Competitive Solicitation No: **K689-RFQQ-2303**

EXHIBIT D – QUALIFICATIONS

BIDDER: Emagined Security, Inc

QUALIFICATIONS SECTION

The Qualifications Section of the proposal must contain information that will demonstrate to the evaluation committee the Firm/Staff understanding of the types of services proposed, the ability to accomplish them, and the ability to meet tight timeframes. Firm experience will be scored based on the capacity and experience of the firm to perform work similar to the tasks described in this RFQQ. Staffing will be scored on how the proposer staffs the project to perform work similar to the tasks described in this RFQQ, including the number of staff and the mix or make of the team and their various levels of experience. Staffing also includes the proposed staff or managers responsible for project oversight and their level of experience with tasks described in the RFQQ.

Recent experience with both government and private industries is a plus for both firm experience and staffing. Describe Vendor's experience and qualifications (in terms of Firm Experience and Staffing), especially with respect to performing work similar to the tasks described in this RFQQ.

Provide experiences comparable to:

i. Vulnerability Assessments: Demonstrated experience in vulnerability assessments that include web applications, thick client applications, mainframes, operational technology, network, and source code. In addition to experience, qualifications could include one or more of the following certifications: certifications from Global Information Assurance Certification (GIAC) including GPEN Penetration Tester Certification, Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Certified Ethical Hacker (CEH) or equivalent certifications as determined by SAO.

ii. Wireless: Demonstrated experience in auditing and assessing wireless networks. In addition to experience, qualifications could include GIAC Assessing and Auditing Wireless Networks (GAWN) or equivalent certifications as determined by SAO.

iii. Penetration testing experience with web applications, thick client applications, mainframes, network, source code, Industrial Control Systems (ICS), Medical equipment, Supervisory Control and Data Acquisition (SCADA) and other Operational Technology (OT) that resides within local government and medical facilities, including exploitation of discovered vulnerabilities in test environments or non-invasive/passive testing in production environments containing highly sensitive information or mission critical systems requiring high availability. In addition to experience, qualifications could include:

certifications from Global Information Assurance Certification (GIAC) including GPEN Penetration Tester Certification, Web application Penetration Tester (GWAPT), Offensive Security Certified Professional (OSCP), Exploit Researcher and Advanced Penetration Tester (GXPN) or equivalent certifications as determined by SAO.

iv. Expert-level knowledge and experience reviewing and providing recommendations to improve security over complex network design and architecture.

In scoring this section, SAO may favor those Vendors describing experience providing services to state agencies or local governments.

The Vendor must describe at least five (5) representative projects the Vendor has performed for customers during the three (3) years preceding the Proposal due date. Describe completed projects only; projects where the services are in the process of being put in place will not satisfy this requirement. The Vendor and their key team members must have had primary responsibility for the various phases of the projects including analysis, testing, document review, implementation and reporting. The project manager is expected to have past primary responsibility for the various phases of the projects including analysis, testing, document review, implementation and reporting. Do not exceed two (2) pages for each project's description. Each description should include, at a minimum, the project's purpose (i.e., Project Statement), the project's deliverables, the project's duration, and the results.

Scores for this section will be based upon, but not limited to, the degree to which the Vendor demonstrates direct experience with all aspects of performing penetration testing, **vulnerability assessments, wireless assessments** and providing expert-level knowledge and experience reviewing and providing recommendations to improve security over complex network design and architecture in large, medium and small networked organizations, and broad expertise with this type of work. Importance is given to the specific project role the Vendor has performed, as well as the scope and complexity of the projects in which the Vendor has participated. Both depth and breadth of experience are important.

- Demonstrate skills to communicate clearly, concisely and effectively both verbally and in writing.
- Describe the firm's methods for maintaining staff qualifications.
- Management approach, methodology and implementation strategies for managing and delivering their product.
- Describe their ability and capacity for delivering services proposed.

QUALIFICATIONS (Optional and separate from section above**)**

As a separate part of the response to this section we are interested to hear the consultant's perspective on what risks the potential contractor cannot control in this project.

Additionally, we would like the consultant's perspective on services that would add value to our proposed scope of work, but that we did not request.

RESUMES

The proposer must provide resumes for key staff and include information on each individual's specific

skills related to penetration testing, education, experience, certifications, significant accomplishments and responsibilities assumed on other similar projects related to the services proposed. U.S. federal government security clearance is a plus.

SAMPLE REPORT

Include a Sample report - Note: report should be cleansed of confidential information.

The proposer must provide one sample report that discusses work, and its related results, in areas similar to those that are referenced in the first set of bulleted items above. This sample report may either be an actual report that the proposer has delivered to a previous client, as long as the contents have been redacted according to any applicable laws, regulations, or agreements with that client, or it may be a mock report that the proposer has generated specifically for their response to this RFQQ.

This sample report will be scored based on how well its components respond to items listed under item “e.” under “Report Results” on page 4 of the RFQQ. The report will also be scored based on whether or not its content and suggested remediation steps are clear and actionable.

ADDENDUM TO EXHIBIT D: EMAGINED QUALIFICATIONS SECTION

The following sections depict Emagined Security's responses to the requested information within Exhibit D. Additional information can be found in Exhibit C responses that included additional details / methodologies for delivery of the services requested in the sample project. This information has not been duplicated into Exhibit D due to page count limitations.

i. Vulnerability Assessments Response

Emagined Security has been performing Vulnerability Assessment and Penetration Testing for over 22 years. Our more experienced team members have been performing penetration testing and ethnical hacking engagements for over 30 years. Emagined Security was founded initially to be a World-Class penetration testing organization and continues to focus on that as its core competency. We believe so deeply in training our Penetration Test team that we have created an **industry leading training program** with a full-time penetration test trainer who focuses on continued penetration test training and improvement.

