Cybersecurity Assessment Statement of Work

A. OBJECTIVE: The Contra Costa County Superior Court is requesting proposals from experienced and qualified organizations to provide a comprehensive cybersecurity vulnerability assessment of the Court's network. The assessment should include information security guidance that is aligned with industry standards, best practices and methodologies outlined in National Institute for Standards and Technology (NIST), Cyber Security Framework (CSF), HIPAA, ISO/IEC, etc. The evaluation should include an information security roadmap to be used to develop a plan for remediation of any items identified.

B. GOAL: The goal of the assessment is to identify and validate weaknesses in the Court's information security architecture and posture from both an internal and external vantage point.

C. SCOPE OF WORK: The following tasks outline the functional areas in which the service provider shall assess in this engagement.

   a. Penetration Testing: The scope of the Penetration testing should include the entire perimeter and any critical systems that may impact the security of the systems. This includes both the external perimeter (public-facing attack surfaces) and the internal perimeter (LAN to LAN attack surfaces).

   b. Perimeter Testing: The Service provider shall test Court's network perimeter both externally and internally. In addition, the test must include critical systems that could affect the security including security systems (e.g., firewalls, authentication servers, etc.) or any assets utilized by privileged users to support and manage the systems. Activities must include, but may not be limited to:

      i. Perform an in-depth cybersecurity vulnerability assessment and penetration testing of Court IT infrastructure of:

         1. Internal network – all internal systems including routers, switches, physical and virtual servers, data storage infrastructure, and public computers and other connected IT devices: including all Demilitarized (DMZ) systems to include flow of controls from external and internal systems.

         2. External network - all external public-facing systems including firewalls, FTP, web servers, and web service interface points.

      ii. Enumerate systems on the network and validate them against known systems. Identify any unknown or unexpected systems.

      iii. Scan network systems and mainframe for potential vulnerabilities. Court will provide the network ranges and any network/host exemptions to these scans.

      iv. Identify, analyze, and confirm vulnerabilities. It is expected that qualified service provider personnel will know how to look deeper into potential vulnerabilities for other security holes, misconfigurations, and other problems to follow the vulnerability to its end. It is expected that the service provider will share method and process (i.e., e-mail's screen

shots, files, etc.) of successful penetration in addition to a list of open ports, missing patches, or possible vulnerabilities.

v. The security service provider will conduct security risk assessment scans on 5 mission-critical applications. All vulnerabilities reported as Critical/High shall be detailed in the 'Findings' section of the final deliverable. A complete list of vulnerabilities shall be provided in a separate appendix. Each vulnerability or risk identified shall be categorized as a Critical/High, Medium, or Low.

vi. The service provider shall attempt to capture user credentials through the collection of the following vectors:
    1. Windows password hashes in-memory
    2. Keystroke logging
    3. Password and hash sniffing
    4. Collecting saved login credentials

vii. User Privilege Escalation: Throughout the assessment, the service provider shall attempt to complete user privilege escalations in order to further compromise, or demonstrate the effectiveness of, the security of established controls within Court's environment. This testing will assist in determining if access control systems are effectively enforcing user access and permission levels are configured correctly based on job function.

viii. Segmentation Testing: The service provider shall test the segmentation controls of all segregated network segments from a sample of completely isolated/segmented networks (ensuring that each type of segmentation point is represented, such as firewalls, VLAN on switch, etc.).

ix. Wireless Scanning (both private and guest): The service provider shall identify rogue wireless devices and additional security architecture weaknesses related to the wireless networks.

x. Applications

    1. Provide authenticated application vulnerability scanning and penetration testing (At a minimum, the test should include OWASP Top 10). The security service provider will conduct security risk assessment scans on 5 external facing applications.

    2. Identify application security vulnerabilities and perform active exploit through identified vulnerabilities (Note: Exploit should stop at the point of proof of compromise but not causing any business interruption).

xi. Database Assessment: We have approximately 50 database servers. In the database assessment phase, the service provider shall take the following actions:
    1. Assess the databases to look for common vulnerabilities such as buffer overflows, default accounts, or default permissions on

database objects such as tables, views, and stored procedures.
2. Look for erroneous configurations that may lead to information leaks, theft of data, or even intrusion and denial of service attacks.
3. Examine several key functional areas that may include but not be limited to:
    a. Authentication and Authorization to Control Database Access
    b. Password Complexity Verification
    c. Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.
    d. Server Security
    e. Database Connections
    f. Table Access Control
    g. Encryption Usage
    h. Certificate Application

xii. Brute Force Attack: The service provider shall conduct a brute force attack to check for weak passwords. The objective of this test is to confirm whether passwords are meeting security best practices.

xiii. Social Engineering (Phone and E-mail): During the Social Engineering phase of the assessment, the service provider shall attempt to impersonate and persuade Court/EMS employees via telephone and/or e-mail to disclose proprietary information. This information may allow the service provider to access sensitive information and/or exploit the integrity and/or availability of data. The sophisticated methods that may be utilized are, but not limited to, as follows:

1. Phishing/spear phishing Attacks – Sending an e-mail to a user falsely claiming to be an established legitimate organization in an attempt to scam the user into surrendering company sensitive/ information. The overall objective here is to measure end-user response to phishing, spear phishing, spam, and other email threats.

