CONTRACT RESULTING FROM REQUEST FOR PROPOSAL NUMBER 10090089-24-S, PAYMENT CARD INDUSTRY (PCI) COMPLIANT CLOUD HOSTING SERVICES

This Contract (Contract) is entered into by and between the City of San Diego, a municipal corporation (City), and the successful proposer to Request for Proposal (RFP) # 10090089-24-S, PAYMENT CARD INDUSTRY (PCI) COMPLIANT CLOUD HOSTING SERVICES (Contractor).

RECITALS

On or about 4/15/2024, City issued an RFP to prospective proposers on services to be provided to the City. The RFP and any addenda and exhibits thereto are collectively referred to as the "RFP." The RFP is attached hereto as Exhibit A.

City has determined that Contractor has the expertise, experience, and personnel necessary to provide the services.

City wishes to retain Contractor to provide security services as further described in the Scope of Work, attached hereto as Exhibit B. (Services).

For good and valuable consideration, the sufficiency of which is acknowledged, City and Contractor agree as follows:

ARTICLE I
CONTRACTOR SERVICES

1.1 Scope of Work. Contractor shall provide the Services to City as described in Exhibit B which is incorporated herein by reference. Contractor will submit all required forms and information described in Exhibit A to the Purchasing Agent before providing Services.

1.2 General Contract Terms and Provisions. This Contract incorporates by reference the General Contract Terms and Provisions, attached hereto as Exhibit C.

1.3 Contract Administrator. The Department of Information Technology (Department) is the Contract Administrator for this Agreement. Contractor shall provide the Services under the direction of a designated representative of the Department as follows:

Ian Brazill, Program Manager
1200 Third Ave., San Diego, CA 92101
619-533-4812
ibrazill@sandiego.gov

ARTICLE II
DURATION OF CONTRACT

2.1 Term. This Contract shall be for a period of three (3) years beginning on the Effective Date. City may, in its sole discretion, extend this Contract for two (2) additional one- year period(s) beginning on the Effective Date. The term of this Contract shall not exceed five years unless approved by the City Council by ordinance.

2.2 Effective Date. This Contract shall be effective on December 13, 2024 or the date it is executed by the last Party to sign the Contract, and approved by the City Attorney in accordance with San Diego Charter Section 40, whichever is later.

ARTICLE III
COMPENSATION

3.1 Amount of Compensation. City shall pay Contractor for performance of all Services rendered in accordance with this Contract as outlined within the Pricing Schedule. Total expenditures under this Contract will not exceed $3,000,000 without approval by City Council via a resolution or ordinance.

ARTICLE IV
WAGE REQUIREMENTS

4.1 Reserved.

ARTICLE V
CONTRACT DOCUMENTS

5.1 Contract Documents. The following documents comprise the Contract between the City and Contractor: this Contract and all exhibits thereto, the RFP; the Notice to Proceed; and the City's written acceptance of exceptions or clarifications to the RFP, if any.

5.2 Contract Interpretation. The Contract Documents completely describe the Services to be provided. Contractor will provide any Services that may reasonably be inferred from the Contract Documents or from prevailing custom or trade usage as being required to produce the intended result whether or not specifically called for or identified in the Contract Documents. Words or phrases which have a well-known technical or construction industry or trade meaning and are used to describe Services will be interpreted in accordance with that meaning unless a definition has been provided in the Contract Documents.

5.3 Precedence. In resolving conflicts resulting from errors or discrepancies in any of the Contract Documents, the Parties will use the order of precedence as set forth below. The 1st document has the highest priority. Inconsistent provisions in the Contract Documents that address the same subject, are consistent, and have different degrees of specificity, are not in conflict and the more specific language will control. The order of precedence from highest to lowest is as follows:

1st Any properly executed written amendment to the Contract

2nd The Contract

3rd The RFP and the City's written acceptance of any exceptions or clarifications to the RFP, if any

4th Contractor's Pricing

5.4 Counterparts. This Contract may be executed in counterparts which, when taken together, shall constitute a single signed original as though all Parties had executed the same page.

5.5 Public Agencies. Other public agencies, as defined by California Government Code section 6500, may choose to use the terms of this Contract, subject to Contractor's acceptance. The City is not liable or responsible for any obligations related to a subsequent Contract between Contractor and another public agency.

IN WITNESS WHEREOF, this Contract is executed by City and Contractor acting by and through their authorized officers.

CONTRACTOR

Armor Defense Inc
Proposer

7700 Windrose Ave, #G300
Street Address

Plano, TX 75024
City

8772623473
Telephone No.

legal@armor.com
E-Mail

BY:
Signature of
Proposer's Authorized
Representative

Anubhav Kela
Print Name

CFO
Title

10/28/2024
Date

CITY OF SAN DIEGO
A Municipal Corporation

BY:
Claudia Abarca
Print Name:
Director, Purchasing & Contracting Department

10/29/2024
Date Signed

Approved as to form this 29 day of October, 20 24.
MARA W. ELLIOTT, City Attorney

BY:
Deputy City Attorney

EXHIBIT A
PROPOSAL SUBMISSION AND REQUIREMENTS

A. PROPOSAL SUBMISSION

1. Timely Proposal Submittal. Proposals must be submitted as described herein to the Purchasing & Contracting Department (P&C).

1.1 Reserved.

1.2 Paper Proposals. The City will accept paper proposals in lieu of eProposals. Paper proposals must be submitted in a sealed envelope to the Purchasing & Contracting Department (P&C) located at 1200 Third Avenue, Suite 200, San Diego, CA 92101. The Solicitation Number and Closing Date must be referenced in the lower left-hand corner of the outside of the envelope. Faxed proposals will not be accepted.

1.3 Proposal Due Date. Proposals must be submitted prior to the Closing Date indicated on the eBidding System. E-mailed and/or faxed proposals will not be accepted.

1.4 Pre-Proposal Conference. No pre-proposal conference will be held for RFP.

1.4.1 Reserved.

1.5 Questions and Comments. Written questions and comments must be submitted electronically via the eBidding System no later than the date specified on the eBidding System. Only written communications relative to the procurement shall be considered. The City's eBidding System is the only acceptable method for submission of questions. All questions will be answered in writing. The City will distribute questions and answers without identification of the inquirer(s) to all proposers who are on record as having received this RFP, via its eBidding System. No oral communications can be relied upon for this RFP. Addenda will be issued addressing questions or comments that are determined by the City to cause a change to any part of this RFP.

1.6 Contact with City Staff. Unless otherwise authorized herein, proposers who are considering submitting a proposal in response to this RFP, or who submit a proposal in response to this RFP, are prohibited from communicating with City staff about this RFP from the date this RFP is issued until a contract is awarded.

2. Proposal Format and Organization. Unless electronically submitted, all proposals should be securely bound and must include the following completed and executed forms and information presented in the manner indicated below:

Tab A - Submission of Information and Forms.

2.1 Completed and signed Contract Signature Page. If any addenda are issued, the latest Addendum Contract Signature Page is required.

2.2 Exceptions requested by proposer, if any. Proposers must list or reference each specific exception they are requesting to the Scope of Work, the Contract, or the Exhibits thereto. For each requested exception, proposers must provide proposed alternative or amended language in

their initial proposal submittal for potential consideration. The proposer must also present written factual or legal justification for any exception requested to the Scope of Work, the Contract, or the Exhibits thereto.

It is not acceptable for proposers to take exception to terms or conditions in general, with a request to later discuss or negotiate specific terms within the RFP / Contract. Nor is it acceptable to refer to other contracts for alternative language. The City will not consider exceptions addressed elsewhere in the proposal, nor will the City consider exceptions for which no specific alternative or amended language is provided.

Any exceptions to the Contract that have not been accepted by the City in writing are deemed rejected. The City, in its sole discretion, may accept some or all of proposer's exceptions, reject proposer's exceptions and deem the proposal nonresponsive, or award the Contract without proposer's proposed exceptions.

2.3 The Contractor Standards Pledge of Compliance Form.

2.4 Equal Opportunity Contracting forms including the Work Force Report and Contractors Certification of Pending Actions.

2.5 Exhibit E (IT City Standards and Technical Alignment Questionnaire).

2.6 Exhibit F (Functional and General Requirements).

2.7 Exhibit G (Interrogatories).

2.8 Exhibit H (Screenshots).

2.9 Exhibit J (PCI DSS).

3.0 Additional Information as required in Exhibit B.

Tab B - Executive Summary and Responses to Specifications.

2.10 A title page.

2.11 A table of contents.

2.12 An executive summary, limited to one typewritten page, that provides a high-level description of the proposer's ability to meet the requirements of the RFP and the reasons the proposer believes itself to be best qualified to provide the identified services.

2.13 Proposer's response to the RFP.

2.14 An additional, redacted version of Proposer's response to the RFP containing all requested redactions of confidential, proprietary or other information which proposer alleges to be exempt from disclosure under the California Public Records Act, including the legal basis for such exemption, as fully set forth in Section 9. Public Records below.

Tab C - Cost/Price Proposal (Exhibit D. Pricing Schedule). Proposers shall submit a cost proposal in the form and format described herein. Failure to provide cost(s) in the form and format requested may result in proposal being declared non-responsive and rejected.

3. Proposal Review. Proposers are responsible for carefully examining the RFP, the Specifications, this Contract, and all documents incorporated into the Contract by reference before submitting a proposal. If selected for award of contract, proposer shall be bound by same unless the City has accepted proposer's exceptions, if any, in writing.

4. Addenda. The City may issue addenda to this RFP as necessary. All addenda are incorporated into the Contract. The proposer is responsible for determining whether addenda were issued prior to a proposal submission. Failure to respond to or properly address addenda may result in rejection of a proposal.

5. Quantities. The estimated quantities provided by the City are not guaranteed. These quantities are listed for informational purposes only. Quantities vary depending on the demands of the City. Any variations from the estimated quantities shall not entitle the proposer to an adjustment in the unit price or any additional compensation.

6. Quality. Unless otherwise required, all goods furnished shall be new and the best of their kind.

6.1 Items Offered. Proposer shall state the applicable trade name, brand, catalog, manufacturer, and/or product number of the required good, if any, in the proposal.

6.2 Brand Names. Any reference to a specific brand name in a solicitation is illustrative only and describes a component best meeting the specific operational, design, performance, maintenance, quality, or reliability standards and requirements of the City. Proposer may offer an equivalent or equal in response to a brand name referenced (Proposed Equivalent). The City may consider the Proposed Equivalent after it is subjected to testing and evaluation which must be completed prior to the award of contract. If the proposer offers an item of a manufacturer or vendor other than that specified, the proposer must identify the maker, brand, quality, manufacturer number, product number, catalog number, or other trade designation. The City has complete discretion in determining if a Proposed Equivalent will satisfy its requirements. It is the proposer's responsibility to provide, at their expense, any product information, test data, or other information or documents the City requests to properly evaluate or demonstrate the acceptability of the Proposed Equivalent, including independent testing, evaluation at qualified test facilities, or destructive testing.