For the State of Washington, over the past 7 years, Emagined Security has performed over 70 Penetration Test engagements including hundreds of web applications, thick-client, API tests, mobile applications, Wireless, Mainframes and thousands of internal and external network IPs tested for Cities, Counties, State Agencies, and Hospitals located in the State of Washington.

In Addition to the State of Washington, Emagined Security has performed Penetration testing for other States Auditor Offices as well as Cities and Counties in California, Texas and Arizona. In addition to government, Emagined Security also specializes in other industry verticals including Healthcare, Financial Services, Technology and Software companies. The vast majority of Emagined Security's contracts continue to be renewed year after year, while also increasing the types and number of tests for each of these clients. Our expertise is recognized internationally through the CREST organization. Additionally, Paul Underwood one of our lead Project Managers, sits on the Board of the CREST organization. A worldwide organization that certifies both Penetration testers and organizations for comprehensive penetration testing methodologies and abilities.

Emagined Security performs hundreds of Web Application Penetration Tests, Network Penetration Tests, API & Mobile Penetration tests, Mobile, Secure Code, Mainframe, Vulnerability Assessments and Wireless Assessments **every year**. This type of testing continues to be **a core service** Emagined Security offers. High level descriptions of some of the engagements are listed in each employee resume provided. Additionally, all Emagined Security Penetration Testers are **full-time Emagined Security employees**, they are also dedicated to the penetration test practice. Emagined Security Penetration Testers hold **background checks with the Washington State Patrol** to handle CJIS information as well are **CJIS Certified**, including the in the State of Washington. Our Penetration Testing is **never outsourced** to a third-party and our Penetration Testers are all **authorized to work in the United States (US)** and are **located in the US** ensuring no sensitive data is ever relayed overseas.

Emagined Security Consultants that we assign to penetration testing in the State of Washington only perform penetration testing services. They are experts and industry leaders in the field of penetration testing. Our consultants possess a variety of certifications. More are listed in *"Exhibit D - Qualifications-Emagined EHTeam Resumes 2023 Final"* and include:

- Certified Information Systems Security Professional (CISSP),
- Certified Ethical Hacker (C|EH)
- Offensive Security Certified Professional (OSCP) certification (PEN-200)
- Offensive Security Web Expert (OSWE) certification (WEB-300)
- Offensive Security Experienced Penetration Tester (OSEP) certification (PEN-300)
- Offensive Security Wireless Hacking
- CREST Registered Penetration Tester
- CREST Practitioner Security Analyst
- Microsoft Certified Professional Systems Engineer (MCSE), Certified in Homeland Security – Level 3 (CHS-III)*,
- GIAC Certified Firewall Analyst (GCFW)*,
- SANS GIAC Certified Incident handler (GCIH)
- SANS GIAC Penetration Tester (GPEN)
- Burp Suite Certified Practitioner (BSCP)
- eLearn Security Certified Penetration Tester eXtreme (eCPTX)
- eLearn Security Certified Professional Penetration Tester (eCPPTv2)
- eLearn Security Mobile Application Penetration Tester (eMAPT)
- eLearn Security Certified eXploit Developer (eCXD)
- eLearn Security Certified Web Application Penetration Tester eXtreme (eWPTXv2)
- ZeroPoint Security Certified Red Team Operator (CRTO)
- TCM Security Practical Network Penetration Tester Certification (PNTP)
- Red Hat Certified Systems Administrator (RHCSA) course.
- CompTIA Security+
- CompTIA PenTest+
- CJIS Certified, Washington State Background Checks

ii. Wireless Response

Emagined Security Consultants have performed wireless penetration tests in over 60 countries around the world including the State of Washington, State of California and the State of Colorado. Emagined Security consultants have also been brought in as guest lecturers at the University of Utah on Wireless penetration testing. Additionally, some Emagined Security consultants have extensive wireless engineering backgrounds to include the construction of the first Wireless ISP in the state of Utah over 20 years ago. Emagined Security consultants are WiFi certified wireless network penetration test specialists. Emagined Security's methodology goes beyond the GAWN methodology and include the following but are not limited to:

- 802.11 testing
- 802.11 Fuzzing Attacks
- Bluetooth
- DECT
- DoS on Wireless Networks
- Rogue Networks
- Securing and Configuring Wireless Clients
- Sniffing Wireless
- TKIP
- WLAN Auditing Methodologies
- WLAN Intrusion Detection Technology
- WPA2
- Zigbee

Emagined Security's methodology consists of the initial wireless penetration testing effort being performed using no knowledge of wireless network locations. Before executing the subsequent

wireless penetration testing effort, the end user department will provide network configuration and product information to Emagined Security. Emagined Security will inform the department representative of the times during which scans will be conducted using the following two-phased approach.

