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

EXHIBIT C – QUOTATIONS

BIDDER: Emagined Security, Inc

The size and complexity of each selected state agency and/or local government will vary.
The evaluation process is designed to award a contract to the Consultant(s) whose proposal best meets the requirements of this RFQQ.

Instructions:
The State Auditor's Office requires two price quotes and a sample proposal for a State Agency for this RFQQ.

1. Proposers must provide a single, not-to-exceed, "blended hourly rate" price quote for the contract term. Proposers shall be bound by the hourly rate they quote in this RFQQ. The rates quoted will be considered "not-to- exceed" rates. The blended hourly rate should include travel and any other anticipated expenses. Note: Travel is anticipated to be limited and will need to be pre-approved.
2. Because the specific state agencies and/or local governments are not identified, bidders are instructed to provide a bid (price quote) for the sample state agency listed below as well.
    - Proposers must consider the following when completing the Price Proposal: Overtime rates are not allowed.
    - Quote all-inclusive rates in United States dollars to include travel and all expenses to accommodate working with State Auditor's Office. Consultants are required to collect and pay Washington State taxes as applicable.

Columns left blank may be deemed nonresponsive and will not continue further in the process.

	Blended Hourly Rate
Security Assessment Services	**$ 170**

	Sample State Agency Cost
Security Assessment Services	**$ 29,920 ***

* The request does not provide details of the application penetration tests requested so Emagined assumes these are Level 1 Small Applications and Level 1 Testing

3. The Proposal must contain a comprehensive description of services including the following elements:

Project Approach/Methodology (MR) – Include a description of the proposed approach and methodology for completing the testing, performing the analysis and preparing the report.

Work Plan (MR) – Include all project requirements and the proposed tasks, services, activities, etc. necessary to accomplish the testing in the scope of the project defined in this RFQQ. This section of the technical proposal must contain sufficient detail to convey to members of the evaluation team the proposer's knowledge of the subjects and skills necessary to successfully complete the testing for this project. Include any required involvement of State Auditor's Office staff.
Project Schedule (MR) – Include a project schedule indicating when the testing would be completed and when deliverables, would be provided. Bidders will consider that documentation detailing the testing completed to identify issues, including screen shots as necessary, is required to support the detailed testing results communicated to agencies.
Deliverables (MR) – Fully describe content and format of deliverables to be submitted under the proposed contract.

The sample state agency is defined as having 1,000 employees; with structured and unstructured data, servers, workstations, network devices, mobile systems, firewalls, virtual private networks and other systems prevalent in an enterprise environment; has some internal development of web facing functions with reliance on third party vendors for some functions; and has confidential data that includes PII, HIPAA, criminal justice and payment card information. The proposer should provide an estimated number of hours expected to be required to complete all deliverables for this sample state agency audit. All the work will be completed remotely, with the exception of the Industrial Control System, which will be completed on-site.

Penetration testing Scope: Internal and External

1. Internal Penetration testing
Internal testing is performed on assets and networks owned by the government agency. Internal systems are used to conduct business internal to the organization.
Internal Application Testing:

(I) Internal Application
- Web application
- Test environment
- Hosted locally
- Authenticated and unauthenticated

(I) Internal Application
- Thick Client
- Test environment
- Hosted locally
- Authenticated and unauthenticated
- Contains CJIS Data

(II) Industrial Control System -Regulating water for a community of 20,000 users
- The SCADA environment consists of a water treatment plant
- 3 Human Machine Interfaces (HMI); one at each of public works, the treatment plant and maintenance facility.
- There are 15 remote sites with 2 Programmable logic controllers per site connecting back to public works over the internet using site-to-site VPN's.