7. Modifications, Withdrawals, or Mistakes. Proposer is responsible for verifying all prices and extensions before submitting a proposal.

7.1 Modification or Withdrawal of Proposal Before Proposal Opening. Prior to the Closing Date, the proposer or proposer's authorized representative may modify or withdraw the proposal by providing written notice of the proposal modification or withdrawal to the City Contact via the eBidding System. E-mail or telephonic withdrawals or modifications are not permissible.

7.2 Proposal Modification or Withdrawal of Proposal After Proposal Opening. Any proposer who seeks to modify or withdraw a proposal because of the proposer's inadvertent computational error affecting the proposal price shall notify the City Contact

identified on the eBidding System no later than three working days following the Closing Date. The proposer shall provide worksheets and such other information as may be required by the City to substantiate the claim of inadvertent error. Failure to do so may bar relief and allow the City recourse from the bid surety. The burden is upon the proposer to prove the inadvertent error. If, as a result of a proposal modification, the proposer is no longer the apparent successful proposer, the City will award to the newly established apparent successful proposer. The City's decision is final.

8. Incurred Expenses. The City is not responsible for any expenses incurred by proposers in participating in this solicitation process.

9. Public Records. By submitting a proposal, the proposer acknowledges that any information submitted in response to this RFP is a public record subject to disclosure unless the City determines that a specific exemption in the California Public Records Act (CPRA) applies. If the proposer submits information clearly marked confidential or proprietary, the City may protect such information and treat it with confidentiality to the extent permitted by law. However, it will be the responsibility of the proposer to provide to the City the specific legal grounds on which the City can rely in withholding information requested under the CPRA should the City choose to withhold such information. General references to sections of the CPRA will not suffice. Rather, the proposer must provide a specific and detailed legal basis, including applicable case law, that clearly establishes the requested information is exempt from the disclosure under the CPRA. If the proposer does not provide a specific and detailed legal basis for requesting the City to withhold proposer's confidential or proprietary information at the time of proposal submittal, City will release the information as required by the CPRA and proposer will hold the City, its elected officials, officers, and employees harmless for release of this information. It will be the proposer's obligation to defend, at proposer's expense, any legal actions or challenges seeking to obtain from the City any information requested under the CPRA withheld by the City at the proposer's request. Furthermore, the proposer shall indemnify and hold harmless the City, its elected officials, officers, and employees from and against any claim or liability, and defend any action brought against the City, resulting from the City's refusal to release information requested under the CPRA which was withheld at proposer's request. Nothing in the Contract resulting from this proposal creates any obligation on the part of the City to notify the proposer or obtain the proposer's approval or consent before releasing information subject to disclosure under the CPRA. Additionally, if the proposer considers any part of its proposal confidential, proprietary, trade secret, or otherwise exempt from disclosure under the CPRA, in addition to the requirements above, proposer must also submit a clearly marked redacted version of the proposal at the time of submittal.

10. Right to Audit. The City Auditor may access proposer's records as described in San Diego Charter section 39.2 to confirm contract compliance.

B. PRICING

1. Fixed Price. All prices shall be firm, fixed, fully burdened, FOB destination, and include any applicable delivery or freight charges, and any other costs required to provide the requirements as specified in this RFP. The lowest total estimated contract price of all the proposals that meet the requirements of this RFP will receive the maximum assigned points to this category as set forth in this RFP. The other price schedules will be scored based on how much higher their total estimated contract prices compare with the lowest:

$$\left(1 - \frac{(\text{contract price} - \text{lowest price})}{\text{lowest price}}\right) \times \text{maximum points} = \text{points received}$$

For example, if the lowest total estimated contract price of all proposals is $100, that proposal would receive the maximum allowable points for the price category. If the total estimated contract price of another proposal is $105 and the maximum allowable points is 60 points, then that proposal would receive (1 – ((105 – 100) / 100) x 60 = 57 points, or 95% of the maximum points. The lowest score a proposal can receive for this category is zero points (the score cannot be a negative number). The City will perform this calculation for each Proposal.

2. Taxes and Fees. Taxes and applicable local, state, and federal regulatory fees should not be included in the price proposal. Applicable taxes and regulatory fees will be added to the net amount invoiced. The City is liable for state, city, and county sales taxes but is exempt from Federal Excise Tax and will furnish exemption certificates upon request. All or any portion of the City sales tax returned to the City will be considered in the evaluation of proposals.

3. Escalation. An escalation factor is not allowed unless called for in this RFP. If escalation is allowed, proposer must notify the City in writing in the event of a decline in market price(s) below the proposal price. At that time, the City will make an adjustment in the Contract or may elect to re-solicit.

4. Unit Price. Unless the proposer clearly indicates that the price is based on consideration of being awarded the entire lot and that an adjustment to the price was made based on receiving the entire proposal, any difference between the unit price correctly extended and the total price shown for all items shall be offered shall be resolved in favor of the unit price.

C. EVALUATION OF PROPOSALS

1. Award. The City shall evaluate each responsive proposal to determine which proposal offers the City the best value consistent with the evaluation criteria set forth herein. The proposer offering the lowest overall price will not necessarily be awarded a contract.

2. Sustainable Materials. Consistent with Council Policy 100-14, the City encourages use of readily recyclable submittal materials that contain post-consumer recycled content.

3. Evaluation Process.

3.1 Process for Award. A City-designated evaluation committee (Evaluation Committee) will evaluate and score all responsive proposals. The Evaluation Committee may require proposer to provide additional written or oral information to clarify responses. Upon completion of the evaluation process, the Evaluation Committee will recommend to the Purchasing Agent that award be made to the proposer with the highest scoring proposal.

3.2 Reserved.

3.3 Mandatory Interview/Oral Presentation. The City will require proposers to interview and/or make an oral presentation if one or more proposals score within thirteen (13) points or less of the proposal with the highest score. Only the proposer with the highest

scoring proposal and those proposers scoring within thirteen (13) points or less of the highest scoring proposal will be asked to interview and/or make an oral presentation. Interviews and/or oral presentations will be made to the Evaluation Committee in order to clarify the proposals and to answer any questions. The interviews and/or oral presentations will be scored as part of the selection process. Additionally, the Evaluation Committee may require proposer's key personnel to interview. Interviews may be by telephone and/or in person. Multiple interviews may be required. Proposers are required to complete their oral presentation and/or interviews within seven (7) workdays after the City's request. Proposers should be prepared to discuss and substantiate any of the areas of the proposal submitted, as well as proposer's qualifications to furnish the subject goods and services. Proposer is responsible for any costs incurred for the oral presentation and interview of the key personnel.

3.4 Discussions/Negotiations. The City has the right to accept the proposal that serves the best interest of the City, as submitted, without discussion or negotiation. Contractors should, therefore, not rely on having a chance to discuss, negotiate, and adjust their proposals. The City may negotiate the terms of a contract with the winning proposer based on the RFP and the proposer's proposal, or award the contract without further negotiation.

3.5 Inspection. The City reserves the right to inspect the proposer's equipment and facilities to determine if the proposer is capable of fulfilling this Contract. Inspection will include, but not limited to, survey of proposer's physical assets and financial capability. Proposer, by signing the proposal agrees to the City's right of access to physical assets and financial records for the sole purpose of determining proposer's capability to perform the Contract. Should the City conduct this inspection, the City reserves the right to disqualify a proposer who does not, in the City's judgment, exhibit the sufficient physical and financial resources to perform this Contract.

3.6 Evaluation Criteria. The following elements represent the evaluation criteria that will be considered during the evaluation process:

	MAXIMUM EVALUATION POINTS
A. Responsiveness to the RFP.	**20**
1. Conformity of the proposed product to the City functional requirements and applicable IT City Standards	
2. Acceptance of City standard documents, including Terms and Conditions, Statement of Work, and other provisions	
3. Technical Aspects	
4. Risk Profile (e.g. exception requests)	
B. Experience and Implementation Plan.	**20**
1. Proposer's previous experience in providing and implementing a PCI-compliant cloud hosting environment solution	
2. Proposer's references in providing and implementing a PCI-compliant cloud hosting environment solution	
3. Project Implementation Plan – thoroughness, clarity, brevity, and minimal disruption of City business	

	MAXIMUM EVALUATION POINTS
C. Firm's Capability/Qualifications, Experience and Past Performance. 1. Demonstrated the Proposers and any listed subcontractor's responsibility, experience, skill, and qualifications to manage and perform the Scope of Services 2. Capacity/Capability to meet The City of San Diego needs in a timely manner 3. Provided Past/Prior Performance i.e. experience in industrial/commercial settings and services performed for contracts of similar scope and size 4. Other pertinent experience	**25**
D. Price.	**15**
E. Mandatory Demonstration/Presentation. 1. Describe in sufficient detail the ability to provide the functions described in the RFP 2. Software 3. Support Model 4. Demonstrate in real time that your program can meet the requirements of the RFP 5. Thoroughness and Clarity of Presentation	**20**
SUB TOTAL MAXIMUM EVALUATION POINTS:	**100**
F. Participation by Small Local Business Enterprise (SLBE) or Emerging Local Business Enterprise (ELBE) Firms*	**12**
FINAL MAXIMUM EVALUATION POINTS INCLUDING SLBE/ELBE:	**112**

*The City shall apply a maximum of an additional 12 percentage points to the proposer's final score for SLBE OR ELBE participation. Refer to Equal Opportunity Contracting Form, Section V.

D. ANNOUNCEMENT OF AWARD

1. Award of Contract. The City will inform all proposers of its intent to award a Contract in writing.

2. Obtaining Proposal Results. No solicitation results can be obtained until the City announces the proposal or proposals best meeting the City's requirements. Proposal results may be obtained by: (1) e-mailing a request to the City Contact identified on the eBidding System or (2) visiting the P&C eBidding System to review the proposal results. To ensure an accurate response, requests should reference the Solicitation Number. Proposal results will not be released over the phone.

3. Multiple Awards. City may award more than one contract by awarding separate items or groups of items to various proposers. Awards will be made for items, or combinations of items, which result in the lowest aggregate price and/or best meet the City's requirements. The additional administrative costs associated with awarding more than one Contract will be considered in the determination.

E. PROTESTS. The City's protest procedures are codified in Chapter 2, Article 2, Division 30 of the San Diego Municipal Code (SDMC). These procedures provide unsuccessful proposers with the opportunity to challenge the City's determination on legal and factual grounds. The City will not consider or otherwise act upon an untimely protest.

