement. Stealth Group takes all necessary steps to ensure that the confidentiality, integrity, and availability of any systems, applications, or data are not unduly impacted during the penetration testing process.

Stealth Group's certified penetration testers use the methodologies outlined in NIST SP 800-115 *Technical Guide to Information Security Testing and Assessment* to perform the testing, gather the evidence of proof of access, and provide the Information Systems Director with an executive summary and technical report. Stealth Group uses a variety of tools for Penetration Testing, including Browser Exploitation Framework (BeEF), Core Impact, w3af, Kali Linux suite, Canvas, Burp Suite, Metasploit, Wireshark, Cain & Able, ZAP, Retina, Maltego, Angry IP, Sam Spade, Shodan, DNSdumpster, scans.io, Nikto, Gophish, and Netcraft.

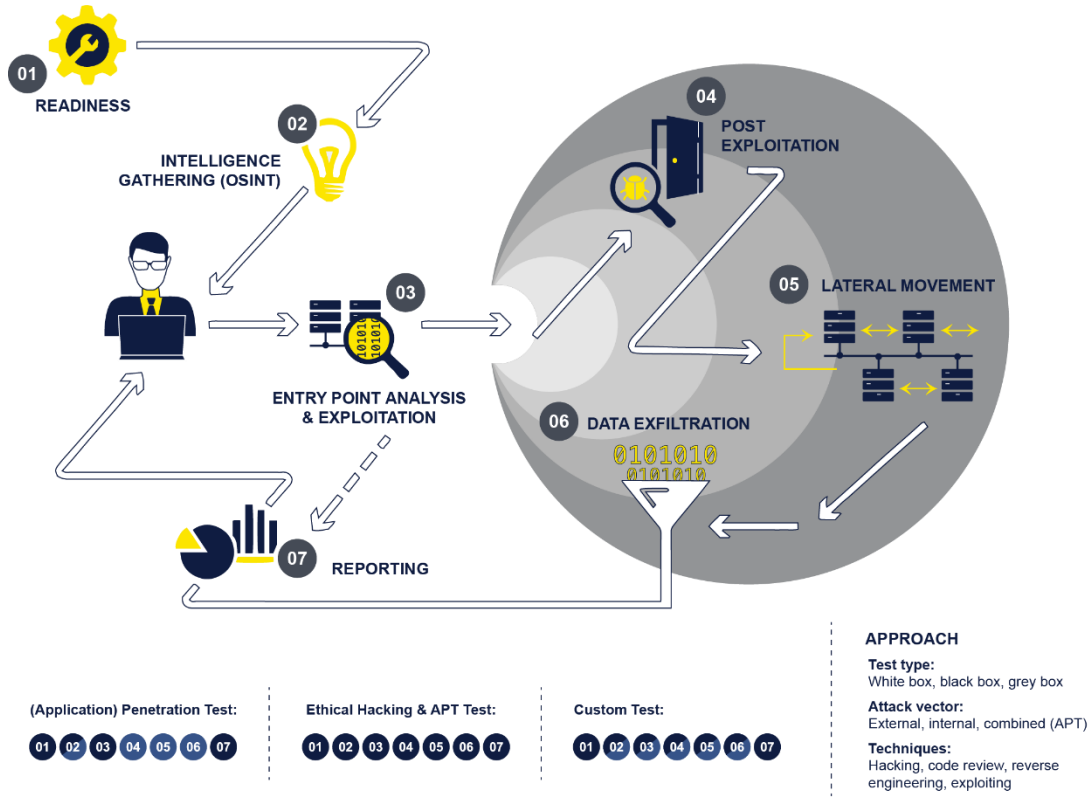


Exhibit 11: Penetration Testing Methodology

Stealth Group recommends penetration testing be completed when significant changes or upgrades to applications and infrastructure have been completed, when new offices or locations are connected to the corporate network, when new network infrastructure or applications are being added, when security patches or software upgrades have been completed, or when user-end policies have been modified. The tool kit we use in these activities are usually full penetration test OS distributions such as Kali Linux, BackBox, Parrot Security, and Pentoo which include the tools used such as Metasploit, Neosploit, and multiple tools to map network traffic flows (TCP/IP, DHCP, DNS) and conduct exploits based on buffer overflow mobile code, cross-site scripting, PL/SQL and injections, race conditions, covert channel, replay, return-oriented attacks, and malicious code.

The items tested include, but are not limited to:

- Track data transmitted across wire
- Secret passwords saved by programmer in a hidden file
- Check if the application returns more data than is needed
- Error pages and condition data exposure
- Sensitive information in binary files
- Checking URL for sensitive data
- Check if internal server contains sensitive information
- Multi-stage elevation testing
- Track data stored in file
- Weak discretionary ACL Testing
- Check for buffer overflow
- Attempt to modify execution flow (for instance, serial key validation)
- Attempt to identify insecure function call for insecure methods
- Attempt to overflow protocol, server name, file name, query string, and file extension
- Check for directory traversal information disclosure
- Check for XML injection attack (crashing XML parser, XQuery injection, etc.)
- Check for format string attack
- Spoofing attack, like changing MAC address and IP address
- Check for COM and ActiveX attacks

Our penetration testing follows this industry-standard process:

Scoping. Define the scope and objective of the penetration test, as well as the parties involved, and agree on Rules of Engagement.

Reconnaissance (Passive & Active). We gain information about targeted computers and networks passively, without actively engaging with the systems. Our methods of passive reconnaissance include: Gathering initial information (e.g., WHOIS, nslookup, SamSpade), determining network ranges and identifying active machines, discovering open ports, fingerprinting the operating systems, mapping the network, and uncovering services on ports. Also, open source (publicly accessible) information about you is checked to find personal

information (names and position/role), locations, links to partners and websites, privacy policies, or other publicly available documents that may help identify security mechanisms and technologies used.

Scanning and Enumeration. Stealth Group conducts scans to detect live systems (network ping sweeps), which are the services and versions of applications currently running. This allows us to identify which target is the best to attack (weakest) to gain access into the network. Port Scanning is first used to identify the vulnerabilities in the services listing on a port within the network. During this process, we identify the host, Operating Systems involved, firewalls, Intrusion Detection Systems, servers/services, perimeter devices, routing, and poorly protected resource shares using active connections to other systems. During the enumeration phase, we use techniques to obtain Active Directory information, discover NetBIOS enumerations, perform DNS queries, and establish null sessions and connections to assets. The tools we use for this phase are readily available on the Internet. The most prevalent tools used by Stealth Group are network mappers such as Nmap and Port Scanner Nmap, network scanners such as OpenVAS, Nessus and Nexpose, and web application scanners such as Syhunt, Burp Suite, OWASP ZAP and BeEF.