(III) Configuration and design review of a Firewall
- Configuration review of the rules on one firewall
- design review of: 3 subnets, Business network, Guest network

(IV) Internal Network Penetration Testing: the scope is limited to 500 internal IPs and includes a sample from the following:

- 1,000 Workstations
- 75 Servers Windows and Linux (Virtual and Physical)
- 10 Servers Windows and Linux (Cloud Hosted)
- 50 Multifunction Printers
- VLANs: management(IT), end user(business), VOIP, SCADA
- 2 AD Domains

2. External Penetration testing

External testing is performed on applications and services owned by the government organization. External applications are those that are accessible by the public or select clientele by way of the internet.

(I) External Website Testing: Government's public website (e.g. GovernmentName.gov)

- Production environment
- Hosted locally
- Unauthenticated

External Application Testing:

(II) External Application 1

- Mobile application (iOS and Android)
- Production environment
- Hosted by vendor
- Authenticated only

(III) External Application 2

- Web Application
- Test environment
- Hosted in the cloud
- Authenticated and unauthenticated

COMPUTATION

The cost proposal will be scored by multiplying the price weight by the best value ratio. The price weight is defined as the lowest proposed price divided by the vendor's proposed contract price.

The best value ratio is defined as all other scored components (excluding costs) divided by the total possible score for these components. This means that the overall score for the cost proposal will account for the robustness of the proposer's qualifications as well as their proposed price. We will include both the blended hourly rate and the price quote in scoring the cost proposal. The cost proposal will be worth up to 10 percent of the total possible points

ADDENDUM TO EXHIBIT C: EMAGINED SAMPLE PROPOSAL

Comprehensive Description of Services - The following are work descriptions for tests that have been simplified due to page limits for the requested tests.

Scope of Testing

1. **Internal Penetration testing (Bullet Omitted Due to Page Limit)**

Internal Application Testing:

(I) Internal Application (Web)
(II) Internal Application (Thick Client)
(III) Industrial Control System -Regulating water for a community of 20,000 users (SCADA Test 30 Systems)
(IV) Configuration and design review of a Firewall
(V) Internal Network Penetration Testing: the scope is limited to 500 internal IPs

2. **External Penetration testing (Bullet Omitted Due to Page Limit)**

(I) External Website Testing: Government's public website (e.g. GovernmentName.gov)

External Application Testing:

(II) External Application 1 (Mobile)
(III) External Application 2 (Web)

Web Application Penetration Testing

EMAGINED will assess CUSTOMER's web application for security vulnerabilities on the following Web Application(s). As such, EMAGINED will attempt to identify the implemented security controls or lack of controls protecting against Internet-based attacks. Access attempts to the web application to scan for vulnerabilities will take place from a location on the Internet, to mimic standard access rights available to general Internet users. EMAGINED testing is designed to be exhaustive, which means that the team will not stop at the first successful penetration but will continue to identify all vulnerabilities and attack vectors.

EMAGINED will test the application's security controls to determine if an attack may result in inappropriately viewing, altering, or deleting information. During the assessment, EMAGINED will perform testing activities mimicking two types of users:

- Unauthorized User attempting to gain access
- Authorized User trying to acquire and utilize enhanced or inappropriate privileges

EMAGINED will require several accounts provided by CUSTOMER to perform these tests. Testing will include but is not limited to the following:

- Login testing - user accounts and passwords
- Encryption/SSL testing
- HTML code and form vulnerabilities
- Server and web server configuration or updating/patching failures or weaknesses
- Executable code testing such as buffer overflows and IIS weaknesses
- Credential, authentication and cookie testing

- Application code, back door or debug option weaknesses
- Hidden field manipulation
- Parameter tampering
- Cookie poisoning

Network Penetration Testing

EMAGINED will perform an external penetration test against the Internet architecture (i.e., firewalls, DNS servers, routers, switches, load balancers, and supporting systems).

As such, EMAGINED will attempt to identify the implemented security controls or lack of controls protecting against Internet-based attacks. Access attempts to the servers to scan for vulnerabilities will take place from a location on the Internet, to mimic standard access rights available to general Internet users.

If EMAGINED successfully penetrates the firewall and/or other filtering devices, EMAGINED will attempt to gain access to systems behind the security mechanism. By attempting to gain access to the systems on the subnet, EMAGINED will attempt to identify risks associated with the current security configuration.