F. SUBMITTALS REQUIRED UPON NOTICE TO PROCEED. The successful proposer is required to submit the following documents to P&C **within ten (10) business days** from the date on the Notice to Proceed letter:

1. Insurance Documents. Evidence of all required insurance, including all required endorsements, as specified in Article VII of the General Contract Terms and Provisions.

2. Taxpayer Identification Number. Internal Revenue Service (IRS) regulations require the City to have the correct name, address, and Taxpayer Identification Number (TIN) or Social Security Number (SSN) on file for businesses or persons who provide goods or services to the City. This information is necessary to complete Form 1099 at the end of each tax year. To comply with IRS regulations, the City requires each Contractor to provide a Form W-9 prior to the award of a Contract.

3. Business Tax Certificate. Unless the City Treasurer determines a business is exempt, all businesses that contract with the City must have a current business tax certificate.

4. Reserved.

5. Payment Card Industry Data Security Documents. Evidence of all required documents, as described in Exhibit B.

6. Sensitive Information Authorization Acknowledgement Form. Administrative Regulation 90.64. Contractor acknowledges and shall comply with the requirements in City of San Diego Administrative Regulation 90.64 PROTECTION OF SENSITIVE INFORMATION AND DATA to ensure the confidentiality and protection of sensitive information and data against unauthorized use. Contractor shall sign the City of San Diego **"Sensitive Information Authorization Acknowledgement Form- City Contractors/Vendors"** which includes a Policy Summary (pertinent excerpts from City Administrative Regulation 90.64). A copy of Administrative Regulation 90.64 is attached as Exhibit I to this Contract and is incorporated herein by reference.

The City may find the proposer to be non-responsive and award the Contract to the next highest scoring responsible and responsive proposer if the apparent successful proposer fails to timely provide the required information or documents.

EXHIBIT B
SCOPE OF WORK

A. OVERVIEW. The City of San Diego (the "City") is the second largest incorporated city in the State of California, and the eighth largest City in the United States. The City occupies 325 square miles of land and is located in the southwest corner of the United States. The City has over 1.4 million residents, is comprised of nine council districts, and has a 'Strong Mayor' form of government. The City has approximately 12,777 positions budgeted in Fiscal Year 2023. These positions are disbursed across almost seventy (70) distinct business areas comprised of departments, agencies, elected official offices, boards, and commissions. Most of these positions are in business areas that are under the responsibility of the Mayor and managed by the Executive Management Team. The remainder are located in other business areas that are headed up by other elected officials or City Agencies. The City operates on a July through June fiscal year.

The City of San Diego's Department of Information Technology has used the PCI-compliant services of Armor Defense, Inc. for approximately six (6) years. During that time, the environment has been integrated with numerous City applications, some of which have been hosted directly in the environment, whereas other SaaS solutions have integrated into standalone "redirect" applications which also exist within the environment. Currently, the City is drastically reducing the scope of applications which will remain within this cloud-hosted environment due to a reconfiguration of how City applications utilize the hosting provider to achieve PCI compliance. In its current state, the environment hosts 13 Virtual Machines in total, consisting of seven (7) Linux servers and six (6) Windows servers. Throughout 2024 there will be an ongoing evaluation of the proper size of the environment as several migration efforts occur.

B. OBJECTIVES. The goal of this Request for Proposal ("RFP") is to identify a qualified provider to ensure stringent security, availability, and compliance. It is the intention of the City that this RFP will result in a contract for a remote, secure, PCI-compliant cloud hosting environment that aligns with the latest PCI DSS 4.0 standards.

C. SPECIFICATIONS. The City has provided both the IT City Standards and Technical Alignment Questionnaire (Exhibit E) & Functional and General Requirements (Exhibit F) matrices required to be completed by proposers.

1. IT City Standards and Technical Alignment Questionnaire (Exhibit E). Proposers are required to do the following:

    a. Indicate whether their Solution is "Fully Compliant", "Partially Compliant", "Not Compliant", or "NA" for each line item.

    b. Provide a complete explanation of how, specifically, the solution does (or does not) comply. Please describe, in detail, how solution does (or does not) comply.

    c. If not fully compliant, provide proposed workarounds, planned updates (with timelines), or alternatives, as available (and associated costs, as applicable). For non-applicability of this standard, please provide explanation / justification.

d. If there are any additional costs associated w/ proposed workarounds or alternatives, they must be explicitly provided herein.

e. Go to the "Technical Alignment" tab and answer each question.

2. Functional and General Requirements (Exhibit F). Proposers are required to indicate the following:

    a. Indicate whether their Solution is "Fully Compliant", "Partially Compliant", or "Not Compliant" for each line item.

    b. Provide a complete explanation of how, specifically, the solution does (or does not) comply. Please describe, in detail, how solution does (or does not) comply.

    c. If not fully compliant, provide proposed workarounds, planned updates (with timelines), or alternatives, as available (and associated costs, as applicable).

    d. If there are any additional costs associated w/ proposed workarounds or alternatives, they must be explicitly provided herein.

    If the Proposer fails to provide an accompanying elaboration for the "Partially Compliant" status, the City shall consider the requirement to be "Not Compliant".

    All requirements identified with a "Not Compliant" response shall be assumed to mean that the Proposer cannot or will not be able to meet this requirement without further customization or development of their product.

    Any "Not Compliant" responses or responses considered not compliant for failure to provide accompanying elaboration for requirements specifically designated as "Mandatory" may be declared non-responsive and rejected.

D. FUNCTIONAL REQUIREMENTS. The selected hosting provider will be responsible for the following along with any additional requirements as outlined in Exhibit F. Functional and General Requirements matrix:

1. Secure Cloud Environment: Creating and maintaining a PCI DSS 4.0-compliant cloud hosting environment.

2. Four 9's (99.99%) Uptime: Ensuring a minimum of 99.99% uptime for the hosting environment.

3. Comprehensive Security Measures: Implementing encryption, multi-factor authentication, firewalls, intrusion detection, and ongoing vulnerability assessments.

4. Continuous Compliance Oversight: Monitoring and reporting on PCI DSS compliance status, including the transition to version 4.0.

5. Incident Response and Recovery: Providing 24/7 monitoring and rapid response to security incidents, with well-defined incident response procedures.

6. Backup and Recovery Services: Establishing regular backup procedures and efficient data recovery protocols to minimize data loss.

7. Load Balancers for High Availability: Implementing load balancers to ensure continuous service availability, particularly during patching windows, to avoid service downtime.

8. File Integrity Monitoring: Implementing file integrity monitoring to detect unauthorized changes to critical system files.

9. Endpoint Detection and Response: Implementing endpoint detection and response mechanisms, including antivirus, behavioral anomaly detection, and containment.

10. Host-based IDS and IPS: Implementing host-based intrusion detection and prevention systems to monitor and block malicious activities.

11. Malware Protection: Deploying malware protection mechanisms to safeguard against malicious software.

12. Vulnerability Scanning and Remediation: Conducting regular vulnerability scans and performing remediation without patching window downtime, using load balancers.

13. IPRM (Internet Protocol Reputation Management) Services: Managing and monitoring Internet Protocol reputations to mitigate potential threats.

14. Web Application Firewall (WAF) Services: Deploying and managing a WAF to protect against web-based attacks.

15. Log Management and Retention: Implementing a robust log management system with retention policies for compliance and security analysis.

16. Troubleshooting and Remediation Coordination: Coordinating troubleshooting and remediation efforts for the general infrastructure within the hosting environment.

17. Firewall Port Administration: Providing an interface within the management portal for firewall port administration.

18. ASV Scanning Solution: List of the service provider's Approved Scanning Vendor solution for vulnerability assessment and compliance scanning.

19. Business Continuity: Deploying high-availability and disaster recovery solutions.

20. Custom Reporting and Dashboarding: Description of availability of custom reports and dashboards.

E. GENERAL REQUIREMENTS. Proposed solution must meet the general system requirements and proposers shall provide the required information as outlined below and in Exhibit F. Functional and General Requirements:

1. Technical Solution: Detailed architecture, security measures, network configuration, and data protection plans to reflect all applicable services in the scope of work.

2. Compliance Documentation: Evidence of PCI DSS compliance and industry certifications. (Additionally, each item on the PCI DSS form (Exhibit J) shall be initialed by the proposer and submitted with the response documents).

3. PCI DSS 4.0 Compliance Approach: Clear outline of steps to achieve compliance with PCI DSS 4.0 standards.

4. Supported Operating Systems List: Comprehensive list of supported operating systems.

5. Vendor Lock-In and Data Portability Strategy: Explanation of handling data portability and migration.

6. Continuous Improvement and Innovation: Explain how hosting provider ensures ongoing innovation and improvement in security practices to stay ahead of emerging threats.

7. Regulatory Compliance Expertise: Company's expertise in other relevant regulations and standards, such as GDPR or HIPAA, depending on your use case.

8. Service Level Agreements (SLAs): Proposed SLAs for uptime, response times, and issue resolution.

9. Data Center Location: The provider's data center must be located within the continental United States.

10. Vendor Lock-In and Data Portability: Discuss how the hosting provider handles data portability and migration should one choose to switch providers in the future.

F. COST PROPOSAL RESPONSE TEMPLATE. Proposers shall complete Exhibit D – Price Proposal Template and return to the City as part of their RFP response. All prices shall be firm, fixed, fully burdened, FOB destination, and include any applicable delivery or freight charges, and any other costs, including, but not limited to, travel, required to provide the requirements as specified in this RFP. Any discount offered other than for prompt payment should be included in the net price quoted instead of shown as a separate item.

Payment for services will be processed via monthly recurring payments based on the unit costs related to the size and scope of the environment at that time, as well as any supplemental costs related to any additional services provided. A one-time payment will also be made following any necessary transition/migration efforts.

G. OTHER REQUIREMENTS. Proposer shall complete Exhibit G. Interrogatories matrix which includes the following:

1. Proposer Key Personnel, Experience, Training, Qualifications, and Certifications

a) Proposer's Background and Experience: Proposer must include a company overview including related experience to the services being requested in this RFP.

b) Resumes: Proposer must include brief resumes for personnel that will be assigned to the implementation project, if awarded the contract. The resumes must identify expertise in the functional areas listed in the RFP. Proven work experience combined with related education will be means of substantiating expertise.

c) References: Client references shall be submitted on the City's Contractor Standards Pledge of Compliance from at least three (3) current and/or prior customers where a Solution of similar size and scope has been implemented within the last five (5) years.

i. References will be verified during evaluation of the proposals.

ii. If the City does not timely receive a reference from the contact provided, the reference may be classified as unsatisfactory. Alternative contacts may be provided, as determined solely by the City.