Exploitation. Operating under relevant guidelines and exclusively within the defined scope of properly authorized exercises, Stealth Group uses a variety of techniques to exploit vulnerabilities, taking advantage of said vulnerabilities to test the potential ability to gain control of a system, allow Privilege Escalation. The standard exploit tactics used by Stealth Group include Web application, network, memory-based attacks, Wi-Fi, Zero-Day, and physical exploitations, as well as social engineering.

In this phase, the test focuses on establishing access to a system or resource by bypassing security restrictions when attacking the organization. Methods to gain access to systems can include phishing, obfuscating or packing data, process injection, or gaining access to memory. Each pen test has a different and customizable exploitation approach based on technology used or tailored exploits (e.g., using existing and public exploits for specific OS). Exploits against your applications require some interaction with the user and may be used in combination with the social engineering method. The most common tools used by Stealth Group are Meterpreter (interactive shell to execute code), Metasploit (payload input), and Cobalt Strike.

Pivoting and Maintaining Access. Stealth Group uses Pivoting as a penetration testing technique, which uses the compromised system to attack other systems on the same network while avoiding Defense-in-Depth Strategies and gaining Super-User privileges. Our team has also used several sequential exploits and tools to access Super-User privileges, initially gaining low-level access, and then sequentially escalating privileges until Root User level is reached. Tools like Mimikatz are used for Pass-the-Hash/Ticket/Cache activities to gain access to systems. Proxy/VPN Pivoting - using a proxy/VPN payload on the machine and then launching attacks from the compromised system.

Covering Tracks/Cleanup. In this phase Stealth Group takes all steps to remove any escalations, user privileges, scripts, and/or traces of Pen Testing activities to return the system

to the state it was prior to testing. During the previous steps, our team takes detailed documentation of what was done, with what tools and how, to be able to have the data for the executive and technical report and return the system to its prior state.

Reporting. Reporting Post-Test deliverables are key to documenting findings and preparing for follow-on action items. Stealth Group deliverables include a technical and executive report, including a network enumeration report detailing system exposure, a host exploitation success/failure report, a findings report detailing vulnerabilities in the customer's network, and recommended remediation steps. Additionally, if the objectives of the Pen Test as per ROE were achieved, a thorough clean-up report with detailed recommendations and prioritization for remediation is included. Common findings include recommendations for patching, configuration (hardening), and password changes. After the completion of each penetration test (internal, external, web, and social engineering), the following reports are delivered:

- Security Assessment Report
- Executive Summary Report
- Risk Matrix
- Proof of Concept/Engagement Logs
- Proposed Mitigations and Workaround

A draft (with your review and comments) and a final report are provided. The report includes all documentation of what was performed, exploits identified and executed, remediation recommendations, and other relevant data required based on the outcome. The draft and final report will be in adherence to your requirements and standards or reporting.

Once you implement the suggested remediation actions to lower risk exposure and mitigate any findings, Stealth Group can perform an additional scan at your request to assess whether the identified vulnerabilities have been satisfactorily remediated. Stealth Group has the expert capabilities required to conduct the remediation activities, if desired by you.

Security Architecture Review

The security profile of any single system or application can change daily. New vulnerabilities can be discovered and published, new exploits can be developed and released, and new systems can be added or reconfigured within any network. This constant variation requires an in-depth, comprehensive defense strategy – one where no single vulnerability can compromise an entire network or critical application. It is not what security applications are running on your systems, or what processes are in place – as critical as that is – the most critical aspect – that many times is forgotten – is the network security design and architecture. If the network architecture does not support the security that you need to have, the technology at the ed points and the defense in depth security approach will not work. Therefore, we as Stealth Group, put a very strong emphasis on assessing the network design and configuration, DMZs, network segmentation, security zones, and traffic flow.

Stealth Group consultants will conduct a detailed review of the organizations network security goals and requirements as well as evaluating any associated security technology policies. Our senior engineers will partner with your network and systems architects to:

- Conduct an in-depth analysis of the network security architecture, including the network topology, solution components, device features and configurations Review firewall, router, and network switch configuration results, as well as security assessments
- Evaluate security technology policies for remote access, network segmentation, server protection, authentication, and firewall design can all be included in the scope of the review.
- Assess cascading security controls over networks, systems, and applications that overlap for vital redundancy

Following the above analysis, Stealth Group will provide a detailed analysis of network security architecture vulnerabilities and operational risks. This will also include an evaluation on how closely the current security architecture aligns with industry network security best practices.

As part of the delivery, you will receive a prioritized recommendation to mitigate the identified operational risks, including improvements to topology, protocols, policy, device configurations and network and security management tools. By following a systematic and detailed approach to assessing network security, the service helps organizations reduce threats to the confidentiality, integrity, and availability of business processes and applications and helps to improve risk management and satisfy compliance needs.

Contact Person

The following contact is designated for the bid, contracting, and contract administration phases:

- Robert Davies, CEO
- Tel: 813-598-3618
- Email: robert.davies@stealth-iss.com

TAB E – REFERENCES

The following recent and highly relevant contracts demonstrate Stealth Group's corporate experience and past performance that is similar in scope and magnitude to NCTCOG's requirements. Our references are evidence of expertise and corporate capabilities relative to all of NCTCOG's requirements, while also demonstrating our strategic vision through use of best practices, tools, processes, and innovation. Our work demonstrates conformance to contract requirements and to standards of great workmanship, record of forecasting and controlling costs, and adherence to contract schedules, including the administrative aspects of performance. Each reference shows a history of reasonable, collaborative, and cooperative behavior, and total commitment to customer satisfaction.

Olympic Broadcasting Services and Olympic Channel Services (OBS/OCS)
Security, Risk and Vulnerability Assessment
Security Architecture Review
Security Operation Center Implementation
Penetration Testing and Vulnerability Management

Description of Relevant Work Performed

- Scaled from nothing to design, build, staff, and operate the Broadcast Services SOC, and scaled it back down again to complete the project at the end of the event
- Once we arrived on site, we completed the SOC and stayed on site for the duration to oversee the operations. Our presence was instrumental when the IOC SOC and Games infrastructure (not supported by Stealth Group) were compromised (this hack is public knowledge) – we worked out of contract with a multitude of security agencies and within court-admissible chain of custody guidelines to investigate, recover to a safe restore point, and repair the compromised infrastructure and devices, restoring service to a fully functional state.
- Implemented from ground up a new Security Incident Event Monitoring tool (SIEM) Splunk to monitor all broadcast and corporate networks for the Olympic Games on site in South Korea
- Fine-tuned the configurations of the central SIEM by creating and implementing business cases and reviewing data logs
- Designed/reviewed activities were compliant to International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST)
- Completed enterprise assessment based on NIST 800-53 and 800-171 for a total of 7 locations worldwide
- Assessed and implemented complete security assessment (policies, procedures, technology, design, and configuration) for OBS/OCS for the 2018 Winter Olympic Games in South Korea.
- Controlled expenses by completing as much work as possible remotely, including the engineering, architecting, and part of the building process