The Penetration Test will begin with passive probes that are designed to avoid detection and will be escalated to aggressive active tests that should be easily detected. The penetration test of the Internet-facing architecture will be structured as follows:

Passive Data Collection:

The initial phase of any security review involves extensive data collection and penetration studies are no exception. The following methods may be used as part of this information-gathering phase:

- Web searches and newsgroup browsing
- DNS zone transfers, InterNIC type queries
- IP scanning and SNMP sweeps
- Network mapping with traceroute and other tools
- Social Engineering (if allowed)
- Initial target identification

Active Intrusion:

Once the active intrusion phase is begun, targets are more likely to be alerted to suspicious activity. This phase serves to identify potential or known vulnerabilities that could be exploited by intruders. This is the main analysis phase that correlates the information gathered. Methods for performing this phase can include:

- Vulnerability scanning
- Port scanning

Aggressive Penetration:

The aggressive phase is typically only used when a CUSTOMER needs to demonstrate actual data or system compromises. This phase involves utilizing the identified vulnerabilities to gain access to internal systems and networks. This phase typically utilizes many tools that may be available in the public domain and are used by actual intruders. The penetration agreement tightly controls the methods used during this phase, and activities are logged extensively.

SCADA Internal Network Penetration Test

EMAGINED will perform an internal SCADA Penetration Test against systems located in a secure SCADA environment onsite at CUSTOMER. Due to the sensitive nature of SCADA testing, many aspects of the SCADA testing will be determined at the review of the SCADA environment. Some SCADA 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 SCADA systems are production, additional care will be provided to ensure systems are not exploited or aggressive testing does not create system stability issues.

The following approach may be used to test the SCADA environment (Details Can Be Found in Exhibit D Due to Page Limitations):

- Vulnerability Scanning with Validation
- Penetration Test
- Passive Penetration Scanner
- Sniffer on Core Switches with Manual Review
- Configuration Reviews of Systems

Based on the information provided by CUSTOMER, Emagined believes that utilizing the following approach:

- **Penetration Test – Low Level of Effort (VM / Physical Scanner Required to be Installed in Network and Allowed to Connect with EMAGINED Facilities)**

Mobile Application Penetration Test

EMAGINED will assess the mobile applications written to run on the Apple iOS **or** Android (pick one platform to test) created for or by CUSTOMER for security vulnerabilities to enable clients to quickly identify, assess and remedy security holes.

Applications may include standalone applications that run on the mobile platform or applications created to communicate to databases, internet or internal servers, thick clients, 3rd party applications, or other general commercial off the shelf (COTS) programs.

Applications are tested utilizing both authenticated and non-authenticated access to the application to ensure a comprehensive approach is taken to validate the security of the application. The mobile penetration test is accomplished by performing scheduled and selective probes of the mobile application's communication services, connections to the operating systems in which the Application is loaded, key application functions, in search of those vulnerabilities. (Sub Bullets have been limited to a sample set due to page limits)

- Application Based Mobile Device Management
  - Certificates
  - URL Filtering
  - Effective use of strong encryption
- Application Data Security
  - Data Segmentation
  - Encryption/SSL testing
- Application Code
  - Application code, back door or debug option weaknesses
  - Cookie poisoning
- Mobile Application Configuration
  - Application patching and configurations
  - Credential, authentication and cookie testing – Anti-Jailbreaking
- Backend Connected Systems
  - Backend Patching and Configurations
  - Backend Server Configuration

Application Penetration Test (Appliance)

EMAGINED will assess specific commercial off the shelf programs (COTS) in use by CUSTOMER or custom built applications developed by CUSTOMER for security vulnerabilities to enable clients to quickly identify, assess and remedy security holes.