2. Project Management, Overall Approach, Training & Support

Proposers shall provide a project plan for the fixed-price delivery of the implementation services. Proposer's response to the requirement in the RFP must include, but not be limited to:

a) Single Point of Contact: The Proposer must identify a single point of contact for all contract management activities. The Proposer's Project Manager's name and resume must be submitted with the proposal. The successful Proposer must not change the Project Manager without written City approval.

b) Project Management Plan: The proposal must contain a comprehensive and practical description of the Proposer's plans for project management with regards to City staff engagement, implementation of the proposed solution, control mechanisms including staff organizational structure, progress reporting, major decision making, sign-off procedures, and internal control procedures. The Proposer shall also indicate flexibility in meeting changes in program requirements and coping with problems.

c) Project Timeline: The Proposer must submit a project plan that meets the needs of the Request for Proposal (RFP) and indicates a thorough understanding of the scope of the work as outlined in this RFP.

d) Project Delays: Proposer must also describe typical project delays when implementing this solution and how project delays will be addressed should they occur. The process for submitting Change Requests, and remedying project delays should also be detailed. All Assurances that sufficient resources and

knowledgeable experienced staff are available to meet any of the project schedule must be described.

e) Scope Management: Proposer must describe the change control process for scope management. This should include the initiation of any scope changes and subsequent approvals.

f) Staffing and Project Organization: The Proposer's organization chart must be included with all proposed personnel, including the supervisor level, functional responsibilities, key personnel, and other staff members who will be involved in the project and percentage of time dedicated to project. Proposers should describe their commitment to ensuring the composition of the project team will remain consistent throughout the course of the implementation phase. Project team cannot be substituted, or staff added without prior notice and acceptance by the City. Prime Contractors may use subcontractors; however, the Prime Contractor must be the Proposer. All subcontractors must be listed in the Contractor Standards Pledge of Compliance form. If Contractor wishes to bring in a subcontractor for performance under the agreement, the City must approve the subcontractor in writing. The Proposer must also identify key resources located in the San Diego area.

g) Migration Strategy: Please describe the migration strategy for this project based on the different databases. (How would the Proposer determine the best process for moving all past/historical data into the new solution?) Detail your methodology for testing/QA and ensuring risk of business disruption is properly mitigated. This migration strategy must be reflected in the migration costs for this proposal. Proposers must describe their experience with migrating these specific database/data types and describe what difficulties may be encountered during migration due to these data types.

h) Final System Testing & Acceptance: Please outline and describe the acceptance testing process that will confirm system operations and ensure that the system meets all of the functional requirements as outlined in this RFP.

i) Transition Plan: Please outline and describe the proposed transition plan that ensures proposed solution has been validated and tested, and have obtained the City's final acceptance that the Contractor is prepared to deliver all services to the requirements described in the Agreement.

j) Training Strategy & Recommended Training Plan: Please outline and describe the appropriate training for the Project Team as Administrators and Trainers as well as End Users based on the requirements in this proposal. This plan must include training materials (e.g. user manuals) and be reflected in the training costs for this proposal. The manuals must be routinely updated as policies or programs are changed. Training will begin no later than thirty (30) calendar days after the solution is installed and accepted by the City. The City prefers virtual training, however we will also want the option for on-site training.

Please describe details of the types of training provided as well as training documents. Indicate if the training is provided as part of this proposal or available as part of continuing support.

k) Levels of Support: Please describe in detail the levels of support provided for this solution and how they align with the City's requirements. In this description, please include the terms of the support and the services provided. The support level pricing must be reflected in the cost proposal. If there are saving opportunities, please provide additional options as available.

l) Licensing. The following licensing requirements shall apply:

i. System User Software License Agreements. Proposer shall provide a copy of all System User software license agreements that they will be requesting the City to execute. The license agreements should address all software components including third-party software, base system software provided by the Proposer, and custom software developed specifically for this project. The software license agreements provided should be the actual documents (or exact duplicates) of the forms used for this project, not a typical sample document.

ii. Licensing Model. Proposer shall clearly indicate the nature of their Solution's licensing model (i.e., Named User, Concurrent User, Flat Subscription, or volume-based metrics [e.g., transactions, unlimited 'enterprise' style licensing or named licenses]). See Exhibit D. Pricing Schedule.

iii. License Transfer. Solution licensing must be easily transferred by a City administrator, should the need occur (e.g., member of staff leaves the organization).

iv. Licensing Volume Changes. Solution must allow the City to increase or decrease its licensing requirements through the duration of the contract.

v. Unused Licensing Volume. Solution must allow the City to 'roll-over' unused licensing (e.g., transactions into subsequent contract terms, should the City choose to exercise its right to extend the Contract term).

vi. Overage Costs. Solution must clearly describe the circumstances and thresholds (if any) under which the City may become liable for overage costs (e.g., exceeding bandwidth, storage, transactions, etc.,).

vii. Not-to-Diminish Rights. Any resulting Agreement between the City and Proposer will ensure that the functionalities of the Solution purchased, irrespective of whether it has been purchased as a set of more than one software product supplied as a single price, will be retained for the duration of the Agreement, inclusive of any agreed extensions. Any resulting incremental unitary purchases of Software will be made against the same Software originally purchased under this Agreement.

viii. Third Party Use. Proposer will grant City a non-exclusive license during the Contract Term to install and/or execute Solution on machines operated by or for City solely to facilitate City's authorized access to and use of the acquired Solution. City's primary third-party information technology service providers shall have access to and use of the Solution solely to provide support for City's internal business use.

3. Minimum Service Level Requirements.

a) Hours of Operation.

The Solution shall be fully functional and available 24 hours a day, 7 days a week, except for Scheduled Maintenance.

b) Uptime Availability

Proposer warrants that the Solution will be available to be accessed by the City at least 99.99% (Uptime Availability) of each calendar month during the Service Period.

1) Uptime Availability Remuneration. Where Proposer fails to meet the Uptime Availability Service Level, then City is entitled to claim the following prorated Service Credits against the annual Subscription Fee:

≥ 99.97% but <99.99% = 10% of prorated monthly Subscription Fee.
≥ 99.95% but <99.97% = 15% of prorated monthly Subscription Fee.
< 99.95% = 25% of prorated monthly Subscription Fee.

2) Service Credits Calculation. Uptime Availability will be calculated monthly by Proposer and such calculation will be deemed binding on the parties in absence of manifest error. Uptime availability is calculated based on the following formula:

UA = (T – M – D) / (T – M) x 100% where UA = Uptime Availability, T = Total Monthly Minutes, M = Schedule Maintenance Minutes, and D = Downtime Minutes. When calculating any service level, any failure to meet the Service Level that is directly or indirectly caused by any one or more of the following items shall not constitute a failure of the Service Level:

- Scheduled Maintenance;
- Any unlawful, negligent, or willful act or omission by City, City's Agents, contractors or invitees or any other person; and
- Any Force Majeure event.

3) Scheduled Maintenance. The Proposer must provide advanced notice of any scheduled downtime, the date of occurrence, anticipated duration, and the start time of the occurrence in the applicable Pacific Standard Time or Pacific Daylight-Saving Time. To the extent possible, if known unscheduled downtime is required or recommended, written notice must be provided and to and approved by the City prior to the downtime occurrence.

4. **Software Revisions**
   The software shall be regularly updated for functionality, stability, and security improvements. The City shall have discretion as to the timing of implementing the update to a newer version of software. The Proposer shall provide the City with the planned end-of-life (support) schedule for all versions of the software.

5. **Multi-Tier Support Helpdesk**
   The Proposer will also provide hours of Tier One and Tier Two Help Desk support while remotely utilizing existing resources to handle all software related user questions as well as to provide remote diagnostics. These resources are available Monday through Friday, 7:00 a.m. to 5:00 p.m. (PT), excluding federal holidays. Calls relating to how to use the application shall be reconciled by Tier One Help Desk support. Tier Two support shall be an escalation resource for more complex problems not easily solved by Tier One support.

H. ADDITIONAL INSURANCE. Below are the insurance requirements in addition to the requirements specified in Article VII of the General Contract Terms and Provisions:

Commercial General Liability Insurance. All requirements as specified in the General Contract Terms and Provisions of the contract apply, however the minimum limits are **$2 million per Occurrence and $4 million General Aggregate**.

Cyber Liability Insurance. Cyber Liability Insurance, with limits not less than $1,000,000 per occurrence or claim, $2,000,000 aggregate. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Vendor in this agreement and shall include, but not be limited to, claims involving security breach, system failure, data recovery, business interruption, cyber extortion, social engineering, infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, and alteration of electronic information. The policy shall provide coverage for breach response costs, regulatory fines and penalties as well as credit monitoring expenses.

I. PAYMENT CARD INDUSTRY DATA SECURITY DOCUMENTS

1. Contractor Certification. Contractor certifies that it will implement and at all times comply with the most current Payment Card Industry Data Security Standards (PCI DSS) regarding data security. Contractor will provide written annual confirmation of PCI DSS compliance from the credit card types used by the City (i.e. VISA, MasterCard, Discover, and American Express). Contractor will immediately notify the City if it undergoes, or has reason to believe that it will undergo, an adverse change resulting in the loss of compliance with the PCI DSS standards and/or other material payment card industry standards. In addition, Contractor shall provide payment card companies, acquiring financial institutions, and their respective designees required access to the Contractor's facilities and all pertinent records as deemed necessary by the City to verify Contractor's compliance with the PCI DSS requirements.

2. Data Security. Contractor acknowledges responsibility for the security of cardholder data as defined within PCI DSS standards. Contractor shall undergo independent

third party quarterly system scans that audit for all known methods hackers use to access private information, in addition to vulnerabilities that would allow malicious software (i.e., viruses and worms) to gain access to or disrupt network devices. Upon request, Contractor will provide the City's Chief Information Security Officer with copies of the quarterly scans for verification. Contractor will provide reasonable care and efforts to detect fraudulent credit card activity in connection with credit card transactions processed during the performance of this Contract.

3. Use of Data. Contractor acknowledges and agrees that Contractor may only use cardholder data for completing the work as described in the Contract Specifications consistent with PCI DSS standards or applicable law. Contractor shall maintain and protect in accordance with all applicable laws and PCI DSS standards the security of all cardholder data when performing the Services.

4. Notification Requirements. Contractor shall immediately notify the City's Chief Information Security Officer of any breach, intrusion, or unauthorized card access to allow the proper PCI DSS breach notification process to commence. Contractor agrees to assume responsibility for informing all affected individuals in accordance with applicable law. All notifications and required compliance documents regarding PCI DSS shall be sent to:

Chief Information Security Officer
1010 2nd Avenue, Suite 500
San Diego, CA 92101
Cybersecurity@sandiego.gov
619-533-4840

5. Indemnity. Contractor shall indemnify and hold harmless the City, its officers, and employees from and against any claims, loss, damages, or other harm related to a data security breach or Contractor's failure to maintain PCI DSS compliance standards.