Phase 1: Blind wireless LAN assessment

Given no information about the wireless network (and not using social engineering), CONSULTANT will perform the following Penetration Test:

- Identify the presence of a wireless WAP/LAN and operating frequency
- Connect to access point
- Impersonate an access point
- Capture information transmitted over the air
- Decrypt and read transmitted information
- Further map/identify internal network
- Gather information from client computer

Phase 2: Wireless LAN assessment

Given network configuration and product information, Emagined Security will attempt to perform the following tasks:

- Identify the presence of a wireless WAP/LAN and operating frequency
- Identify the components and network from outside of the physical office
- Connect to access point
- Impersonate an access point
- Capture information transmitted over the air (confirm encryption)
- Decrypt and read transmitted information (analyze traffic to map other network components)
- Further map/identify internal network
- Gather information from client computer

See Section i. above for additional information on certifications.

iii. Experience with ICS / SCADA / OT in Government Response

Emagined has experience in testing live sensitive environments with high availability requirements. Testing in highly sensitive areas such as Industrial Control Systems (ICS), Medical equipment, Supervisory Control and Data Acquisition (SCADA) and other Operational Technology (OT) located in a secure environment requires extra care and evaluation. Due to the sensitive nature of testing, many aspects of the testing will be determined at the review of the environment. Some systems may require a more passive approach to testing with may include packet capture of data and replay of data based on potential vulnerabilities. Since most of these types of systems are production, additional care must be provided to ensure systems are not exploited or aggressive testing and create system stability issues.

The following testing approach options may be used to test high availability networks and systems while choosing the right approach for the associated risk level:

- Vulnerability Scanning with Validation

    - Lowest Level of Effort
    - VM / Physical Scanner Required to be Installed in Network and Allowed to Connect with EMAGINED Facilities
- Penetration Test (Favorite Approach)
    - Low Level of Effort
    - VM / Physical Scanner Required to be Installed in Network and Allowed to Connect with EMAGINED Facilities
- Passive Penetration Scanner
    - Medium Level of Effort
    - Span Ports Required
    - Additional Tool License Fees Required As They Installed In An Environment
- Sniffer on Core Switches with Manual Review
    - Very High Level of Effort
    - Span Ports Required
- Configuration Reviews of Systems
    - Very High Level of Effort
    - System / Application Details Required in Advance

Emagined will work with the SOA to ensure the appropriate test is chosen to balance the comprehensiveness vs associated risks before testing in these areas.

See Section i. above for additional information on certifications.

iv. Expert-level Knowledge and Experience Response

Emagined Security performs hundreds of penetration tests, vulnerability assessments and wireless assessments including reviewing complex network designs and architectures every year. Our consultants have been performing architecture reviews and creating complex secure networks for over 25 years. Additionally, Emagined Security Consultants have expert knowledge of network and web application architecture to ensure the sensitive data flow of information in organizations is protected during the lifecycle of the data. **During one engagement, Emagined Security was able to identify, during our manual penetration testing, 10 new zero-day vulnerabilities. Emagined Security uses a combination of automated and custom-built testing tools to identify both known vulnerabilities (those that are found in the CVE database) as well as identifying unknown vulnerabilities which cannot be identified using automated tools.**

Emagined Security, when necessary, provides expertise reviewing customer architecture and data flow(s) to ensure customers understand the appropriate methods of security for their digital information wherever it is transported.

After engagements complete, Emagined Security **continues to answer questions** regarding pervious penetration tests for several months / to a year to ensure state entities and agencies can remediate from vulnerabilities and feel comfortable with their security posture.

In reports, each finding includes detailed information as to the issue of concern and possible remediation or resolution to the problem. As such, each identified finding will be labeled with a severity rating, as follows: (Bullets details have been removed due to page limits - Details can be found in the Sample Report)

- Critical
- High

- Medium
- Low
- Informational

Additionally, each finding identified has been categorized by the difficulty of exploitation. The difficulty of exploitation is subdivided into the following categories:

- Easy
- Moderate
- Hard

If additional detail is requested, Emagined can also create a high-level risk register to define required data in order to scope remediation efforts based upon the identified risks. The risk register creation may utilize both vulnerability scanning and data provided by the agency about the networks and systems. The risk register may contain the following types of data as desired and available: (Only Sample Bullet Presented Due to Page Limit)

- Vulnerability Title
- Vulnerability Type
- Vulnerability Score
- Remediation Assignees
- Service / System Owner
- Asset Type (System / Application / Data)
- Compliance Requirements (Regulatory & Policy Driven)
- Likelihood of Occurrence
- Risk Rating
- Remediation Priority
- Remediation Status
- Comments

This risk register can also establish definition, understanding, and measurement of Risk Tolerance and Risk Appetite for Information Security

Relevant State and Local Government Experience

As stated above, over the past 7 years, Emagined Security has performed for the **State of Washington** over **70 Penetration Test engagements on State Agencies, Counties, Cities, Schools, Municipalities and Hospitals. This includes hundreds of web applications, mainframes, thick clients, thousands of network IPs and Wireless Network** tested for **Cities, Counties, State Agencies, and Hospitals** and identifying multiple **zero-day exploits** in the testing. In Addition to the State of Washington, Emagined Security has performed Penetration testing for other States Auditor Offices as well as Cities and Counties in California, Texas and Arizona.

Many penetration tests are performed on production web applications that require a high degree of skill to ensure that applications are not taken offline during the testing. To ensure that sensitive production applications are not impacted by penetration testing, Emagined Security does limit automated penetration testing with specific, tested configurations created by Emagined Security to not impact production capabilities. Emagined Security's penetration testing is exceptionally thorough and finds many vulnerabilities that just running a "tool" does not uncover. This is due to the combination of automated testing tools mixed with Emagined-created tools that frequently identify zero-day vulnerabilities.