- Created security guidelines for all third-party networks including all radio and TV stations covering the Olympics on-site based on NIST framework and NIST 800
- Responsible for and delivered all vulnerability scanning, penetration testing, forensic analysis, security, and log monitoring.
- Provided Network Mapping, Vulnerability Scanning, Penetration testing, Phishing Assessment, Wireless Assessment, Web Application Assessment, Operating System Security Assessment (OSSA), and Database Assessments.
- Provided technical security assessments for infrastructure architecture, data flows, interconnections, and interdependencies (including 3rd party connectivity).
- Created remediation plans, and security characteristics of the technology and architectures used.
- Assessed data classification and security requirements appropriate for High Value Assets (HVA)

Outcome Achieved

- Identified over 3,000 high risk vulnerabilities within two weeks
- Created a baseline for security monitoring of new vulnerabilities
- Minimized the risk by 78% to the infrastructure
- Brought the risk level to almost zero risk at the start of the Olympic games.
- 100% protection of infrastructure even during third-party network attack on connected network segment
- Forensic analysis of the malware, following the NIST chain of custody guidelines
- Segmentation of critical assets
- Designed, implemented, and staffed 24/7 Security Operations Center for South Korean Winter Olympic Games in 2018
- Project was delivered on time, and within budget

Reference Contact – Program Manager

Dalmacio Tola	Calle Torrelaguna 75
Director of IT Systems, OBS	28027 Madrid, Spain
d.tola@obs.net	+34 91 839 75 00

Federal Retirement Thrift Investment Board Penetration Test	

Description of Relevant Work Performed
• Conducted penetration testing to identify the risk of an incident on the network, including:
  ○ The external network, internet-facing applications and infrastructure
  ○ Social engineering testing to identify susceptibility to phishing attacks
• Analyzed site/enterprise policies and configurations
• Evaluated compliance with regulations and enterprise directives
• Deliverables included: Security Assessment Report, Executive Summary Report, Risk Matrix, Proof of Concept/Engagement Logs, Proposed Mitigations and Workarounds, Draft Report, and Final Report
• Conducted independent verification and validation of the corrective actions to the observations in the Final Report	

Outcome Achieved • Successfully completed External, Web Application and Social Engineering Aspects of the test series. • Assisted with the selection of cost-effective security controls to mitigate risk	
Reference Contact – Program Manager	
Barbara Holmes COR / Chief Audit Executive Barbara.Holmes@tsp.gov	77 K Street NE, Suite 1000 Washington DC 20002 Office: 202-864-8793 Mobile: 202-604-2394
Reference Contact – Contracting Officer	
Timothy Costas Division Chief of Contracting	Timothy.Costas@tsp.gov 202-942-1689

Maryland State Board of Elections Black Box Penetration Test	

Description of Relevant Work Performed
• Assessed current security posture of Maryland State Board of Elections to identify the ability of security controls to prevent security incidents, including:
  ○ External black box penetration test of external perimeter defenses
  ○ External black box penetration test of web applications
  ○ Penetration test of the internal environment
  ▪ Test internal network segmentation and strength
  ▪ Check effectiveness of malware defenses
  ○ Reviewing vulnerability management policies for effectiveness	

Outcome Achieved • Identified risk within the scope of the contract that allowed exploitation and could have led to unauthorized access to systems and data. • Delivered final report with technical and remediation details to client on-time and within budget and project timelines.	
Reference Contact Art Treichel State Board of Elections CISO art.treichel@maryland.gov	 151 West St. Suite 200 Annapolis, Maryland 21401 410-269-2863
Reference Contact Nikki Charlson Deputy State Administrator nikki.charlson@maryland.gov	 151 West St. Suite 200 Annapolis, Maryland 21401 410-269-2863

Town of North Kingstown, Rhode Island Information Systems Security Risk Assessment Audit	
Description of Relevant Work Performed • Provided independent assessment of the Town's IT operations, internal security, and compliance controls. • Performed gap analysis to implementing NIST Cybersecurity Framework. • Audited critical systems security model and workflows to identify vulnerabilities and threats. • Conducted a physical security assessment of the premises of the Town and any Application Service Providers (ASP), As-A-Service, and Cloud offerings. • Recommended corrective and preventative solutions for the Town to implement in an effort to improve the informational environment. • Recommended appropriate security policies and procedures. • Provided periodic on-site risk management and review of Information Systems security procedures, analysis of system output data to identify potential breaches, suggest best practice, and apprise the Information Systems Director of threats.	
Outcome Achieved • Conducted Penetration Testing as well as Risk assessment of IT systems, data and corporate security posture. • Identified risk within the scope of the contract that allowed exploitation and could have led to gain unauthorized access to systems and data. • Delivered final report with technical and remediation details to client on-time and within budget and project timelines. • Details of engagements cannot be provided due to NDA and potential risk to the client.	
Reference Contact Michael Forlingier MIS/GIS Manager mforlingier@northkingstown.org	 100 Fairway Drive North Kingstown, Rhode Island 02852 401-268-1500, ext. 152
Reference Contact Kris Kinder Purchasing/Finance kkinder@northkingstown.org	 100 Fairway Drive North Kingstown, Rhode Island 02852 401-294-3331, ext. 142

TAB F – PROPOSAL PRICING

Pricing Methodology

Stealth Group's pricing approach is heavily weighted in cost realism. This is a result of our ability to control internal costs, indirect rate pools, and through our past experience, salary research, and active, national recruiting.

To calculate pricing, we first identified which direct labor categories would be best suited for the project. As a GSA Schedule 70 Contractor, we identified which of our standard GSA labor categories would be best suited for the project. We typically offer discounts of 5% - 25% on these rates depending the labor category and scope of work as negotiated with the SHARE members.

A complete price breakdown is as follows:

Pricing Format Request Example	**Procurement No.:**	**NCT 2021-043**
Respondent Name:	Stealth-ISS Group Inc.	
Notes:	1. This pricing sheet is an EXAMPLE of how pricing should be submitted for RFP 2021-043 2. Please provide hourly rates for **all** staff that would be involved in Cyber Security projects. 3. Use as many lines as needed. 4. Detail any additional information necessary. 5. Proposers are encouraged to offer additional Cyber Security Consulting functions or services to be offered as a catalog option. Please provide any additional options with 'list less' or 'cost plus' percentages for pricing. A copy of any catalog services your firm can provide should be included with this response.	