6. **Payment Card Industry Data Security Standards (PCI DSS) Form.** Each item on the PCI DSS form **(Exhibit J)** shall be initialed by the bidder and submitted with bid response documents.

EXHIBIT C

THE CITY OF SAN DIEGO

GENERAL CONTRACT TERMS AND PROVISIONS

APPLICABLE TO GOODS, SERVICES, AND CONSULTANT CONTRACTS

ARTICLE I
SCOPE AND TERM OF CONTRACT

1.1 Scope of Contract. The scope of contract between the City and a provider of goods and/or services (Contractor) is described in the Contract Documents. The Contract Documents are comprised of the Request for Proposal, Invitation to Bid, or other solicitation document (Solicitation); the successful bid or proposal; the letter awarding the contract to Contractor; the City's written acceptance of exceptions or clarifications to the Solicitation, if any; and these General Contract Terms and Provisions.

1.2 Effective Date. A contract between the City and Contractor (Contract) is effective on the last date that the contract is signed by the parties and approved by the City Attorney in accordance with Charter section 40. Unless otherwise terminated, this Contract is effective until it is completed or as otherwise agreed upon in writing by the parties, whichever is the earliest. A Contract term cannot exceed five (5) years unless approved by the City Council by ordinance.

1.3 Contract Extension. The City may, in its sole discretion, unilaterally exercise an option to extend the Contract as described in the Contract Documents. In addition, the City may, in its sole discretion, unilaterally extend the Contract on a month-to-month basis following contract expiration if authorized under Charter section 99 and the Contract Documents. Contractor shall not increase its pricing in excess of the percentage increase described in the Contract.

ARTICLE II
CONTRACT ADMINISTRATOR

2.1 Contract Administrator. The Purchasing Agent or designee is the Contract Administrator for purposes of this Contract, and has the responsibilities described in this Contract, in the San Diego Charter, and in Chapter 2, Article 2, Divisions 5, 30, and 32.

2.1.1 Contractor Performance Evaluations. The Contract Administrator will evaluate Contractor's performance as often as the Contract Administrator deems necessary throughout the term of the contract. This evaluation will be based on criteria including the quality of goods or services, the timeliness of performance, and adherence to applicable laws, including prevailing wage and living wage. City will provide Contractors who receive an unsatisfactory rating with a copy of the evaluation and an opportunity to respond. City may consider final evaluations, including Contractor's response, in evaluating future proposals and bids for contract award.

2.2 Notices. Unless otherwise specified, in all cases where written notice is required under this Contract, service shall be deemed sufficient if the notice is personally delivered or deposited in the United States mail, with first class postage paid, attention to the Purchasing Agent. Proper notice is effective on the date of personal delivery or five (5) days after deposit in a United States postal mailbox unless provided otherwise in the Contract. Notices to the City shall be sent to:

Purchasing Agent
City of San Diego, Purchasing and Contracting Division
1200 3rd Avenue, Suite 200
San Diego, CA 92101-4195

ARTICLE III
COMPENSATION

3.1 Manner of Payment. Contractor will be paid monthly, in arrears, for goods and/or services provided in accordance with the terms and provisions specified in the Contract.

3.2 Invoices.

3.2.1 Invoice Detail. Contractor's invoice must be on Contractor's stationary with Contractor's name, address, and remittance address if different. Contractor's invoice must have a date, an invoice number, a purchase order number, a description of the goods or services provided, and an amount due.

3.2.2 Service Contracts. Contractor must submit invoices for services to City by the 10th of the month following the month in which Contractor provided services. Invoices must include the address of the location where services were performed and the dates in which services were provided.

3.2.3 Goods Contracts. Contractor must submit invoices for goods to City within seven days of the shipment. Invoices must describe the goods provided.

3.2.4 Parts Contracts. Contractor must submit invoices for parts to City within seven calendar (7) days of the date the parts are shipped. Invoices must include the manufacturer of the part, manufacturer's published list price, percentage discount applied in accordance with Pricing Page(s), the net price to City, and an item description, quantity, and extension.

3.2.5 Extraordinary Work. City will not pay Contractor for extraordinary work unless Contractor receives prior written authorization from the Contract Administrator. Failure to do so will result in payment being withheld for services. If approved, Contractor will include an invoice that describes the work performed and the location where the work was performed, and a copy of the Contract Administrator's written authorization.

3.2.6 Reporting Requirements. Contractor must submit the following reports using the City's web-based contract compliance portal. Incomplete and/or delinquent reports may cause payment delays, non-payment of invoice, or both. For questions, please view the City's online tutorials on how to utilize the City's web-based contract compliance portal.

3.2.6.1 Monthly Employment Utilization Reports. Contractor and Contractor's subcontractors and suppliers must submit Monthly Employment Utilization Reports by the fifth (5th) day of the subsequent month.

3.2.6.2 Monthly Invoicing and Payments. Contractor and Contractor's subcontractors and suppliers must submit Monthly Invoicing and Payment Reports by the fifth (5^{th}) day of the subsequent month.

3.3 Annual Appropriation of Funds. Contractor acknowledges that the Contract term may extend over multiple City fiscal years, and that work and compensation under this Contract is contingent on the City Council appropriating funding for and authorizing such work and compensation for those fiscal years. This Contract may be terminated at the end of the fiscal year for which sufficient funding is not appropriated and authorized. City is not obligated to pay Contractor for any amounts not duly appropriated and authorized by City Council.

3.4 Price Adjustments. Based on Contractor's written request and justification, the City may approve an increase in unit prices on Contractor's pricing pages consistent with the amount requested in the justification in an amount not to exceed the increase in the Consumer Price Index, San Diego Area, for All Urban Customers (CPI-U) as published by the Bureau of Labor Statistics, or 5.0%, whichever is less, during the preceding one year term. If the CPI-U is a negative number, then the unit prices shall not be adjusted for that option year (the unit prices will not be decreased). A negative CPI-U shall be counted against any subsequent increases in the CPI-U when calculating the unit prices for later option years. Contractor must provide such written request and justification no less than sixty days before the date in which City may exercise the option to renew the contract, or sixty days before the anniversary date of the Contract. Justification in support of the written request must include a description of the basis for the adjustment, the proposed effective date and reasons for said date, and the amount of the adjustment requested with documentation to support the requested change (e.g. CPI-U or 5.0%, whichever is less). City's approval of this request must be in writing.

ARTICLE IV
SUSPENSION AND TERMINATION

4.1 City's Right to Suspend for Convenience. City may suspend all or any portion of Contractor's performance under this Contract at its sole option and for its convenience for a reasonable period of time not to exceed six (6) months. City must first give ten (10) days' written notice to Contractor of such suspension. City will pay to Contractor a sum equivalent to the reasonable value of the goods and/or services satisfactorily provided up to the date of suspension. City may rescind the suspension prior to or at six (6) months by providing Contractor with written notice of the rescission, at which time Contractor would be required to resume performance in compliance with the terms and provisions of this Contract. Contractor will be entitled to an extension of time to complete performance under the Contract equal to the length of the suspension unless otherwise agreed to in writing by the Parties.

4.2 City's Right to Terminate for Convenience. City may, at its sole option and for its convenience, terminate all or any portion of this Contract by giving thirty (30) days' written notice of such termination to Contractor. The termination of the Contract shall be effective upon receipt of the notice by Contractor. After termination of all or any portion of the Contract, Contractor shall: (1) immediately discontinue all affected performance (unless the notice directs otherwise); and (2) complete any and all additional work necessary for the orderly filing of

documents and closing of Contractor's affected performance under the Contract. After filing of documents and completion of performance, Contractor shall deliver to City all data, drawings, specifications, reports, estimates, summaries, and such other information and materials created or received by Contractor in performing this Contract, whether completed or in process. By accepting payment for completion, filing, and delivering documents as called for in this section, Contractor discharges City of all of City's payment obligations and liabilities under this Contract with regard to the affected performance.

4.3 City's Right to Terminate for Default. Contractor's failure to satisfactorily perform any obligation required by this Contract constitutes a default. Examples of default include a determination by City that Contractor has: (1) failed to deliver goods and/or perform the services of the required quality or within the time specified; (2) failed to perform any of the obligations of this Contract; and (3) failed to make sufficient progress in performance which may jeopardize full performance.

4.3.1 If Contractor fails to satisfactorily cure a default within ten (10) calendar days of receiving written notice from City specifying the nature of the default, City may immediately cancel and/or terminate this Contract, and terminate each and every right of Contractor, and any person claiming any rights by or through Contractor under this Contract.

4.3.2 If City terminates this Contract, in whole or in part, City may procure, upon such terms and in such manner as the Purchasing Agent may deem appropriate, equivalent goods or services and Contractor shall be liable to City for any excess costs. Contractor shall also continue performance to the extent not terminated.

4.4 Termination for Bankruptcy or Assignment for the Benefit of Creditors. If Contractor files a voluntary petition in bankruptcy, is adjudicated bankrupt, or makes a general assignment for the benefit of creditors, the City may at its option and without further notice to, or demand upon Contractor, terminate this Contract, and terminate each and every right of Contractor, and any person claiming rights by and through Contractor under this Contract.

4.5 Contractor's Right to Payment Following Contract Termination.

4.5.1 Termination for Convenience. If the termination is for the convenience of City an equitable adjustment in the Contract price shall be made. No amount shall be allowed for anticipated profit on unperformed services, and no amount shall be paid for an as needed contract beyond the Contract termination date.

4.5.2 Termination for Default. If, after City gives notice of termination for failure to fulfill Contract obligations to Contractor, it is determined that Contractor had not so failed, the termination shall be deemed to have been effected for the convenience of City. In such event, adjustment in the Contract price shall be made as provided in Section 4.3.2. City's rights and remedies are in addition to any other rights and remedies provided by law or under this Contract.

4.6 Remedies Cumulative. City's remedies are cumulative and are not intended to be exclusive of any other remedies or means of redress to which City may be lawfully entitled in case of any breach or threatened breach of any provision of this Contract.

ARTICLE V
ADDITIONAL CONTRACTOR OBLIGATIONS

5.1 Inspection and Acceptance. The City will inspect and accept goods provided under this Contract at the shipment destination unless specified otherwise. Inspection will be made and acceptance will be determined by the City department shown in the shipping address of the Purchase Order or other duly authorized representative of City.

5.2 Responsibility for Lost or Damaged Shipments. Contractor bears the risk of loss or damage to goods prior to the time of their receipt and acceptance by City. City has no obligation to accept damaged shipments and reserves the right to return damaged goods, at Contractor's sole expense, even if the damage was not apparent or discovered until after receipt.