Emagined Security's methodology is similar to the methodology prescribed in this document and in Exhibit C, with limited dependence on automated scanning. Due to page limitations, Emagined has not included a full penetration testing methodology. Emagined Security can provide this if requested.

Emagined Security has been successfully testing production systems with manual testing, designed by Emagined Security, to ensure that production is not impacted during testing. Emagined Security's manual testing methodology is comprehensive to ensure that applications are tested thoroughly without impacting performance.

Some of Emagined Security's experience in performing these tests are:

- *Emagined Security has performed Penetration Testing for dozens of Cities, State Agencies, Hospitals and Counties in The State of Washington*
- *Emagined Security has performed Penetration Testing for several Cities in The State of California*
- Emagined Security has tested **CJIS certified** applications and networks where exposure of this data could cause major impact to law enforcement.
- Emagined Security has performed **SCADA testing**, remotely with successful results and comprehensive testing with no outages.
- Emagined Security has performed testing on production web applications for eCommerce while in production and processing thousands of transactions per minute.
- Emagined Security has tested credit card networks that require 99.99995% uptime requirements ensuring that no downtime was incurred during the testing.
- Emagined Security has tested financial applications where loss of transactional information would have resulted in large financial losses for the customer we tested.
- Emagined Security has tested Certificate validation systems where the loss of OCSP connectivity would have resulted in the inability to validate highly sensitive certificates in production.
- Emagined Security has tested mainframe applications (without causing outages) where causing an outage could impact state usage of traffic systems.

These are just some examples of production testing performed by Emagined Security without taking a system offline. Emagined Security ethical hackers possess a variety of certifications that have been previously listed above.

Representative Projects

Representative Project Number 1

Project Statement: Emagined Security was contracted to perform a penetration test for a [redacted] [12]

Project Scope: Emagined Security scoped the project to include multiple types of penetration testing. In scope was 6 Web application Penetration Tests, 1 Thick Client Penetration Test, SCADA Testing of 25 systems, External Network Penetration Testing of 50 IP addresses, Internal Network Penetration Testing of 1,200 IP addresses and a Firewall Review.

Project Background: Emagined Security assigned a **Project Manager** and a **Principal Penetration Tester** to work with the agency to scope out the required assets that needed penetration tested. The Project manager and Principal Penetration Tester provided the scope to the agency for confirmation. After the scope was agreed upon, the Project manager worked with the agency on a Rules of Engagement to provide the scope of all items to be included in the penetration test and included the types of testing to be performed, items out of scope and contacts to be contacted in case of an issue during the approved testing windows. Rules of engagement also included the methodology of the penetration testing to be performed. Rules of

engagement also included IP Addresses and URLs of scope to be tested as well as out of scope systems and subnets that were not to be tested.

During the course of project, Emagined Security provided daily start and stop notices as well as a status of testing which included the test being performed, any identified vulnerabilities per application or network and the percentage completed. Additionally, each day, per the agency's request, Emagined Security scheduled a 15-minute conference call with the agency and Emagined Security to discuss any issues identified during testing or any complications to completing testing as well as to get go/no go on application testing per the agency's timing needs.

The Principal Penetration Tester assigned penetration testers to kick off the project by starting automated scans of the network systems in scope for the internal and external networks. This was followed up by a Senior Penetration Tester reviewing the information and determining the next steps for manual penetration testing of the systems. Additionally, a Principal Penetration Tester reviewed and assigned web and thick client tests based on the skills needed to perform the penetration test to the appropriate penetration tester. The Senior Penetration Tester continued to follow up with each penetration tester to ensure they did not have any questions in performing the penetration testing they were assigned and consolidated all findings into a "Vulnerability List".

Emagined Security additionally worked with Agency to setup a sensor in a [redacted][12][redacted] as well as performed a firewall review based on configuration management and automated testing of the configuration files from the firewall.

Project Duration: Project duration was 4 weeks

Scheduled Resources: Emagined Security provided 2 Principal Penetration Testers (15+ years' experience), 3 Senior Penetration Testers (10+ years' experience) and 3 Mid-level Penetration testers (5+ years' experience) who are all employed by Emagined Security as full-time penetration testers.

Project Results: Results included detailed information about vulnerabilities identified during the course of the engagement. An out brief meeting was held with the agency to relay information about the final testing and vulnerabilities identified where Emagined Security went over each vulnerability to ensure the agency understood the impact of the identified vulnerabilities.

Project Deliverables: During the course of the project, there were several deliverables that Emagined Security agreed to which included a daily status update including identified vulnerabilities; A daily start and stop notice sent to a pre-agreed upon list of agency employees that needed to know what was being tested and a comprehensive report detailing out each identified and validated vulnerability per application and network that provided the agency with clear information on the vulnerabilities identified during the course of the engagement. The Comprehensive report with details of how to recreate the testing Emagined Security performed was included in the final report that was accepted by the [redacted][12]

Representative Project Number 2 (Note: Emagined has performed over 75 engagements that are similar to this Project Representation and Project 1)

Project Statement: Emagined Security was contracted to perform a penetration test for a [redacted].

Project Scope: Emagined Security scoped the project to include multiple types of penetration testing. In scope were:

- 4 Web application Penetration Tests,
- 2 Thick Client Penetration Test,
- IoT Testing of 2 subnets of sensitive medical equipment,
- External Network Penetration Testing of 20 IP addresses
- Internal Network Penetration Testing of approximately 2,000 IP addresses
- Firewall Review
- OSINT Review

Project Background: [redacted] are extremely high risk as targets for ransomware and other security issues including compromises by 3rd party vendors and open VPN connections. Since Hospitals are normally severely underfunded and understaffed, our goal was to minimize the amount of staff time required from the customer to assist with project coordination and involvement during active testing.