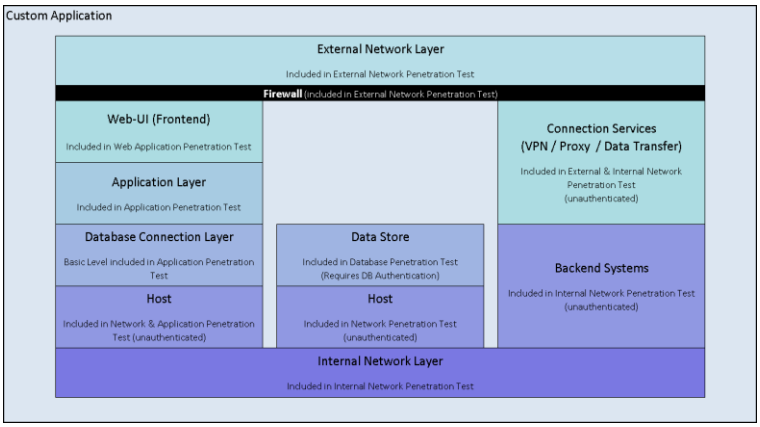
Applications may include databases, thick or thin clients, 3rd party applications, or general commercial off the shelf (COTS) programs, to include full host to end-user environments.

EMAGINED will specifically focus utilizing our methodology on the following company objectives:

- Engage individuals with expertise in software and platform security to provide an independent view of the target's robustness and platform security.
- The evaluation team will operate from an external (no credentials) point of view. NOTE: Additional testing may be performed after credentials are provided if desired.
- Where the attacking team believes they have an exploit but cannot fully understand the circumstances or details in which to trigger it, they may contact the CUSTOMER Platform Security.
- Coordinate with CUSTOMER for assistance under the premise of saving time of which an attacker would have at their disposal.
- Provide security testing that adds significant value beyond the multiple scanning tools that CUSTOMER may utilize

EMAGINED will start the project by assessing the impact of potential interruptions on CUSTOMER operations and business. EMAGINED will explain the ramifications of each identified potential interruption and inform CUSTOMER of the processes necessary to reduce risks from the effects of these potential interruptions. EMAGINED will prepare a general strategy for recovery, will identify alternative responses that are practical for CUSTOMER and specify approaches necessary for implementation. EMAGINED will work with CUSTOMER as its partner during its growth and search for solutions designed to meet CUSTOMER's steadily changing needs.

Applications are tested utilizing both authenticated and non-authenticated access in order to ensure a comprehensive approach is taken to validate the security of the application. The application penetration test is accomplished by performing scheduled and selective probes of the application: (Sub Bullets have been limited to a sample set due to page limits)



Testing will focus on a variety of security issues such as:

- User interface
- Business logic
- Application framework
- Communication services
- Authentication
- Authorization
- Access control
- Protocol analysis (manipulation / fuzzing)
- Abuse of functionality / fraud

A custom application penetration test will be structured as a merging of application and network penetration tests with detailed methodology changes that consider the different architectures. This includes distinct testing components as depicted above.

Project Approach/Methodology (MR)

Emagined Security will follow the OWASP Top 10, NIST and CREST methodologies to complete the assigned testing. As a CREST Certified company with highly certified and experienced Penetration Testers, Emagined Security will utilize the appropriate model to perform the specific testing requested for the state agency. An effective penetration test project approach and methodology start at introduction to the project. The individual scoping the penetration testing must be equally skilled in penetration testing management, methodology and performance as the penetration testers. Emagined Security Project Managers have over **25 years of experience working with Penetration Testing**. Since this sample Agency has CJIS data, **ALL PENETRATION TESTER ASSIGNED TO THIS ENGAGEMENT WILL HAVE CJIS CERTIFICATION AND WASHINGTON STATE BACKGROUND CHECKS COMPLETED.** Emagined has scoped these as *Tier 1* applications to ensure competitiveness with other bids.