5.3 Responsibility for Damages. Contractor is responsible for all damage that occurs as a result of Contractor's fault or negligence or that of its' employees, agents, or representatives in connection with the performance of this Contract. Contractor shall immediately report any such damage to people and/or property to the Contract Administrator.

5.4 Delivery. Delivery shall be made on the delivery day specified in the Contract Documents. The City, in its sole discretion, may extend the time for delivery. The City may order, in writing, the suspension, delay or interruption of delivery of goods and/or services.

5.5 Delay. Unless otherwise specified herein, time is of the essence for each and every provision of the Contract. Contractor must immediately notify City in writing if there is, or it is anticipated that there will be, a delay in performance. The written notice must explain the cause for the delay and provide a reasonable estimate of the length of the delay. City may terminate this Contract as provided herein if City, in its sole discretion, determines the delay is material.

5.5.1 If a delay in performance is caused by any unforeseen event(s) beyond the control of the parties, City may allow Contractor to a reasonable extension of time to complete performance, but Contractor will not be entitled to damages or additional compensation. Any such extension of time must be approved in writing by City. The following conditions may constitute such a delay: war; changes in law or government regulation; labor disputes; strikes; fires, floods, adverse weather or other similar condition of the elements necessitating cessation of the performance; inability to obtain materials, equipment or labor; or other specific reasons agreed to between City and Contractor. This provision does not apply to a delay caused by Contractor's acts or omissions. Contractor is not entitled to an extension of time to perform if a delay is caused by Contractor's inability to obtain materials, equipment, or labor unless City has received, in a timely manner, documentary proof satisfactory to City of Contractor's inability to obtain materials, equipment, or labor, in which case City's approval must be in writing.

5.6 Restrictions and Regulations Requiring Contract Modification. Contractor shall immediately notify City in writing of any regulations or restrictions that may or will require Contractor to alter the material, quality, workmanship, or performance of the goods and/or services to be provided. City reserves the right to accept any such alteration, including any resulting reasonable price adjustments, or to cancel the Contract at no expense to the City.

5.7 Warranties. All goods and/or services provided under the Contract must be warranted by Contractor or manufacturer for at least twelve (12) months after acceptance by City, except automotive equipment. Automotive equipment must be warranted for a minimum of 12,000 miles or 12 months, whichever occurs first, unless otherwise stated in the Contract. Contractor is responsible to City for all warranty service, parts, and labor. Contractor is required to ensure that warranty work is performed at a facility acceptable to City and that services, parts, and labor are available and provided to meet City's schedules and deadlines. Contractor may establish a warranty service contract with an agency satisfactory to City instead of performing the warranty service itself. If Contractor is not an authorized service center and causes any damage to equipment being serviced, which results in the existing warranty being voided, Contractor will be liable for all costs of repairs to the equipment, or the costs of replacing the equipment with new equipment that meets City's operational needs.

5.8 Industry Standards. Contractor shall provide goods and/or services acceptable to City in strict conformance with the Contract. Contractor shall also provide goods and/or services in accordance with the standards customarily adhered to by an experienced and competent provider of the goods and/or services called for under this Contract using the degree of care and skill ordinarily exercised by reputable providers of such goods and/or services. Where approval by City, the Mayor, or other representative of City is required, it is understood to be general approval only and does not relieve Contractor of responsibility for complying with all applicable laws, codes, policies, regulations, and good business practices.

5.9 Records Retention and Examination. Contractor shall retain, protect, and maintain in an accessible location all records and documents, including paper, electronic, and computer records, relating to this Contract for five (5) years after receipt of final payment by City under this Contract. Contractor shall make all such records and documents available for inspection, copying, or other reproduction, and auditing by authorized representatives of City, including the Purchasing Agent or designee. Contractor shall make available all requested data and records at reasonable locations within City or County of San Diego at any time during normal business hours, and as often as City deems necessary. If records are not made available within the City or County of San Diego, Contractor shall pay City's travel costs to the location where the records are maintained and shall pay for all related travel expenses. Failure to make requested records available for inspection, copying, or other reproduction, or auditing by the date requested may result in termination of the Contract. Contractor must include this provision in all subcontracts made in connection with this Contract.

5.9.1 Contractor shall maintain records of all subcontracts entered into with all firms, all project invoices received from Subcontractors and Suppliers, all purchases of materials and services from Suppliers, and all joint venture participation. Records shall show name, telephone number including area code, and business address of each Subcontractor and Supplier, and joint venture partner, and the total amount actually paid to each firm. Project relevant records, regardless of tier, may be periodically reviewed by the City.

5.10 Quality Assurance Meetings. Upon City's request, Contractor shall schedule one or more quality assurance meetings with City's Contract Administrator to discuss Contractor's performance. If requested, Contractor shall schedule the first quality assurance meeting no later than eight (8) weeks from the date of commencement of work under the Contract. At the quality assurance meeting(s), City's Contract Administrator will provide Contractor with feedback, will note any deficiencies in Contract performance, and provide Contractor with an opportunity to address and correct such deficiencies. The total number of quality assurance meetings that may be required by City will depend upon Contractor's performance.

5.11 Duty to Cooperate with Auditor. The City Auditor may, in his sole discretion, at no cost to the City, and for purposes of performing his responsibilities under Charter section 39.2, review Contractor's records to confirm contract compliance. Contractor shall make reasonable efforts to cooperate with Auditor's requests.

5.12 Safety Data Sheets. If specified by City in the solicitation or otherwise required by this Contract, Contractor must send with each shipment one (1) copy of the Safety Data Sheet (SDS) for each item shipped. Failure to comply with this procedure will be cause for immediate termination of the Contract for violation of safety procedures.

5.13 Project Personnel. Except as formally approved by the City, the key personnel identified in Contractor's bid or proposal shall be the individuals who will actually complete the work. Changes in staffing must be reported in writing and approved by the City.

5.13.1 Criminal Background Certification. Contractor certifies that all employees working on this Contract have had a criminal background check and that said employees are clear of any sexual and drug related convictions. Contractor further certifies that all employees hired by Contractor or a subcontractor shall be free from any felony convictions.

5.13.2 Photo Identification Badge. Contractor shall provide a company photo identification badge to any individual assigned by Contractor or subcontractor to perform services or deliver goods on City premises. Such badge must be worn at all times while on City premises. City reserves the right to require Contractor to pay fingerprinting fees for personnel assigned to work in sensitive areas. All employees shall turn in their photo identification badges to Contractor upon completion of services and prior to final payment of invoice.

5.14 Standards of Conduct. Contractor is responsible for maintaining standards of employee competence, conduct, courtesy, appearance, honesty, and integrity satisfactory to the City.

5.14.1 Supervision. Contractor shall provide adequate and competent supervision at all times during the Contract term. Contractor shall be readily available to meet with the City. Contractor shall provide the telephone numbers where its representative(s) can be reached.

5.14.2 City Premises. Contractor's employees and agents shall comply with all City rules and regulations while on City premises.

5.14.3 Removal of Employees. City may request Contractor immediately remove from assignment to the City any employee found unfit to perform duties at the City. Contractor shall comply with all such requests.

5.15 Licenses and Permits. Contractor shall, without additional expense to the City, be responsible for obtaining any necessary licenses, permits, certifications, accreditations, fees and approvals for complying with any federal, state, county, municipal, and other laws, codes, and regulations applicable to Contract performance. This includes, but is not limited to, any laws or regulations requiring the use of licensed contractors to perform parts of the work.

5.16 Contractor and Subcontractor Registration Requirements. Prior to the award of the Contract or Task Order, Contractor and Contractor's subcontractors and suppliers must register with the City's web-based vendor registration and bid management system. The City may not award the Contract until registration of all subcontractors and suppliers is complete. In the event this requirement is not met within the time frame specified by the City, the City reserves the right to rescind the Contract award and to make the award to the next responsive and responsible proposer of bidder.

ARTICLE VI
INTELLECTUAL PROPERTY RIGHTS

6.1 Rights in Data. If, in connection with the services performed under this Contract, Contractor or its employees, agents, or subcontractors, create artwork, audio recordings, blueprints, designs, diagrams, documentation, photographs, plans, reports, software, source code, specifications, surveys, system designs, video recordings, or any other original works of authorship, whether written or readable by machine (Deliverable Materials), all rights of Contractor or its subcontractors in the Deliverable Materials, including, but not limited to publication, and registration of copyrights, and trademarks in the Deliverable Materials, are the sole property of City. Contractor, including its employees, agents, and subcontractors, may not use any Deliverable Material for purposes unrelated to Contractor's work on behalf of the City without prior written consent of City. Contractor may not publish or reproduce any Deliverable Materials, for purposes unrelated to Contractor's work on behalf of the City, without the prior written consent of the City.

6. 2 Intellectual Property Rights Assignment. For no additional compensation, Contractor hereby assigns to City all of Contractor's rights, title, and interest in and to the content of the Deliverable Materials created by Contractor or its employees, agents, or subcontractors, including copyrights, in connection with the services performed under this Contract. Contractor

shall promptly execute and deliver, and shall cause its employees, agents, and subcontractors to promptly execute and deliver, upon request by the City or any of its successors or assigns at any time and without further compensation of any kind, any power of attorney, assignment, application for copyright, patent, trademark or other intellectual property right protection, or other papers or instruments which may be necessary or desirable to fully secure, perfect or otherwise protect to or for the City, its successors and assigns, all right, title and interest in and to the content of the Deliverable Materials. Contractor also shall cooperate and assist in the prosecution of any action or opposition proceeding involving such intellectual property rights and any adjudication of those rights.

6. 3 Contractor Works. Contractor Works means tangible and intangible information and material that: (a) had already been conceived, invented, created, developed or acquired by Contractor prior to the effective date of this Contract; or (b) were conceived, invented, created, or developed by Contractor after the effective date of this Contract, but only to the extent such information and material do not constitute part or all of the Deliverable Materials called for in this Contract. All Contractor Works, and all modifications or derivatives of such Contractor Works, including all intellectual property rights in or pertaining to the same, shall be owned solely and exclusively by Contractor.

6. 4 Subcontracting. In the event that Contractor utilizes a subcontractor(s) for any portion of the work that comprises the whole or part of the specified Deliverable Materials to the City, the agreement between Contractor and the subcontractor shall include a statement that identifies the Deliverable Materials as a "works for hire" as described in the United States Copyright Act of 1976, as amended, and that all intellectual property rights in the Deliverable Materials, whether arising in copyright, trademark, service mark or other forms of intellectual property rights, belong to and shall vest solely with the City. Further, the agreement between Contractor and its subcontractor shall require that the subcontractor, if necessary, shall grant, transfer, sell and assign, free of charge, exclusively to City, all titles, rights and interests in and to the Deliverable Materials, including all copyrights, trademarks and other intellectual property rights. City shall have the right to review any such agreement for compliance with this provision.