2. Employee Impersonation – Calling employees and attempt to convince them to release sensitive information (e.g., passwords of systems, unpublished e-mail addresses, names of other employees, names, and virtual locations of systems).

3. Pretexting – This method is the act of creating and using an invented scenario to persuade a targeted victim to release information or perform an action and is typically done over the telephone. It is more than a simple lie as it most often involves some prior research or set up and the use of pieces of known information (e.g., for impersonation: date of birth, Social Security Number, last bill amount or other specific company information to establish legitimacy in the mind of the target).

Cybersecurity Assessment Statement of Work

D. REQUIRED DELIVERABLES

a. Executive summary: The executive summary should include high level overview of the assessment including the following:

   i. Overall assessment results.
   ii. Overall risk ranking and key areas of risk.
   iii. Current maturity level score card against NIST cybersecurity framework.
   iv. Strategic recommendations and key areas of focus for remediation.

b. Detailed report: The detailed report should include detail of the assessment including the following:
   i. Assessment methodology.
   ii. Detailed assessment results in a sortable spreadsheet, risk ranking and actionable recommendations for all areas within the assessment scope.
   iii. Detailed score card of current maturity level for each NIST subcategory

c. Road map: This should include both tactical and strategic recommendations in a risk-based approach with consideration of business environment, technology, people, and process.

   i. Tactical recommendations: This should identify issues that are tactical in nature, simple to implement, and will have a positive impact on overall NIST alignment. Recommendations should be made and presented in a risk-ranked format along with technical, resource and process requirements.

   ii. Strategic Recommendations: This should identify issues that are strategic in nature, complex to implement, and require management decisions to fund, but will have a significant impact on the overall architecture program. Recommendations should be made and presented in a risk-ranked format along with technical, resource and process requirements.

   iii. Appropriate milestones and key performance indicators to enhance Court's information security posture and address key risk findings.

   iv. Identification of security projects based on individual or combined recommendations with detailed activities and action plans.

   v. An assessment of how the implementation of each project would remediate risk and position Court with respect to industry best practices.

d. Prioritized project plan: The project plan is developed to support the road map. At a minimum, the project plan should include the following elements:
   i. Project description
   ii. Priority
   iii. Risk rank
   iv. Supported road map item #
   v. Recommended solution
   vi. Level of complexity to implement.
   vii. Resource requirement

e. Presentation deliverable: The service provider should prepare and deliver an executive-level presentation of the assessment. It is important to note that once Cybersecurity vulnerability assessment testing is completed, the Service provider must remove all agents, backdoors, any software used for the Cybersecurity risk assessment project, thus removing any trace of existence in the Court's IT infrastructure.

E. QUALIFICATIONS

Service providers who have completed at least two comprehensive cybersecurity vulnerability assessments in last five years for organizations of size comparable to the Court as on date of proposal submission will be preferred.

F. PROPOSAL FORMAT

To be considered, service provider must submit a COMPLETE proposal in response to this procurement using the format specified. There should be no attachments, enclosures, or exhibits other than those required in the procurement or considered by the service provider to be essential to a complete understanding of the proposal. Each section of the proposal should be clearly identified with appropriate headings.

The contents of the proposal should be as follows:

i. Business Organization and History

State the full name, address, and phone and facsimile number of your organization and, if applicable, the branch office or other subordinate element that will perform, or assist in performing, the work hereunder. Indicate whether it operates as an individual, partnership, or corporation; if as a corporation, include the state in which it is incorporated. If appropriate, the proposal must state whether the organization is licensed to operate in the State of California.

ii. Statement of the Problem

State in succinct terms your understanding of the problem(s) presented by this procurement.

iii. Technical Work Plans

a. Narrative — Include a narrative summary description of the proposed effort and of the services(s) that will be delivered. Also indicate how your organization is best suited to provide the requested service.
b. Provide a detailed outline and timelines for accomplishing the work. Include the challenges you expect during execution and how you will overcome them.

iv. Experience:

Describe the prior experience of your organization in last five years, which you consider relevant to the successful accomplishment of the project defined in this procurement. Include sufficient detail to demonstrate the relevance of such an experience. Proposals submitted should include descriptions of qualifying experience to include project descriptions, costs,

and starting and completion dates of projects successfully completed; also include the name, address, and phone number of the responsible officials of two client organization for whom prior comprehensive cybersecurity vulnerability assessments have been completed. Court may contact them for reference check. The Court may evaluate the service provider's prior performance, and prior performance information may be a factor in the award decision.

v. Staffing:

Please provide names, qualification and experience of staff who would work for providing the requested service.

vi. Fees and Payment Schedule:

Provide a fixed total fee for the services requested and a payment schedule. The fixed total fee should include all business-related travel expenses. Court will not make advance payments. Payments will be made against clearly identified deliverables.