Cyber Security Checklist Rate Chart - SHARE Cooperative Purchasing Program
Incident Response Staff

Item	Description	Minimum Education / Certification Level	Minimum Years of Experience	Offered Price	
1	Incident Response Analyst 1	Bachelors	0	$102.68	per hour rate
2	Incident Response Analyst 2	Bachelors	2	$133.48	per hour rate
3	Incident Response Analyst 3	Bachelors	5	$184.83	per hour rate
4	Risk and Vulnerability Threat Analyst 1	Bachelors	0	$97.55	per hour rate
5	Risk and Vulnerability Threat Analyst 2	Bachelors	4	$123.22	per hour rate
6	Risk and Vulnerability Threat Analyst 3	Bachelors	7	$169.42	per hour rate

Item	Description	Minimum Education / Certification Level	Minimum Years of Experience	Offered Price
7	Cyber Malware Reverse Engineer II	Bachelors	4	$215.63 per hour rate
8	Cyber Malware Reverse Engineer III	Bachelors	7	$256.70 per hour rate
9	Cyber Countermeasures Expert II	Bachelors	4	$179.69 per hour rate
10	Cyber Countermeasures Expert III	Bachelors	7	$215.63 per hour rate

Cyber Security Checklist Rate Chart - SHARE Cooperative Purchasing Program
Additional Cybersecurity Services Staff

Item	Description	Minimum Education / Certification Level	Minimum Years of Experience	Offered Price
11	Program Support Specialist	High school Diploma	2	$104.73 per hour rate
12	Sr. Program Support Specialist	High school Diploma	5	$130.40 per hour rate
13	Admin/Data Analyst I	High school Diploma	2	$103.71 per hour rate
14	Admin/Data Analyst II	High school Diploma	5	$156.07 per hour rate
15	IT Technical Writer	High school Diploma	2	$102.68 per hour rate
16	IT Technical Writer II	High school Diploma	5	$150.94 per hour rate
17	Program Manager I	Bachelors	2	$159.16 per hour rate
18	Program Manager II	Bachelors	5	$205.36 per hour rate
19	Program Manager III	Bachelors	7	$246.43 per hour rate
20	Information Services Consultant I	Bachelors	2	$133.48 per hour rate
21	Information Services Consultant II	Bachelors	5	$164.29 per hour rate
22	Information Services Consultant III	Bachelors	7	$179.69 per hour rate
23	Systems Engineer I	Bachelors	2	$133.48 per hour rate
24	Systems Engineer II	Bachelors	5	$148.89 per hour rate
25	Systems Engineer III	Bachelors	7	$169.42 per hour rate
26	Software Engineer I	Bachelors	2	$143.75 per hour rate
27	Software Engineer II	Bachelors	5	$164.29 per hour rate
28	Software Engineer III	Bachelors	7	$205.36 per hour rate
29	Network Engineer I	Bachelors	2	$128.35 per hour rate
30	Network Engineer II	Bachelors	5	$159.16 per hour rate

Item	Description	Minimum Education / Certification Level	Minimum Years of Experience	Offered Price
31	Network Engineer III	Bachelors	7	$215.63 per hour rate
32	Systems Administrator I	Bachelors	<1	$123.22 per hour rate
33	Systems Administrator II	Bachelors	5	$143.75 per hour rate
34	Systems Administrator III	Bachelors	7	$189.96 per hour rate
35	Database Administrator I	Bachelors	2	$123.22 per hour rate
36	Database Administrator II	Bachelors	5	$148.89 per hour rate
37	Database Administrator III	Bachelors	7	$169.42 per hour rate
38	Subject Matter Expert I	Bachelors	2	$215.63 per hour rate
39	Subject Matter Expert II	Bachelors	5	$246.43 per hour rate
40	Subject Matter Expert III	Bachelors	7	$282.37 per hour rate
41	Subject Matter Expert IV	Bachelors	10	$308.04 per hour rate
42	IT Specialist I	Bachelors	2	$205.36 per hour rate
43	IT Specialist II	Bachelors	5	$225.90 per hour rate
44	IT Specialist III	Bachelors	7	$246.43 per hour rate
45	Computer Programmer I	Bachelors	2	$123.22 per hour rate
46	Computer Programmer II	Bachelors	6	$133.48 per hour rate
47	Computer Programmer III	Bachelors	10	$154.02 per hour rate
48	Web Developer I	Bachelors	2	$102.68 per hour rate
49	Web Developer II	Bachelors	5	$112.95 per hour rate
50	Web Developer III	Bachelors	7	$143.75 per hour rate
51	IT Security Specialist I	Bachelors	2	$92.41 per hour rate
52	IT Security Specialist II	Bachelors	5	$102.68 per hour rate
53	IT Security Specialist III	Bachelors	7	$133.48 per hour rate
54	Quality Assurance Specialist I	Bachelors	2	$77.01 per hour rate
55	Quality Assurance Specialist II	Bachelors	6	$102.68 per hour rate
56	Cyber Application Architect 1	Bachelors	3	$164.29 per hour rate
57	Cyber Application Systems Analyst	Bachelors	4	$154.02 per hour rate
58	Cyber Enterprise Architect	Bachelors	8	$225.90 per hour rate
59	Cyber Operations Manager	Bachelors	3	$154.02 per hour rate
60	Cyber Program Analyst	Bachelors	2	$133.48 per hour rate
61	Cyber Security Engineer 1	Bachelors	1	$112.95 per hour rate
62	Cyber Security Engineer 2	Bachelors	3	$154.02 per hour rate
63	Cyber Security Engineer 3	Bachelors	6	$205.36 per hour rate
64	Cyber Security Specialist 1	Bachelors	0	$102.68 per hour rate
65	Cyber Security Specialist 2	Bachelors	3	$133.48 per hour rate
66	Cyber Security Specialist 3	Bachelors	7	$179.69 per hour rate
67	Cyber Subject Matter Authority (SMA) 1	Bachelors	8	$225.90 per hour rate
68	Cyber Subject Matter Authority (SMA) 2	Bachelors	12	$256.70 per hour rate