6. 5 Intellectual Property Warranty and Indemnification. Contractor represents and warrants that any materials or deliverables, including all Deliverable Materials, provided under this Contract are either original, or not encumbered, and do not infringe upon the copyright, trademark, patent or other intellectual property rights of any third party, or are in the public domain. If Deliverable Materials provided hereunder become the subject of a claim, suit or allegation of copyright, trademark or patent infringement, City shall have the right, in its sole discretion, to require Contractor to produce, at Contractor's own expense, new non-infringing materials, deliverables or works as a means of remedying any claim of infringement in addition to any other remedy available to the City under law or equity. Contractor further agrees to indemnify, defend, and hold harmless the City, its officers, employees and agents from and against any and all claims, actions, costs, judgments or damages, of any type, alleging or threatening that any Deliverable Materials, supplies, equipment, services or works provided under this contract infringe the copyright, trademark, patent or other intellectual property or proprietary rights of any third party (Third Party Claim of Infringement). If a Third Party Claim

of Infringement is threatened or made before Contractor receives payment under this Contract, City shall be entitled, upon written notice to Contractor, to withhold some or all of such payment.

6.6 Software Licensing. Contractor represents and warrants that the software, if any, as delivered to City, does not contain any program code, virus, worm, trap door, back door, time or clock that would erase data or programming or otherwise cause the software to become inoperable, inaccessible, or incapable of being used in accordance with its user manuals, either automatically, upon the occurrence of licensor-selected conditions or manually on command. Contractor further represents and warrants that all third party software, delivered to City or used by Contractor in the performance of the Contract, is fully licensed by the appropriate licensor.

6.7 Publication. Contractor may not publish or reproduce any Deliverable Materials, for purposes unrelated to Contractor's work on behalf of the City without prior written consent from the City.

6.8 Royalties, Licenses, and Patents. Unless otherwise specified, Contractor shall pay all royalties, license, and patent fees associated with the goods that are the subject of this solicitation. Contractor warrants that the goods, materials, supplies, and equipment to be supplied do not infringe upon any patent, trademark, or copyright, and further agrees to defend any and all suits, actions and claims for infringement that are brought against the City, and to defend, indemnify and hold harmless the City, its elected officials, officers, and employees from all liability, loss and damages, whether general, exemplary or punitive, suffered as a result of any actual or claimed infringement asserted against the City, Contractor, or those furnishing goods, materials, supplies, or equipment to Contractor under the Contract.

ARTICLE VII
INDEMNIFICATION AND INSURANCE

7.1 Indemnification. To the fullest extent permitted by law, Contractor shall defend (with legal counsel reasonably acceptable to City), indemnify, protect, and hold harmless City and its elected officials, officers, employees, agents, and representatives (Indemnified Parties) from and against any and all claims, losses, costs, damages, injuries (including, without limitation, injury to or death of an employee of Contractor or its subcontractors), expense, and liability of every kind, nature and description (including, without limitation, incidental and consequential damages, court costs, and litigation expenses and fees of expert consultants or expert witnesses incurred in connection therewith and costs of investigation) that arise out of, pertain to, or relate to, directly or indirectly, in whole or in part, any goods provided or performance of services under this Contract by Contractor, any subcontractor, anyone directly or indirectly employed by either of them, or anyone that either of them control. Contractor's duty to defend, indemnify, protect and hold harmless shall not include any claims or liabilities arising from the sole negligence or willful misconduct of the Indemnified Parties.

7.2 Insurance. Contractor shall procure and maintain for the duration of the contract insurance against claims for injuries to persons or damages to property which may arise from or

in connection with the performance of the work hereunder and the results of that work by Contractor, his agents, representatives, employees or subcontractors.

Contractor shall provide, at a minimum, the following:

7.2.1 Commercial General Liability. Insurance Services Office Form CG 00 01 covering CGL on an "occurrence" basis, including products and completed operations, property damage, bodily injury, and personal and advertising injury with limits no less than $1,000,000 per occurrence. If a general aggregate limit applies, either the general aggregate limit shall apply separately to this project/location (ISO CG 25 03 or 25 04) or the general aggregate limit shall be twice the required occurrence limit.

7.2.2 Commercial Automobile Liability. Insurance Services Office Form Number CA 0001 covering Code 1 (any auto) or, if Contractor has no owned autos, Code 8 (hired) and 9 (non-owned), with limit no less than $1,000,000 per accident for bodily injury and property damage.

7.2.3 Workers' Compensation. Insurance as required by the State of California, with Statutory Limits, and Employer's Liability Insurance with limit of no less than $1,000,000 per accident for bodily injury or disease.

7.2.4 Professional Liability (Errors and Omissions). For consultant contracts, insurance appropriate to Consultant's profession, with limit no less than $1,000,000 per occurrence or claim, $2,000,000 aggregate.

If Contractor maintains broader coverage and/or higher limits than the minimums shown above, City requires and shall be entitled to the broader coverage and/or the higher limits maintained by Contractor. Any available insurance proceeds in excess of the specified minimum limits of insurance and coverage shall be available to City.

7.2.5 Other Insurance Provisions. The insurance policies are to contain, or be endorsed to contain, the following provisions:

7.2.5.1 Additional Insured Status. The City, its officers, officials, employees, and volunteers are to be covered as additional insureds on the CGL policy with respect to liability arising out of work or operations performed by or on behalf of Contractor including materials, parts, or equipment furnished in connection with such work or operations. General liability coverage can be provided in the form of an endorsement to Contractor's insurance (at least as broad as ISO Form CG 20 10 11 85 or if not available, through the addition of both CG 20 10, CG 20 26, CG 20 33, or CG 20 38; and CG 20 37 if a later edition is used).

7.2.5.2 Primary Coverage. For any claims related to this contract, Contractor's insurance coverage shall be primary coverage at least as broad as ISO CG 20 01 04 13 as respects the City, its officers, officials, employees, and volunteers. Any insurance or self-insurance maintained by City, its officers, officials, employees, or volunteers shall be excess of Contractor's insurance and shall not contribute with it.

7.2.5.3 Notice of Cancellation. Each insurance policy required above shall provide that coverage shall not be canceled, except with notice to City.

7.2.5.4 Waiver of Subrogation. Contractor hereby grants to City a waiver of any right to subrogation which the Workers' Compensation insurer of said Contractor may acquire against City by virtue of the payment of any loss under such insurance. Contractor agrees to obtain any endorsement that may be necessary to affect this waiver of subrogation, but this provision applies regardless of whether or not the City has received a waiver of subrogation endorsement from the insurer.

7.2.5.5 Claims Made Policies (applicable only to professional liability). The Retroactive Date must be shown, and must be before the date of the contract or the beginning of contract work. Insurance must be maintained and evidence of insurance must be provided for at least five (5) years after completion of the contract of work. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a Retroactive Date prior to the contract effective date, Contractor must purchase "extended reporting" coverage for a minimum of five (5) years after completion of work.

7.3 Self Insured Retentions. Self-insured retentions must be declared to and approved by City. City may require Contractor to purchase coverage with a lower retention or provide proof of ability to pay losses and related investigations, claim administration, and defense expenses within the retention. The policy language shall provide, or be endorsed to provide, that the self-insured retention may be satisfied by either the named insured or City.

7.4 Acceptability of Insurers. Insurance is to be placed with insurers with a current A.M. Best's rating of no less than A-VI, unless otherwise acceptable to City.

City will accept insurance provided by non-admitted, "surplus lines" carriers only if the carrier is authorized to do business in the State of California and is included on the List of Approved Surplus Lines Insurers (LASLI list). All policies of insurance carried by non-admitted carriers are subject to all of the requirements for policies of insurance provided by admitted carriers described herein.

7.5 Verification of Coverage. Contractor shall furnish City with original certificates and amendatory endorsements or copies of the applicable policy language effecting coverage required by this clause. All certificates and endorsements are to be received and approved by City before work commences. However, failure to obtain the required documents prior to the work beginning shall not waive Contractor's obligation to provide them. City reserves the right to require complete, certified copies of all required insurance policies, including endorsements required by these specifications, at any time.

7.6 Special Risks or Circumstances. City reserves the right to modify these requirements, including limits, based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

7.7 Additional Insurance. Contractor may obtain additional insurance not required by this Contract.

7.8 Excess Insurance. All policies providing excess coverage to City shall follow the form of the primary policy or policies including but not limited to all endorsements.

7.9 Subcontractors. Contractor shall require and verify that all subcontractors maintain insurance meeting all the requirements stated herein, and Contractor shall ensure that City is an additional insured on insurance required from subcontractors. For CGL coverage, subcontractors shall provide coverage with a format at least as broad as the CG 20 38 04 13 endorsement.

ARTICLE VIII
BONDS

8.1 Payment and Performance Bond. Prior to the execution of this Contract, City may require Contractor to post a payment and performance bond (Bond). The Bond shall guarantee Contractor's faithful performance of this Contract and assure payment to contractors, subcontractors, and to persons furnishing goods and/or services under this Contract.

8.1.1 Bond Amount. The Bond shall be in a sum equal to twenty-five percent (25%) of the Contract amount, unless otherwise stated in the Specifications. City may file a claim against the Bond if Contractor fails or refuses to fulfill the terms and provisions of the Contract.

8.1.2 Bond Term. The Bond shall remain in full force and effect at least until complete performance of this Contract and payment of all claims for materials and labor, at which time it will convert to a ten percent (10%) warranty bond, which shall remain in place until the end of the warranty periods set forth in this Contract. The Bond shall be renewed annually, at least sixty (60) days in advance of its expiration, and Contractor shall provide timely proof of annual renewal to City.

8.1.3 Bond Surety. The Bond must be furnished by a company authorized by the State of California Department of Insurance to transact surety business in the State of California and which has a current A.M. Best rating of at least "A-, VIII."

8.1.4 Non-Renewal or Cancellation. The Bond must provide that City and Contractor shall be provided with sixty (60) days' advance written notice in the event of non-renewal, cancellation, or material change to its terms. In the event of non-renewal, cancellation, or material change to the Bond terms, Contractor shall provide City with evidence of the new source of surety within twenty-one (21) calendar days after the date of the notice of non-renewal, cancellation, or material change. Failure to maintain the Bond, as required herein, in full force

and effect as required under this Contact, will be a material breach of the Contract subject to termination of the Contract.

8.2 Alternate Security. City may, at its sole discretion, accept alternate security in the form of an endorsed certificate of deposit, a money order, a certified check drawn on a solvent bank, or other security acceptable to the Purchasing Agent in an amount equal to the required Bond.