Emagined Security starts every project by assigned a Project Manager and a Principal Penetration Tester to work with the organization to scope out the required assets that need penetration tested. The Project Manager and Principal Penetration Tester provided the scope to the Hospital for confirmation that this would be the comprehensive penetration testing they were looking perform.

After the scope was agreed upon, the Project Manager worked with the [redacted] on a Rules of Engagement to provide the scope of all items to be included in the penetration test and included the types of testing to be performed, items out of scope and contacts to be contacted in case of an issue during the approved testing windows. Rules of engagement also included the methodology of the penetration testing to be performed. Rules of engagement also included IP Addresses and URLs of scope to be tested as well as out of scope systems and subnets that were not to be tested.

During the course of project, Emagined Security provided daily start and stop notices as well as a status of testing which included the test being performed, any identified vulnerabilities per application or network and the percentage completed. Additionally, each day, per the hospital's request, Emagined Security scheduled a 15-minute conference call with the hospital and Emagined Security to discuss any issues identified during testing or any complications to completing testing as well as to get go/no go on application testing per the hospital's timing needs.

The Principal Penetration Tester assigned penetration testers to kick off the project by starting automated scans of the network systems in scope for the internal and external networks. This was followed up by another Principal Penetration Tester reviewing the information and determining the next steps for manual penetration testing of the systems. Additionally, 2 Principal Penetration Testers were assigned web and thick client tests based on the skills needed to perform the penetration test. Emagined never assigns tests to team members that are not skilled to perform the work needed for the specific test. The Principal Penetration Tester continued to follow up with each penetration tester to ensure they did not have any questions in performing the penetration testing they were assigned and consolidated all findings into a "Vulnerability List".

Firewall and OSINT assessments were additionally kicked off to validate any potential lost data from the hospital. In reviewing the Firewall it was noted that there were quite a few open VPN connections to 3rd parties. We had a discussion with the hospital about these connections to help them understand the security risks associated with these connections and urged them to review them in more detail with the asset owners so they could help lock down some of these VPNs.

Project Duration: Project duration was 3 weeks

Scheduled Resources: Emagined Security provided 3 Principal Penetration Testers (15+ years' experience), 2 Senior Penetration Testers (10+ years' experience) and 2 Mid-level Penetration testers (5+ years' experience) who are all employed by Emagined Security as full time penetration testers.

Project Results: Results included detailed information about vulnerabilities identified during the course of the engagement. An out brief meeting was held with the hospital to relay information about the final testing and vulnerabilities identified where Emagined Security went over each vulnerability to ensure the hospital understood the impact of the identified vulnerabilities.

[redacted] [12]

Project Deliverables: During the course of the project, there were several deliverables that Emagined Security agreed to which included a daily status update including identified vulnerabilities; A daily start and stop notice sent to a pre-agreed upon list of hospital employees that needed to know what was being tested and a comprehensive report detailing out each identified and validated vulnerability per application and network that provided the hospital with clear information on the vulnerabilities identified during the course of the engagement. The Comprehensive report with details of how to recreate the testing Emagined Security performed was included in the final report that was accepted by the [redacted] [12]

Emagined has developed a specialized consolidated report for these types of engagements. This consolidated report allows the organization to have a full picture of the testing but also separate out needed vulnerability information to provide to technical resources to fix vulnerabilities or security issues.

Representative Project Number 3

Project Statement: Emagined Security was contracted to perform an Open-Source Intelligence review (OSINT) and External penetration test for a [redacted] [12] [redacted]

Project Scope: Emagined Security can scope out an External penetration test and open-source intelligence projects without impacting an organization heavily. Emagined Security has a methodology specific to scoping these engagements.

Project Background: [redacted] [12] [redacted]

Since this engagement was purely an external engagement our scoping and project management are more minimalized. Our goal is normally to:

- Have an introductory call with the [redacted] to determine any issues with the potential testing
- Determine the scope of IP addresses and Domains associated with the [redacted]
- Perform the OSINT review to identify any issues with lost or public information
- From the OSINT review identify any items that could need additional testing or reviews

Rules of Engagement are still used on these small [redacted] engagements. Emagined Security believes even small engagements should be treated as valued test opportunities and Emagined Security uses the same care and diligence on these small tests to provide value.

We started this engagement by providing a timeline for the OSINT and External Pen Testing and provided a detailed list of tasks and timeframes to perform the work. Once completed, Emagined Security created a status update of identified issues and vulnerabilities from the testing.

Project Duration: Project duration was 2 weeks.

Scheduled Resources: Emagined Security provided 1 Principal Penetration Testers (15+ years' experience), 1 Senior Penetration Testers (10+ years' experience) who are both employed by Emagined Security as full-time penetration testers.

Project Results: Emagined Provided Comprehensive Testing of their external network resources and discovery information from the OSINT review.

Project Deliverables: During the course of the project, there were two deliverables that Emagined Security agreed to provide. One was the external penetration testing report and the second was an OSINT review deliverable report.

Representative Project Number 4

Project Statement: Emagined Security performed multiple application and infrastructure penetration tests at hospitals and infrastructures managed / operated by a [redacted]. This penetration testing is required to assist in the protection of [redacted].