Item	Description	Minimum Education / Certification Level	Minimum Years of Experience	Offered Price	
69	Cyber Subject Matter Authority (SMA) 3	Bachelors	15	$308.04	per hour rate
70	Cyber Technical Architect 1	Bachelors	7	$154.02	per hour rate
71	Cyber Technical Architect 2	Bachelors	10	$205.36	per hour rate
72	Cyber Training Specialist	Bachelors	2	$118.08	per hour rate
73	Security Operations Center (SOC) Analyst 1	Associates	0	$102.68	per hour rate
74	Security Operations Center (SOC) Analyst 2	Associates	2	$112.95	per hour rate
75	Security Operations Center (SOC) Analyst 3	Associates	5	$133.48	per hour rate
76	Vulnerability Assessment Analyst and Penetration Tester 1	Associates	0	$102.68	per hour rate
77	Vulnerability Assessment Analyst and Penetration Tester 2	Associates	3	$123.22	per hour rate
78	Vulnerability Assessment Analyst and Penetration Tester 3	Bachelors	5	$184.83	per hour rate
79	Cyber Security Analyst I	Bachelors	0	$87.28	per hour rate
80	Cyber Security Analyst II	Bachelors	3	$123.22	per hour rate
81	Cyber Security Analyst III	Bachelors	7	$154.02	per hour rate
82	Cyber Security Engineer I	Bachelors	2	$123.22	per hour rate
83	Cyber Security Engineer II	Bachelors	4	$164.29	per hour rate
84	Cyber Security Engineer III	Bachelors	7	$205.36	per hour rate
85	Cyber Project Manager I	Bachelors	2	$143.75	per hour rate
86	Cyber Project Manager II	Bachelors	4	$169.42	per hour rate
87	Cyber Project Manager III	Bachelors	7	$195.09	per hour rate
88	Cyber Program Manager I	Bachelors	2	$154.02	per hour rate
89	Cyber Program Manager II	Bachelors	4	$179.69	per hour rate
90	Cyber Program Manager III	Bachelors	7	$205.36	per hour rate
91	Penetration Tester I	Bachelors	2	$123.22	per hour rate
92	Penetration Tester II	Bachelors	4	$154.02	per hour rate
93	Penetration Tester III	Bachelors	7	$205.36	per hour rate
94	Virtual CISO (vCISO)	Bachelors	20	$318.04	per hour rate
Contractor shall provide additional Cyber Security goods or services at cost plus:				**20%**	

TAB G – REQUIRED ATTACHMENTS

Attachment I: Instructions for Proposals Compliance and Submittal

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT I:
INSTRUCTIONS FOR PROPOSALS COMPLIANCE AND SUBMITTAL

Compliance with the Solicitation

Submissions must be in strict compliance with this solicitation. Failure to comply with all provisions of the solicitation may result in disqualification.

Acknowledgment of Insurance Requirements

By signing its submission, Offeror acknowledges that it has read and understands the insurance requirements for the submission. Offeror also understands that the evidence of required insurance may be requested to be submitted within ten (10) working days following notification of its offer being accepted; otherwise, NCTCOG may rescind its acceptance of the Offeror's proposals. The insurance requirements are outlined in Section 6.

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

RFP 2021-043 Cyber Security Consulting Services Page **17** of **32**

Attachment II: Certifications of Offeror

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT II:
CERTIFICATIONS OF OFFEROR

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment III: Certification Regarding Debarment, Suspension, and Other Responsibility Matters

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT III:
CERTIFICATION REGARDING DEBARMENT, SUSPENSION AND OTHER RESPONSIBILITY MATTERS

This certification is required by the Federal Regulations Implementing Executive Order 12549, Debarment and Suspension, 45 CFR Part 93, Government-wide Debarment and Suspension, for the Department of Agriculture (7 CFR Part 3017), Department of Labor (29 CFR Part 98), Department of Education (34 CFR Parts 85, 668, 682), Department of Health and Human Services (45 CFR Part 76).

The undersigned certifies, to the best of his or her knowledge and belief, that both it and its principals:

1. Are not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction by any federal department or agency;

2. Have not within a three-year period preceding this contract been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (Federal, State, or Local) transaction or contract under a public transaction, violation of federal or State antitrust statues or commission of embezzlement, theft, forgery, bribery, falsification, or destruction of records, making false Proposals, or receiving stolen property;

3. Are not presently indicated for or otherwise criminally or civilly charged by a government entity with commission of any of the offense enumerated in Paragraph (2) of this certification; and,

4. Have not within a three-year period preceding this contract had one or more public transactions terminated for cause or default.

Where the prospective recipient of federal assistance funds is unable to certify to any of the qualifications in this certification, such prospective recipient shall attach an explanation to this certification form.

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment IV: Restrictions on Lobbying

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT IV:
RESTRICTIONS ON LOBBYING

Section 319 of Public Law 101-121 prohibits recipients of federal contracts, grants, and loans exceeding $100,000 at any tier under a federal contract from using appropriated funds for lobbying the Executive or Legislative Branches of the federal government in connection with a specific contract, grant, or loan. Section 319 also requires each person who requests or receives a federal contract or grant in excess of $100,000 to disclose lobbying.

No appropriated funds may be expended by the recipient of a federal contract, loan, or cooperative agreement to pay any person for influencing or attempting to influence an officer or employee of any federal executive department or agency as well as any independent regulatory commission or government corporation, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with any of the following covered federal actions: the awarding of any federal contract, the making of any federal grant, the making of any federal loan the entering into of any cooperative agreement and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

As a recipient of a federal grant exceeding $100,000, NCTCOG requires its subcontractors of that grant to file a certification, set forth in Appendix B.1, that neither the agency nor its employees have made, or will make, any payment prohibited by the preceding paragraph.

Subcontractors are also required to file with NCTCOG a disclosure form, set forth in Appendix B.2, if the subcontractor or its employees have made or have agreed to make any payment using nonappropriated funds (to include profits from any federal action), which would be prohibited if paid for with appropriated funds.

LOBBYING CERTIFICATION
FOR CONTRACTS, GRANTS, LOANS, AND COOPERATIVE AGREEMENTS

The undersigned certifies, to the best of his or her knowledge or belief, that:

1. No federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an officer or employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal loan, the entering into of any cooperative Contract, and the extension, continuation, renewal, amendment, or modification or any federal contract, grant, loan, or cooperative contract; and

2. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this federal contract, grant, loan, and or cooperative contract, the undersigned shall complete and submit Standard Form – LLL, "Disclosure Form to Report Lobbying", in accordance with the instructions.

3. The undersigned shall require that the language of this certification be included in the award documents for all sub-awards at all tiers and that all sub-recipients shall certify accordingly.

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment V: Drug-Free Workplace Certification

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT V:
DRUG-FREE WORKPLACE CERTIFICATION

The Stealth-ISS Group, Inc. (company name) will provide a Drug Free Work Place in compliance with the Drug Free Work Place Act of 1988. The unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited on the premises of the Stealth-ISS Group, Inc. (company name) or any of its facilities. Any employee who violates this prohibition will be subject to disciplinary action up to and including termination. All employees, as a condition of employment, will comply with this policy.

CERTIFICATION REGARDING DRUG-FREE WORKPLACE

This certification is required by the Federal Regulations Implementing Sections 5151-5160 of the Drug-Free Workplace Act, 41 U.S.C. 701, for the Department of Agriculture (7 CFR Part 3017), Department of Labor (29 CFR Part 98), Department of Education (34 CFR Parts 85, 668 and 682), Department of Health and Human Services (45 CFR Part 76).