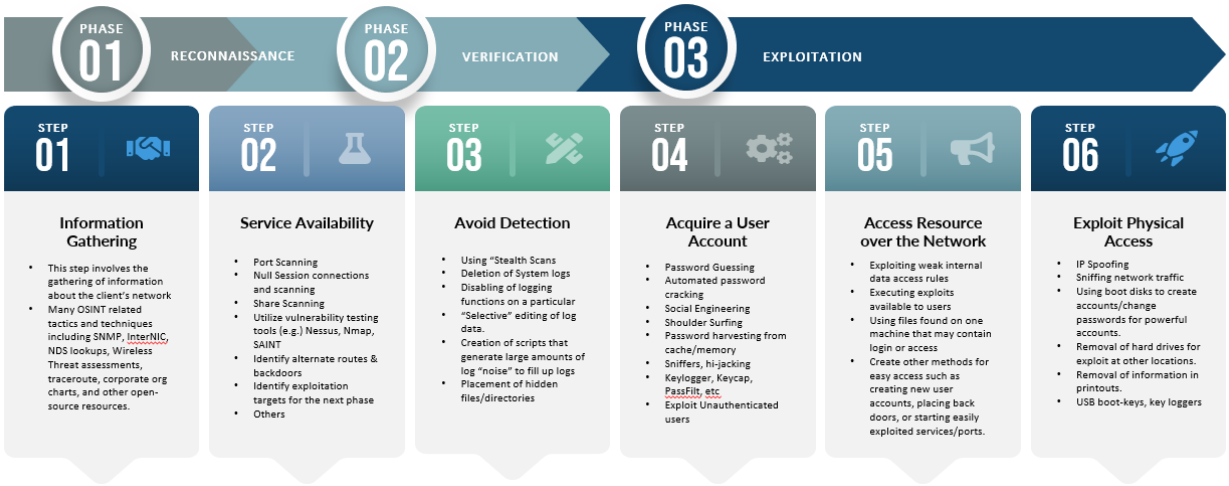
Based upon the sample organization , Emagined Security will provide the following staff:

- 1 Penetration Test Coordinator – Will provide scheduling and reviews of scoping, Rules of Engagement (RoE) creation and coordination to ensure that the lead penetration tester can meet the engagement obligations

- 1 Project Lead / Principal Penetration Test Lead (with OSCP / OSWE Certification, **CJIS Certified**) – Will provide day-to-day coordination of the penetration test objectives and ensure that that ROE and scope are consistently met. Additionally, daily communications are handled by the lead to ensure that agency objectives are met, and any critical or high vulnerabilities are address in a timely manner
- 2 Senior Web Application Penetration Testers (with OSCP / CEH Certification, **CJIS Certified**) – Will provide web application and thick client application testing
- 1 Web Application Penetration Tester (with minimum CEH Certification, **CJIS Certified**) – Will handle static external web application
- 1 Network Penetration Testers (with minimum CEH Certification, **CJIS Certified**) – Will perform internal and external penetration testing

Emagined Security employees over a dozen penetration testers and can staff multiple engagements of this size simultaneously. This is a dedicated penetration test team and current members have been background checked by the State of Washington including CJIS certification and undergone Washington State Patrol fingerprint background checks.

At completion of the testing Emagined Security Senior Penetration Tester that is managing the project will coordinate the accumulation of findings in reports specific to each test and work with the Emagined Penetration Testing team to consolidate these identified findings into a report for SAO and Agency.



Work Plan (MR)

Emagined Security will initially assign a Senior Project Manager. This Senior Project Manager will then assign a lead Penetration Tester to assist with coordination of the technical details of this engagement. The Senior Project Manager will work with SAO to scope the appropriate tasks to be included within the scope of the engagement. This scoping will determine appropriate applications, networks, systems and services that should be in scope. Meetings will be scheduled between the SAO, State Agency and Emagined Security to review items requested to be in scope by Agency to determine the Security risk and value of the applications, systems and networks to ensure the engagement can be kept in the appropriate budged allotted by the State Agency for the Agency testing.