Project Scope: Emagined Security penetration testing scope included an External penetration test along with open-source intelligence projects. This included an attack surface review to ensure all appropriate systems were in scope.

Project Background: We started this engagement by providing a timeline for the attack threat vector review followed by External Pen Testing. Once completed, Emagined Security created a status update of identified issues and vulnerabilities from the testing.

During the scope of penetration testing a potential **indicator of compromise was identified** (a port known to be used by bad actors). The [redacted] personnel were immediately advised of our potential finding and an initial review of the situation was conducted. [redacted]

[redacted] [12] [redacted]. At that time, the penetration test was resumed and completed.

Project's Duration: Penetration Testing was completed in about 4 weeks. Additional time was allocated to the incident response activities that spanned a 2–3-week period including reporting.

Scheduled Resources: Emagined Security provided 1 Principal Penetration Testers (15+ years' experience), 1 Senior Penetration Testers (10+ years' experience) who are both employed by Emagined Security as full-time penetration testers.

Project Results: Emagined Provided Comprehensive Testing of their external network resources and discovery information from the OSINT / attack surface review and penetration testing.

Project Deliverables: During the course of the project, there were two deliverables that Emagined Security agreed to provide. One was the external penetration testing report and the second was an OSINT / attack surface review deliverable report. Additionally, a separate Incident Response report was provided.

Representative Project Number 5

Project Statement: Emagined Security was contracted to perform a penetration test for a [redacted] [12] [redacted]

Project Scope: Emagined Security scoped the project to include multiple types of penetration testing. In scope were:

- 6 Web application Penetration Tests service over 5,000 clients
- External Network Penetration Testing of 12,000 IP addresses
- Internal Network Penetration Testing of approximately 40,000 IP addresses
- Segmentation Testing of 12 networks

Project Background: Vendor chose Emagined Security to perform the penetration testing due to our **CREST Certification**. Since they are a global company, they needed to provide penetration testing by a CERTIFIED company that was recognized globally for penetration testing expertise. Many of their customers additionally require seeing that the testing is performed by a CREST Certified organization.

This project with its global nature required significant planning and project management. The Project Management of this engagement started before the SOW was completed due to the complexity. Emagined worked with the customer to identify the scope that needed to be tested and the regions the testing was to be performed in. Next Emagined Security provided a detailed list of client needs to ensure the project could be kicked off and started upon execution of the SOW. Emagined put together a detailed plan that documented the work to be completed and when each milestone would be attained.

During the course of project, Emagined Security provided daily start and stop notices as well as a status of testing which included the test being performed, any identified vulnerabilities per application or network and the percentage completed. No status calls were requested but the

Client asked that if we identify any critical or high findings Emagined Security would contact them immediately.

The Principal Penetration Tester reviewed the project plan with the project manager and worked with our VP of projects to assign the needed resources to meet the challenge of a global test with both internal and external components and timeframe for each test. The Project kickoff provided details of all the penetration tester assigned and the dates and times of each scheduled test.

Project Duration: Project duration was 12 weeks.

Scheduled Resources: Emagined Security provided 2 Principal Penetration Testers (15+ years' experience), 3 Senior Penetration Testers (10+ years' experience) and 2 Mid-level Penetration testers (5+ years' experience) who are all employed by Emagined Security as full-time penetration testers.

Project Results: Emagined met each client timeframe and date as originally planned, even with an application not being able to start on time. Emagined was able to get on a call with the Software engineers and help get the issues with the application identified and handled quickly.

Results included detailed information about vulnerabilities identified during the course of the engagement. An out brief meeting was held with the organization as well as a few of their software development groups to help them understand some of the vulnerabilities identified. During the course of the application testing, **Emagined identified several zero-day exploits** identified that needed immediate attention and required **custom exploit development**. Emagined Resources worked with the Software engineers to show them how we identified these vulnerabilities so the software engineers could test their fixes before Emagined did during remediation testing.

Project Deliverables: During the course of the project, there were several deliverables that Emagined Security agreed to which included a daily status update including identified vulnerabilities; A daily start and stop notice sent to a pre-agreed upon list of employees that needed to know what was being tested and a comprehensive report detailing out each identified and validated vulnerability per application and network and **per location** that provided the client with clear information on the vulnerabilities identified during the course of the engagement.

Direct Experience

- Demonstrate skills to communicate clearly, concisely and effectively both verbally and in writing.

  Emagined Security believes the best way to communicate is with our proven project management methodology. Emagined Security will assign an experienced project manager that enables the teams to communicate in both team meetings, emails and written documents (see our project methodology and project management approaches detailed below) in addition to the information presented in Exhibit C.

- Describe the firm's methods for maintaining staff qualifications.

  All penetration testers' skills are being continually reevaluated

- Emagined has a **dedicated VP of Penetration Test Training** whose main focus it to continually evaluate the team, work to enhance their skills, and educate them on the latest attach techniques
- All penetration testers are required to acquire at least one additional certification per year to ensure skills are up to date
- During all training penetration tester are challenged to continually identify ways to improve our methodology
- We have scheduled a new internal program of bi-weekly training to further enhance our skills
- An annual review process is being created to reassess skills each year for all penetration testers

All work is completed by **CISSP, CEH, OSWE and OSCP Certified** engineers located in the United States.