The undersigned subcontractor certifies it will provide a drug-free workplace by:

Publishing a policy Proposal notifying employees that the unlawful manufacture, distribution, dispensing, possession or use of a controlled substance is prohibited in the workplace and specifying the consequences of any such action by an employee;

Establishing an ongoing drug-free awareness program to inform employees of the dangers of drug abuse in the workplace, the subcontractor's policy of maintaining a drug-free workplace, the availability of counseling, rehabilitation and employee assistance programs, and the penalties that may be imposed on employees for drug violations in the workplace;

Providing each employee with a copy of the subcontractor's policy Proposal;

Notifying the employees in the subcontractor's policy Proposal that as a condition of employment under this subcontract, employees shall abide by the terms of the policy Proposal and notifying the subcontractor in writing within five days after any conviction for a violation by the employee of a criminal drug abuse statue in the workplace;

Notifying the Board within ten (10) days of the subcontractor's receipt of a notice of a conviction of any employee; and,

Taking appropriate personnel action against an employee convicted of violating a criminal drug statue or requires such employee to participate in a drug abuse assistance or rehabilitation program.

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment VI: Certification Regarding Disclosure of Conflict of Interest

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT VI:
CERTIFICATION REGARDING DISCLOSURE OF CONFLICT OF INTEREST

The undersigned certifies that, to the best of his or her knowledge or belief, that:

"No employee of the contractor, no member of the contractor's governing board or body, and no person who exercises any functions or responsibilities in the review or approval of the undertaking or carrying out of this contract shall participate in any decision relating to this contract which affects his/her personal pecuniary interest.

Executives and employees of contractor shall be particularly aware of the varying degrees of influence that can be exerted by personal friends and associates and, in administering the contract, shall exercise due diligence to avoid situations which give rise to an assertion that favorable treatment is being granted to friends and associates. When it is in the public interest for the contractor to conduct business with a friend or associate of an executive or employee of the contractor, an elected official in the area or a member of the North Central Texas Council of Governments, a permanent record of the transaction shall be retained.

Any executive or employee of the contractor, an elected official in the area or a member of the NCTCOG, shall not solicit or accept money or any other consideration from a third person, for the performance of an act reimbursed in whole or part by contractor or Department. Supplies, tools, materials, equipment or services purchased with contract funds shall be used solely for purposes allowed under this contract. No member of the NCTCOG shall cast a vote on the provision of services by that member (or any organization which that member represents) or vote on any matter which would provide a direct or indirect financial benefit to the member or any business or organization which the member directly represents".

No officer, employee or paid consultant of the contractor is a member of the NCTCOG.

No officer, manager or paid consultant of the contractor is married to a member of the NCTCOG.

No member of NCTCOG directly owns, controls or has interest in the contractor.

The contractor has disclosed any interest, fact, or circumstance that does or may present a potential conflict of interest.

No member of the NCTCOG receives compensation from the contractor for lobbying activities as defined in Chapter 305 of the Texas Government Code.

Should the contractor fail to abide by the foregoing covenants and affirmations regarding conflict of interest, the contractor shall not be entitled to the recovery of any costs or expenses incurred in relation to the contract and shall immediately refund to the North Central Texas Council of Governments any fees or expenses that may have been paid under this contract and shall further be liable for any other costs incurred or damages sustained by the NCTCOG as it relates to this contract.

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment VII: Certification of Fair Business Practices

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT VII:
CERTIFICATION OF FAIR BUSINESS PRACTICES

That the submitter has not been found guilty of unfair business practices in a judicial or state agency administrative proceeding during the preceding year. The submitter further affirms that no officer of the submitter has served as an officer of any company found guilty of unfair business practices in a judicial or state agency administrative during the preceding year.

Name of Organization/Contractor(s):

Stealth-ISS Group, Inc.

Signature of Authorized Representative:

DocuSigned by:
Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment VIII: Certification of Good Standing

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT VIII:
CERTIFICATION OF GOOD STANDING
TEXAS CORPORATE FRANCHISE TAX CERTIFICATION

Pursuant to Article 2.45, Texas Business Corporation Act, state agencies may not contract with for profit corporations that are delinquent in making state franchise tax payments. The following certification that the corporation entering into this offer is current in its franchise taxes must be signed by the individual authorized on Form 2031, Corporate Board of Directors Resolution, to sign the contract for the corporation.

The undersigned authorized representative of the corporation making the offer herein certified that the following indicated Proposal is true and correct and that the undersigned understands that making a false Proposal is a material breach of contract and is grounds for contract cancellation.

Indicate the certification that applies to your corporation:

✔ The Corporation is a for-profit corporation and certifies that it is not delinquent in its franchise tax payments to the State of Texas.

_____ The Corporation is a non-profit corporation or is otherwise not subject to payment of franchise taxes to the State of Texas.

Type of Business (if not corporation):

- ☐ Sole Proprietor
- ☐ Partnership
- ☐ Other

Pursuant to Article 2.45, Texas Business Corporation Act, the North Central Texas Council of Governments reserves the right to request information regarding state franchise tax payments.

Stealth-ISS Group, Inc. ROBERT DAVIES Chief Executive Officer
(Printed/Typed Name and Title of Authorized Representative)

DocuSigned by:
Signature Robert Davies
22E0EECA6FFF474...

Date: 5/18/2021

Attachment IX: Historically Underutilized Businesses, Minority or Women-Owned or Disadvantaged Business Enterprises

Stealth Group is not a Historically Underutilized Business (HUB), minority-owned, women-owned, or disadvantaged business enterprise (M/W/DBE) as certified by the State of Texas Program and the North Central Texas Regional Certification Agency. However, Stealth Group is a Federally recognized Service-Disabled Veteran-Owned Small Business (SDVOSB) and Economically Disadvantaged Woman-Owned Small Business (EDWOSB). Below is certification from the Small Business Administration of Stealth Group's EDWOSB status.

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

Date: 2017-08-02 23:04:10 UTC

From: Office of Government Contracting
To: SISS CONSULTING INC.

Subject: Documents Uploaded to WOSB Program Repository

SBA has received documents uploaded by you to the WOSB Program Repository. In order to submit an offer on a contract reserved for competition among EDWOSBs or WOSBs under the WOSB Program, you must be registered in the System for Award Management (SAM.gov), have a current representation posted on SAM.gov that you qualify as an EDWOSB or WOSB, and have provided the required documents to the WOSB Program Repository. 13 C.F.R. 127.300(a). It is your responsibility to ensure you have uploaded all of the documents required by 13 C.F.R. 127.300, remember to log into SAM.gov and update your small business certification status.

You must update your WOSB Program Certification (WOSB or EDWOSB) in the WOSB Program Repository and your EDWOSB/WOSB representations and self-certification in SAM.gov as necessary, but at least annually, to ensure they are kept current, accurate, and complete. The certification and representations are effective for a period of one year from the date of submission or update. You must update the supporting documents submitted to the WOSB Program Repository as necessary to ensure they are kept current, accurate and complete. 13 C.F.R. 127.300(f). In accordance with 13 C.F.R. 127.400, SBA, at its choosing, retains the authority to conduct an Eligibility Examination of your submitted documentation. If this should occur, you will be notified per the regulations.