The Workplan will include specifics on escalation of identified vulnerabilities, how communications channels are defined and will provide comprehensive details of each application being tested. (Bullets details have been removed due to page limits)

- Attacker Persona
- Methods Allowed
- Access to Results
- Systems Allowed
- Monitoring
- Professional Manner
- Social Engineering

Once the scope has been refined and approved by the State Agency and the SAO. Emagined Security will work on creating a Rules of Engagement (RoE) Document that will detail out for the engagement the scope of the work to be performed including Applications to be tested, External and Internal Networks, SCADA systems, Mobile Applications and any other specific scoping items that will be tested. The RoE will additionally provide a high-level methodology of the testing to be performed, the tools to be utilized, dates and times of testing, the contacts for all individuals at SAO, Agency and Emagined Security involved with the testing.

Based on the needs of the Agency and SAO for the specific engagement, Emagined Security will either arrange travel to the location for testing or create a remote sensor that will enable Emagined Security the ability to access and test remotely. Emagined will additionally assign the appropriate resources to perform the specified tests. This testing will consist of Emagined Security penetration testers and will not be outsourced to non-authorized individuals. All Members of the Emagined Security Penetration Testing Team will be authorized to work in the United States, have completed CJIS training and background checks as requested my SAO. Most Members of the Emagined Security Penetration Testing team have additionally completed Washington State Background Checks and are held on file with the State of Washington.

After Completion of the Rules of Engagement and Signature, Testing will commence on the dates and times listed in the RoE. Testing will be scheduled with SAO and Agency to fit within the timing window and will start application and network testing. Emagined Security will follow methodology presented to SAO and Agency and will provide during the testing timeframes:

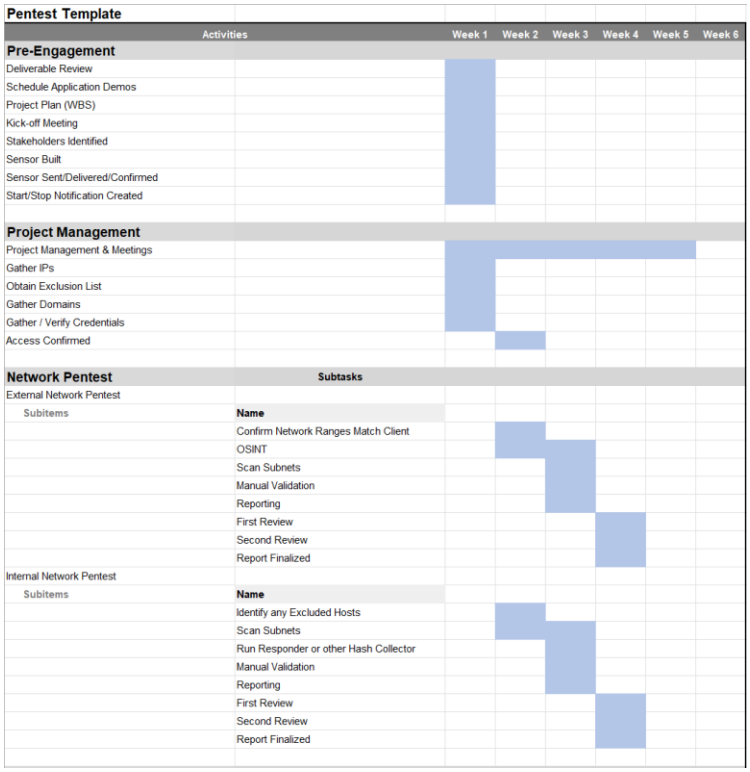
- Daily start and stop notices
- Daily quick check in meetings as necessary from the agency and SAO
- Daily status updates including any identified vulnerabilities broken down by the application or network and % complete of the application testing
- A final Status update email
- A final debrief with the customer at the completion of the testing

Project Schedule (MR)

While scoping the penetration testing, the Emagined Team will identify how many hours are expected to be utilized to perform all the testing and will create a Project Schedule. This schedule will be confirmed with the SAO and Agency to meet their deadlines and requirements. Emagined will work with SAO and Agency to determine what applications and networks can be tested during the period and will schedule them appropriately. Additionally, Emagined will work with SAO and Agency to identify the need for any additional time to handle issues or emergencies that may be identified during testing.