- No testing or data is off-shored
- All employees are authorized to work in the United States
- All employees are background checked by the State of Washington Auditors office as well as pass Emagined Security's background check
- **No penetration testing** is outsourced to 3rd parties
- All Penetration Testers are full time Penetration Testers and do not deliver other Emagined Security services

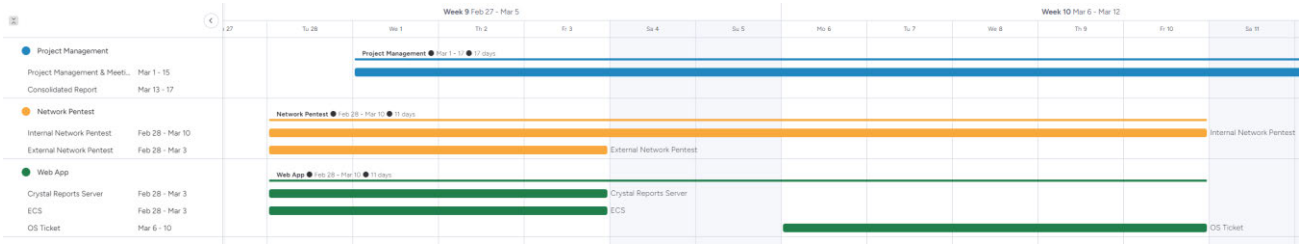
- Management approach, methodology and implementation strategies for managing and delivering their product.

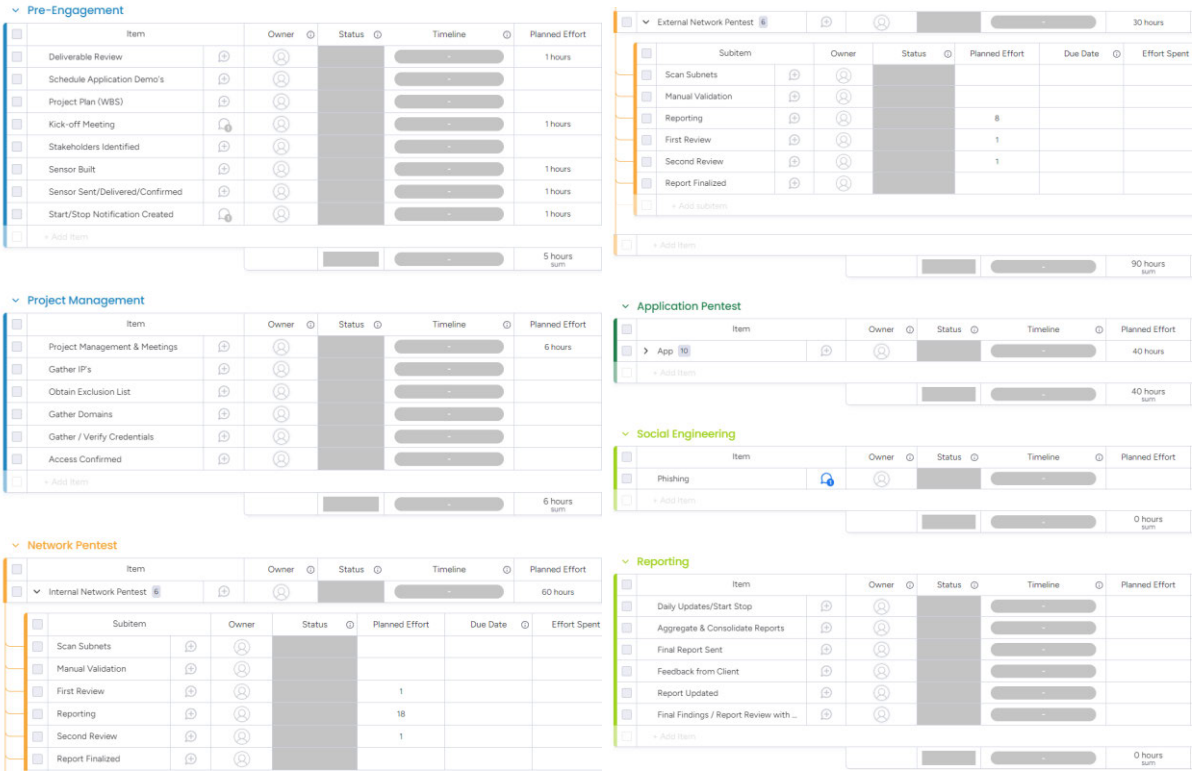
Emagined Security utilizes a proven project management methodology that allows us to consistently monitor project status, budgets and quickly escalate and resolve issues. Emagined Security has performed a similar engagement for other State agencies such as the State of Colorado.

At a minimum, we recommend that the following project management methods be established for the project.

High Level Project Plan:

The following high level project plan portrays the general approach and estimated milestones associated with our proposed approach.





Emagined Security has broken project management into two (2) types of engagement. Small Web application and infrastructure tests that are performed over a short period (Normally one – two weeks) and longer engagements that may span weeks to months.

Project Tracking and Status Reporting:

A detailed project plan will be developed at the beginning of the project. The plan will be reviewed and approved by the project sponsors. Progress will be monitored against the approved plan. Formal status reports will be delivered on a schedule defined by the project sponsor. The status report should include activities completed in the reporting period, activities not completed, a discussion of tasks and deliverables in each individual project activity to be completed in the following reporting period. Any issues that potentially bear on project success will be identified in this section. The status reports will be reviewed in regular project status meetings. The project sponsor will define the frequency of status reporting, but Emagined Security recommends that the status meetings be conducted on a weekly basis. The primary point of contact from Emagined Security will attend the status meetings.