Sincerely,

U.S. Small Business Administration Office of Government Contracting

Attachment X: Request for Proposal/Solicitation Language for Compliance with the Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment

ATTACHMENT X
REQUEST FOR PROPOSAL/SOLICITATION LANGAUGE
FOR COMPLIANCE WITH THE
PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

Pursuant to Public Law 115-232, Section 889, and 2 Code of Federal Regulations (CFR) Part 200, including §200.216 and §200.471, NCTCOG is prohibited from using federal funds to procure, contract with entities who use, or extend contracts with entities who use certain telecommunications and video surveillance equipment or services provided by certain Chinese controlled entities. Proposers shall certify its compliance with these requirements as part of their proposal response by completing the "Prohibited Telecommunications and Video Surveillance Services or Equipment Certification" included with the RFP Document. Failure to submit the required certification statement may be grounds for finding the proposal nonresponsive.

Attachment XI: Prohibited Telecommunications and Video Surveillance Services or Equipment Certification

DocuSign Envelope ID: 2E16DC9E-A922-4D23-B8E6-921B27D8EDE1

ATTACHMENT XI
PROHIBITED TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT CERTIFICATION

This RFP and any resulting Contract is subject to the Public Law 115-232, Section 889, and 2 Code of Federal Regulations (CFR) Part 200, including §200.216 and §200.471, for prohibition on certain telecommunications and video surveillance or equipment.

Public Law 115-232, Section 889, identifies that restricted telecommunications and video surveillance equipment or services (e.g. phones, internet, video surveillance, cloud servers) include the following:

A) Telecommunications equipment that is produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliates of such entities).
B) Video surveillance and telecommunications equipment produced by Hytera Communications Corporations, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliates of such entities).
C) Telecommunications or video surveillance services used by such entities or using such equipment.
D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, Director of the National Intelligence, or the Director of the Federal Bureau of Investigation reasonably believes to be an entity owned or controlled by the government of a covered foreign country.

The entity identified below, through its authorized representative, hereby certifies that no funds under this RFP or any resulting Contract will be obligated or expended to procure or obtain telecommunication or video surveillance services or equipment or systems that use covered telecommunications equipment or services as a substantial or essential component of any system, or as a critical technology as part of any system prohibited by 2 CFR §200.216 and §200.471, or applicable provisions in Public Law 115-232 Section 889.

✔The Respondent hereby certifies that it does comply with the requirements of 2 CFR §200.216 and §200.471, or applicable regulations in Public Law 115-232 Section 889.

SIGNATURE OF AUTHORIZED PERSON: DocuSigned by: Robert Davies 22E0EECA6FFF474...

NAME OF AUTHORIZED PERSON: Robert Davies

NAME OF COMPANY: Stealth-ISS Group, Inc.

DATE: 5/18/2021

-OR-

☐ The Respondent hereby certifies that it cannot comply with the requirements of 2 CFR §200.216 and §200.471, or applicable regulations in Public Law 115-232 Section 889.

SIGNATURE OF AUTHORIZED PERSON: _____

NAME OF AUTHORIZED PERSON: _____

NAME OF COMPANY: _____

DATE: _____

Signed Addenda

owned hired, and non-owned vehicles. Minimum Required Limit: $1,000,000 combined single limit.

Professional liability:
a. Minimum Required Limits:
$1,000,000 Each Claim
$1,000,000 Policy Aggregate

If you have any exceptions to any of our terms and conditions or clauses contained in this RFP, please state your exceptions in your response.

Brent Moll
Buyer II

Proposers: Please acknowledge and return a copy of this Addendum with your proposal.

COMPANY NAME: Stealth-ISS Group Inc.

SIGNATURE: Robert Davies

NOTE: Company name and signature must be the same as on the RFP documents.

APPENDIX A: RESUMES

We have provided abbreviated resumes below. If the proposed staff member is unavailable at the time of the project start, staff with equal or better experience, qualifications, and certifications will be selected for NCTCOG's review.

Dasha D.	Technical Lead
Experience: 25+ years of IT and IT Security, U.S. Navy Veteran	**Education:** MS (Summa Cum Laude) IT Project Management/IT Security, MBA Advanced Business Management, BA International Relations & Foreign Affairs
Certifications: • Trained by CMMC-AB Board as a CMMC Provisional Assessor • Certified Information System Security Professional (CISSP) • Disaster Recovery & Business Continuity, Cyber Security, Lean Six Sigma, ITIL • Certified in Risk and Information Systems Control (CRISC) • Certified in the Governance of Enterprise IT (CGEIT) • National Security Agency – NSA IAM/ IEM (Information Assessment/Evaluation Methodologies) • Certified Chief Information Security Officer (C|CISO) • Payment Card Industry Qualified Security Assessor (PCI QSA) • Payment Card Industry Professional (PCIP) • Project Management Professional (PMP) • Health Care Security Professional (HCISSP) • FEMA/CERT – Incident Command Systems • National Incident Management System, Risk Assessments • Certified Confidentiality Officer/Business Espionage (CCO)	**Professional Memberships:** • Institute of Electrical and Electronics Engineers (IEEE) • International Information System Security Certification Consortium $(ISC)^2$ • Information Systems Audit and Control Association (ISACA) • FBI – InfraGard • PMI (Project Management Institute) • WikiStrat – Sr. Analyst (Cybersecurity) • Civil Air Patrol – 2nd Lieutenant • FBI – CyberDefense Response Team **Achievements:** U.S. Navy 2006-2008 – Achievement Medal for successful management of Aviation Department with $45M budget (deployment operations, logistics, inventory)