The project scheduled will then be defined initially by the State of Washington SAO office Rules of Engagement that will lay out the applications, dates and contacts of the organization to be tested. This workplan will expand to include the dates/times, contacts and communication to be provided during the penetration testing. Each test is independently scheduled in the number of man weeks to perform a test. As multiple penetration testers may be assigned to an engagement, these tasks may overlap in

calendar weeks. A sample schedule may look like the following. Detailed project charts can also be found in the *"Exhibit D - Qualifications-Emagined 16 Pages Final"*:



Pentest Template							
Activities		Week 1	Week 2	Week 3	Week 4	Week 5	Week 6
Pre-Engagement							
Deliverable Review							
Schedule Application Demos							
Project Plan (WBS)							
Kick-off Meeting							
Stakeholders Identified							
Sensor Built							
Sensor Sent/Delivered/Confirmed							
Start/Stop Notification Created							
Project Management							
Project Management & Meetings							
Gather IPs							
Obtain Exclusion List							
Gather Domains							
Gather / Verify Credentials							
Access Confirmed							
Network Pentest	**Subtasks**						
External Network Pentest							
Subitems	**Name**						
	Confirm Network Ranges Match Client						
	OSINT						
	Scan Subnets						
	Manual Validation						
	Reporting						
	First Review						
	Second Review						
	Report Finalized						
Internal Network Pentest							
Subitems	**Name**						
	Identify any Excluded Hosts						
	Scan Subnets						
	Run Responder or other Hash Collector						
	Manual Validation						
	Reporting						
	First Review						
	Second Review						
	Report Finalized						

Application Pentest	Subtasks
App 1	
Subitems	**Name**
	Identify apps (web, API, thick, etc.)
	Assign testers
	Confirm Demos have taken place
	Confirm Authentication, Authorization
	Identify Roles to be tested
	Confirm access to applications
	Browse/Spider App
	OWASP Top 10
	OWASP Testing Guide
	Manual testing/validation
	Reporting
	First Review
	Second Review
	Report Finalized
Social Engineering	**Subtasks**
Phishing / Vishing	
Subitems	**Name**
	Confirm the Scope of Phishing (L0-4)
	Create Mock-Ups & Deliver to Client
	Final Design Sign-off by Client
	Phishing Domain Acquired
	Phishing Server Configured
	Test email (allow listing etc) with client
	Targets identified (email addresses etc)
	Initiate Campaign (Launch)
	Close Campaign & Finalize Metric Collection
	Aggregate Metrics for Report
	Report Review 1 (internal)
	Report Review 2 (Internal)
	Final - Sent to Client
Reporting	
Daily Updates/Start Stop	
Aggregate & Consolidate Reports	
Final Report Sent	
Feedback from Client	
Report Updated	
Final Findings / Report Review with Stakeholders	

Deliverables (MR)

Emagined Security has worked with the SAO over previous engagements on a detailed report format that meets their needs. Emagined Security will work with the SAO to update any deliverables to an agreed upon format as necessary. As such, deliverables will be provided in a format approved by the SAO to ensure it includes all necessary information for SAO to feel the report is complete and concise. The report will be submitted to SAO initially for their review of details associated with testing and to ensure it meets their standards before it is sent to the Agency. The report will consist at a high level of the following:

- Executive Summary – Detailing out the engagement and any details to relay to the agency about the testing. This may also include any concerns or issues identified during the testing
- Engagement Objective – Detailing out the testing performed during the testing
- Identified Vulnerabilities charts and presentation information.
- Findings broken down by Application and network
- A final summary of testing
- Any appendices for configuration reporting or items identified as needed by the testing

A copy of a sample report has been provided as *"Exhibit D - Qualifications-Emagined ACME_Sample_Report_2023 Final"*