Issues Management and Escalation:

Effective issue management is a critical success factor for the management of challenges that are experienced during the project life cycle and allows for the following:

- Visible decision-making process
- Means for reaching consensus on questions concerning the project
- Project key decision documentation

An issues log will be maintained to log and track all issues. Open issues will be reviewed during project status meetings and escalated if needed to the executive project sponsor.

Scope Change Management:

A key to success in project management is the ability of the project manager and project team to effectively manage scope. When issues occur, either the requirements are not properly bounded or the scope is not controlled. There is a natural discovery process in all projects due to factors such as omissions, mistakes, creativity, misunderstandings, and external influences. This discovery process normally creates pressure to expand scope. The purpose of a scope management process is to constructively manage that pressure.

Scope expansion is acceptable as long as:

- Both parties agrees that the new requirements are justified
- Impact to the project is analyzed and understood
- Resulting changes to the project (e.g., cost, timing, quality, and human resources) are approved and properly implemented

The main tool the project manager uses to manage scope is the Statement of Work (SOW) and associated Rules of Engagement (ROE) and recorded change requests. The SOW & ROE specifies the original agreement between the Customer and Emagined Security. Change requests are created to document any subsequent change to this baseline scope and are tracked by the project manager. Throughout the project, proposed changes are documented and screened by the project manager. The primary vehicle communicating potential scope issues is the weekly status report. The project manager determines which suggested changes might be necessary, and these are investigated to determine the impact of accepting or rejecting them. When the impact analysis is complete, the change is either approved and the project plan is adjusted to reflect the decision or the change is rejected. At any point in time, the current project scope is determined by the baseline scope defined in the SOW plus all the approved change requests.

Critical Success Factors:

Critical success factors assist all parties in ensuring the project's ultimate success. They include the following:

- An Executive Sponsor who actively supports the project and project team should be able to spend sufficient time on the project to stay abreast of any issues and the status of the engagement at any point in time.
- Efficient communications of work-in-process and gathered materials input into the project. We will establish a common repository of project-related data that will be maintained for the engagement team and this data will be a final deliverable of the engagement. The Project Sponsor will be notified of the value-added opportunities identified as a direct result of this engagement.
- Dedication to timely responses to requests from the consulting team.

At the highest level, we consider a project successful when the client agrees that the co-developed goals have been achieved. A few key aspects of ensuring and measuring success are:

- Co-developing goals and success criteria before the project begins.
- Continuous communication throughout the project to keep both parties abreast of progress and to obtain interim buy-in to work-in-process as it emerges.

- Customer satisfaction interview with the Project and Executive Sponsors at the end of the project to determine the level of satisfaction based on deliverables as compared to success criteria defined at the beginning of the project.

This approach is based on our belief that to obtain optimal results, it is essential to maintain feedback throughout the engagement.

Knowledge Transfer

At Emagined Security **we practice Knowledge Transfer** to better enable our clients to meet the challenges of securing business operations. Our experience shows that those clients who are best informed are better clients because they quickly grasp the impact of our analysis and the fact that we are working with their best interest in mind. Through knowledge transfer, our clients become stronger, better informed and more responsive to the results of Emagined Security's analysis and support.

- Describe their ability and capacity for delivering services proposed.

Emagined Security has several project and program managers that work to schedule penetration tests efficiently and coordinated to ensure that customers have penetration tests scheduled in a timely manner.

Emagined Security **core service is providing penetration testing**, vulnerability assessments and risk assessments. All consultants are familiar with our proposed methodologies and have performed these services for numerous customers over the course of Emagined Security's approximately 23 years.

Emagined Security has over 40 consultants with extensive information security backgrounds. Of those 40 consultants, 20 have capabilities to perform penetration testing, 12 are full time penetration testers. **All have extensive experience with state and local governments**. Emagined Security understands how to work with smaller agencies and how to not over engineer responses to penetration test reports to overwhelm those agencies.

As demonstrated in our detailed methodologies above, Emagined Security has the proven methodologies, the skills and the experience to provide the services which have been proposed. If additional details are requested, a Teams Meeting can be setup to demonstrate our abilities / capacity.

QUALIFICATIONS (Optional and separate from section above**)**

As Emagined has been performing these tests for the SAO for the past **7 years**, Emagined Security does not envision any complications in delivering the work requested.

Many other areas of Penetration Testing / Red Teaming areas have not been included in the list of potential projects listed in the RFP that are available services from Emagined Security:

- Penetration Testing
  - Internet Presence Discovery
  - Physical Stand-alone System Testing
  - Cloud Docker Kubernetes
  - DAST Testing
  - API Testing
  - PCI CDE Testing
  - Database Testing
  - Source Code Reviews

    - Sensitive Data Flow Reviews

- Red Team Testing
    - Attack Surface Reviews
    - Internal Red Team Testing
    - External Red Team Testing
    - SOC MSSP Effectiveness
    - Fuzz Testing
    - Ransomware Simulation Testing
    - Physical Control Assessments
    - Social Engineering
    - Open-Source Intelligence Reviews (OSINT)

RESUMES

<See *"Exhibit D - Qualifications-Emagined EHTeam Resumes 2023 Final"*– Not Included In Page Count>

SAMPLE REPORT

<See Sample Report *"Exhibit D - Qualifications-Emagined ACME_Sample_Report_2023 Final"* – Not Included In Page Count>