General Qualifications to Meet Requirements	
Accomplished cybersecurity professional with over 25 years' experience in the IT sector. Has successfully completed assessments and gap analysis in both the Federal and Commercial sectors, and closely involved with risk identification and mitigation procedures. Thorough knowledge of NIST CSF, PCI DSS, ISO 27K, and HIPAA.	
Relevant Experience and Positions Held	
Stealth-ISS Group Inc., CO-FOUNDER AND PRESIDENT	**10/2002 – Present**
• Serves Fortune 1000 clients worldwide • Manages consultants and maintains pool of 30 Cybersecurity Subject Matter Experts • Business development • Execution of various consulting engagements and projects	
Stealth-ISS Group, Inc., Atos SE - PyeongChang 2018 Olympic Games, 2016 Rio Olympics Games, Security Design, SR. SECURITY CONSULTANT – SPECIAL PROJECTS (CONTRACT)	**01/2017 – 03/2018**
• Project 1: Set up and design of new Security Operations Center for PyeongChang 2018 Olympic Games for Olympic Broadcast Services (OBS) and Olympic Channel including selection of team members, technology, staff and client training, standard operation procedures creation, table-top exercises including 24/7 monitoring operations. • Project 2: Acted as Single Point of Contact and Manager for all Security Escalations and Security Incidents during the 2016 Rio Olympics Games for Olympic Broadcast Services and Olympic Channel. • Project 3: In charge of $12Million security design and implementation for global client and their 50+ commercial and government agencies starting with gap analysis, recommendations and execution. Managed team of 27 and acted as PCI DSS QSA. Design for Security Operations Plan meeting PCI requirements	
Stealth-ISS Group, Inc., Atos SE – N/S America, DIRECTOR – CYBERSECURITY (CONTRACT)	**03/2015 – 12/2016**
• Identified, developed and managed cybersecurity offerings (services and tools) for global roll-out including pricing structures and various global delivery solutions for mid-size and large Fortune 500 corporations • Successfully managed and completed eight-month long Data & Risk Get Well Plan for McGraw-Hill to meet SEC compliancy	
Stealth-ISS Group, Inc., Atos SE, DIRECTOR GLOBAL CSIRT (CONTRACT)	**02/2013 – 12/2016**
• Designed and implemented first global Cybersecurity Incident Response Team (CSIRT) for Atos internally and all managed clients with three Operations Centers worldwide and 24/7 operations • Implemented corporate security standards for CSIRT operations, corporate training and awareness	

• Integrated all existing services and technologies into CSIRT for efficient monitoring and response times • Selected and trained CSIRT team and Atos Departments; technology selection, configuration and management • Acted as the escalation point for all major security incidents within Atos and their clients • Headed Forensic Analysis, Incident Response management and communication (internal, vendors and partners)	
Stealth-ISS Group, Inc., AGT International, DISASTER RECOVERY PROGRAM/ IT EXPERT	**06/2012 – 01/2013**
• Responsible for fulfilling Disaster Recovery (DR) Program for National Security Infrastructure Project: delivery of DR Plan, DR testing and management of all aspects of system design, run books, Purchase Orders, BOM/BOQ, test labs and acceptance testing.	
Stealth-ISS Group, Inc., Deutsche Bank, GLOBAL DLP/IT SECURITY ANALYST (CONTRACT)	**02/2012 – 05/2012**
• Designed and managed global Data Loss Prevention (DLP) implementation - focus on operational and technical processes for Symantec DLP rollout (Asia, Europe, Americas). Responsible for country specific policies, rules and processes based on applicable data privacy laws.	
Stealth-ISS Group, Inc., British Gas, GLOBAL IT SECURITY AND COMPLIANCE (CONTRACT)	**06/2011 – 02/2012**
• Lead project manager for Symantec Control Compliance Suite (CCS) and lead technical manager for implementation/configurations of global Data Loss Prevention (DLP), End Point Protection, data encryption (Symantec PGP), Endur trading, IBM Maximo, RSA Envision and Archer, Qualys and CyberArk. • Provided strategic consulting to senior management (global VP and C-level), Global Compliance and IT engineers to align and improve information security strategy and facilitate its implementation globally. • Implemented and managed cyber-security and forensic analysis lab, used for corporate cyber threat analysis, incident response, reverse engineering and forensic investigations.	
The Cosmopolitan of Las Vegas, DISASTER RECOVERY PROGRAM & DATA SECURITY (CISO)	**02/2010 – 06/2011**
• Designed, led and delivered complete enterprise information security program (people, process and technology) for new Las Vegas Hotel/Casino. This included infrastructure security, Identity and Access Management, Disaster Recovery, SIEM, Information Risk and Compliance, Training/Awareness Program.	

Misty R.	PROJECT MANAGER
Experience: 12+ years in contracts & compliance 6+ years in program & project management	**Education:** B.S. Business Management, Southwest Technical College, 1993 B.S. Project Management, Rockford University

Certifications:
• Project Management Professional (PMP)
• National Contract Management Association (NCMA)
  ○ Certified Commercial Contracts Manager (CCCM)
  ○ Certified Federal Government Contracts Manager (CFCM)
	Professional Memberships:
	• Coalition for Government Procurement
	  ○ Small Business Committee
	  ○ General Products Committee
	  ○ E-Commerce Committee
	• GSA Industrial Products & Services Supplier Research Panel
	
	Clearance: DoD Top Secret (inactive)

General Qualifications to Meet Requirements

Federal Business: Responsible for overall business development growth strategy. Accountable for federal contract administration, compliance, policy and procures.

Service Delivery: Responsible for the overall direction, coordination, implementation, execution, control and completion of specific projects ensuring consistency with company strategy, commitments and goals. Manage multiple priorities within expected timelines while effectively meeting client quality expectations.

- Knowledge of both theoretical and practical aspects of project management
- Knowledge of project management techniques and tools
- Direct work experience in project management capacity
- Proven experience in people management, strategic planning, risk management, change management
- Proficient in project management software

Relevant Experience and Positions Held

Stealth-ISS Group, Inc. – VICE PRESIDENT OF FEDERAL BUSINESS AND SERVICE DELIVERY	**06/2020 – Present**
STEALTH-ISS GROUP PROJECT MANAGER EXPERIENCE	
Absolute Dental – CMMC Pre-Assessment	**03/2021 – Present**
PLX Inc. – CMMC Pre-Assessment and Remediation	**01/2021 – Present**
Barge Design Solutions Consulting Group, Inc. – CMMC Pre-Assessment	**11/2020 – 01/2021**
Maryland State Board of Elections – Penetration Testing	**09/2020 – 10/2020**

Applied Thin-Film Products (ATP) – CMMC Pre-Assessment	**07/2020 – 10/2020**
Town of North Kingstown, Rhode Island – Vulnerability Assessment	**06/2020 – 12/2020**
Epoch Concepts LLC – CMMC Pre-Assessment	**05/2020 – 07/2020**
ADDITIONAL EXPERIENCE	
Continental Mapping Consultants – DIRECTOR OF FEDERAL BUSINESS	**02/2020 – 06/2020**
Responsible for federal business development & proposal team, post award contracts & compliance and the federal service delivery team for JANIS, USACE FEMA BlueRoof, GSA IT 70, and various protected clients. Security Clearance obtained – currently inactive	
SupplyCore – DIRECTOR OF OPERATIONS	**4/2017 – 2/2020**
Responsible for federal business development & proposal team, post award contracts & compliance and the federal service delivery team for DLA-MRO - 9 Global Contracts, GSA MAS which include 51V, 23, 84, INDOPACOM, MRO BPA & FSSI BPA), Israel Weapon Systems contract.	

Thank you!

STEALTH
ISS GROUP®

Get Sharp. Get Serious. Get Safe.