ARTICLE IX
CITY-MANDATED CLAUSES AND REQUIREMENTS

9.1 Contractor Certification of Compliance. By signing this Contract, Contractor certifies that Contractor is aware of, and will comply with, these City-mandated clauses throughout the duration of the Contract.

9.1.1 Drug-Free Workplace Certification. Contractor shall comply with City's Drug-Free Workplace requirements set forth in Council Policy 100-17, which is incorporated into the Contract by this reference.

9.1.2 Contractor Certification for Americans with Disabilities Act (ADA) and State Access Laws and Regulations: Contractor shall comply with all accessibility requirements under the ADA and under Title 24 of the California Code of Regulations (Title 24). When a conflict exists between the ADA and Title 24, Contractor shall comply with the most restrictive requirement (i.e., that which provides the most access). Contractor also shall comply with the City's ADA Compliance/City Contractors requirements as set forth in Council Policy 100-04, which is incorporated into this Contract by reference. Contractor warrants and certifies compliance with all federal and state access laws and regulations and further certifies that any subcontract agreement for this contract contains language which indicates the subcontractor's agreement to abide by the provisions of the City's Council Policy and any applicable access laws and regulations.

9.1.3 Non-Discrimination Requirements.

9.1.3.1 Compliance with City's Equal Opportunity Contracting Program (EOCP). Contractor shall comply with City's EOCP Requirements. Contractor shall not discriminate against any employee or applicant for employment on any basis prohibited by law. Contractor shall provide equal opportunity in all employment practices. Prime Contractors shall ensure that their subcontractors comply with this program. Nothing in this Section shall be interpreted to hold a Prime Contractor liable for any discriminatory practice of its subcontractors.

9.1.3.2 Non-Discrimination Ordinance. Contractor shall not discriminate on the basis of race, gender, gender expression, gender identity, religion, national origin, ethnicity, sexual orientation, age, or disability in the solicitation, selection, hiring or treatment of subcontractors, vendors or suppliers. Contractor shall provide equal opportunity for subcontractors to participate in subcontracting opportunities. Contractor understands and agrees that violation of this clause shall be considered a material breach of the Contract and may result

in Contract termination, debarment, or other sanctions. Contractor shall ensure that this language is included in contracts between Contractor and any subcontractors, vendors and suppliers.

9.1.3.3 Compliance Investigations. Upon City's request, Contractor agrees to provide to City, within sixty calendar days, a truthful and complete list of the names of all subcontractors, vendors, and suppliers that Contractor has used in the past five years on any of its contracts that were undertaken within San Diego County, including the total dollar amount paid by Contractor for each subcontract or supply contract. Contractor further agrees to fully cooperate in any investigation conducted by City pursuant to City's Nondiscrimination in Contracting Ordinance. Contractor understands and agrees that violation of this clause shall be considered a material breach of the Contract and may result in Contract termination, debarment, and other sanctions.

9.1.4 Equal Benefits Ordinance Certification. Unless an exception applies, Contractor shall comply with the Equal Benefits Ordinance (EBO) codified in the San Diego Municipal Code (SDMC). Failure to maintain equal benefits is a material breach of the Contract.

9.1.5 Contractor Standards. Contractor shall comply with Contractor Standards provisions codified in the SDMC. Contractor understands and agrees that violation of Contractor Standards may be considered a material breach of the Contract and may result in Contract termination, debarment, and other sanctions.

9.1.6 Noise Abatement. Contractor shall operate, conduct, or construct without violating the City's Noise Abatement Ordinance codified in the SDMC.

9.1.7 Storm Water Pollution Prevention Program. Contractor shall comply with the City's Storm Water Management and Discharge Control provisions codified in Division 3 of Chapter 4 of the SDMC, as may be amended, and any and all applicable Best Management Practice guidelines and pollution elimination requirements in performing or delivering services at City owned, leased, or managed property, or in performance of services and activities on behalf of City regardless of location.

Contractor shall comply with the City's Jurisdictional Urban Runoff Management Plan encompassing Citywide programs and activities designed to prevent and reduce storm water pollution within City boundaries as adopted by the City Council on January 22, 2008, via Resolution No. 303351, as may be amended.

Contractor shall comply with each City facility or work site's Storm Water Pollution Prevention Plan, as applicable, and institute all controls needed while completing the services to minimize any negative impact to the storm water collection system and environment.

9.1.8 Service Worker Retention Ordinance. If applicable, Contractor shall comply with the Service Worker Retention Ordinance (SWRO) codified in the SDMC.

9.1.9 Product Endorsement. Contractor shall comply with Council Policy 000-41 which requires that other than listing the City as a client and other limited endorsements, any advertisements, social media, promotions or other marketing referring to the City as a user of a product or service will require prior written approval of the Mayor or designee. Use of the City Seal or City logos is prohibited.

9.1.10 Business Tax Certificate. Unless the City Treasurer determines in writing that a contractor is exempt from the payment of business tax, any contractor doing business with the City of San Diego is required to obtain a Business Tax Certificate (BTC) and to provide a copy of its BTC to the City before a Contract is executed.

9.1.11 Equal Pay Ordinance. Unless an exception applies, Contractor shall comply with the Equal Pay Ordinance codified in San Diego Municipal Code sections 22.4801 through 22.4809. Contractor shall certify in writing that it will comply with the requirements of the EPO.

9.1.11.1 Contractor and Subcontract Requirement. The Equal Pay Ordinance applies to any subcontractor who performs work on behalf of a Contractor to the same extent as it would apply to that Contractor. Any Contractor subject to the Equal Pay Ordinance shall require all of its subcontractors to certify compliance with the Equal Pay Ordinance in its written subcontracts.

ARTICLE X
CONFLICT OF INTEREST AND VIOLATIONS OF LAW

10.1 Conflict of Interest Laws. Contractor is subject to all federal, state and local conflict of interest laws, regulations, and policies applicable to public contracts and procurement practices including, but not limited to, California Government Code sections 1090, *et. seq.* and 81000*, et. seq.,* and the Ethics Ordinance, codified in the SDMC. City may determine that Contractor must complete one or more statements of economic interest disclosing relevant financial interests. Upon City's request, Contractor shall submit the necessary documents to City.

10.2 Contractor's Responsibility for Employees and Agents. Contractor is required to establish and make known to its employees and agents appropriate safeguards to prohibit employees from using their positions for a purpose that is, or that gives the appearance of being, motivated by the desire for private gain for themselves or others, particularly those with whom they have family, business or other relationships.

10.3 Contractor's Financial or Organizational Interests. In connection with any task, Contractor shall not recommend or specify any product, supplier, or contractor with whom Contractor has a direct or indirect financial or organizational interest or relationship that would violate conflict of interest laws, regulations, or policies.

10.4 Certification of Non-Collusion. Contractor certifies that: (1) Contractor's bid or proposal was not made in the interest of or on behalf of any person, firm, or corporation not identified; (2) Contractor did not directly or indirectly induce or solicit any other bidder or proposer to put in a sham bid or proposal; (3) Contractor did not directly or indirectly induce or

solicit any other person, firm or corporation to refrain from bidding; and (4) Contractor did not seek by collusion to secure any advantage over the other bidders or proposers.

10.5 Hiring City Employees. This Contract shall be unilaterally and immediately terminated by City if Contractor employs an individual who within the twelve (12) months immediately preceding such employment did in his/her capacity as a City officer or employee participate in negotiations with or otherwise have an influence on the selection of Contractor.

ARTICLE XI
DISPUTE RESOLUTION

11.1 Mediation. If a dispute arises out of or relates to this Contract and cannot be settled through normal contract negotiations, Contractor and City shall use mandatory non-binding mediation before having recourse in a court of law.

11.2 Selection of Mediator. A single mediator that is acceptable to both parties shall be used to mediate the dispute. The mediator will be knowledgeable in the subject matter of this Contract, if possible.

11.3 Expenses. The expenses of witnesses for either side shall be paid by the party producing such witnesses. All other expenses of the mediation, including required traveling and other expenses of the mediator, and the cost of any proofs or expert advice produced at the direct request of the mediator, shall be borne equally by the parties, unless they agree otherwise.

11.4 Conduct of Mediation Sessions. Mediation hearings will be conducted in an informal manner and discovery will not be allowed. The discussions, statements, writings and admissions will be confidential to the proceedings (pursuant to California Evidence Code sections 1115 through 1128) and will not be used for any other purpose unless otherwise agreed by the parties in writing. The parties may agree to exchange any information they deem necessary. Both parties shall have a representative attend the mediation who is authorized to settle the dispute, though City's recommendation of settlement may be subject to the approval of the Mayor and City Council. Either party may have attorneys, witnesses or experts present.

11.5 Mediation Results. Any agreements resulting from mediation shall be memorialized in writing. The results of the mediation shall not be final or binding unless otherwise agreed to in writing by the parties. Mediators shall not be subject to any subpoena or liability, and their actions shall not be subject to discovery.

ARTICLE XII
MANDATORY ASSISTANCE

12.1 Mandatory Assistance. If a third party dispute or litigation, or both, arises out of, or relates in any way to the services provided to the City under a Contract, Contractor , its agents, officers, and employees agree to assist in resolving the dispute or litigation upon City’s request. Contractor’s assistance includes, but is not limited to, providing professional consultations,

attending mediations, arbitrations, depositions, trials or any event related to the dispute resolution and/or litigation.

12.2 Compensation for Mandatory Assistance. City will compensate Contractor for fees incurred for providing Mandatory Assistance. If, however, the fees incurred for the Mandatory Assistance are determined, through resolution of the third party dispute or litigation, or both, to be attributable in whole, or in part, to the acts or omissions of Contractor, its agents, officers, and employees, Contractor shall reimburse City for all fees paid to Contractor, its agents, officers, and employees for Mandatory Assistance.

12.3 Attorneys' Fees Related to Mandatory Assistance. In providing City with dispute or litigation assistance, Contractor or its agents, officers, and employees may incur expenses and/or costs. Contractor agrees that any attorney fees it may incur as a result of assistance provided under Section 12.2 are not reimbursable.

ARTICLE XIII
MISCELLANEOUS

13.1 Headings. All headings are for convenience only and shall not affect the interpretation of this Contract.

13.2 Non-Assignment. Contractor may not assign the obligations under this Contract, whether by express assignment or by sale of the company, nor any monies due or to become due under this Contract, without City's prior written approval. Any assignment in violation of this paragraph shall constitute a default and is grounds for termination of this Contract at the City's sole discretion. In no event shall any putative assignment create a contractual relationship between City and any putative assignee.

13.3 Independent Contractors. Contractor and any subcontractors employed by Contractor are independent contractors and not agents of City. Any provisions of this Contract that may appear to give City any right to direct Contractor concerning the details of performing or providing the goods and/or services, or to exercise any control over performance of the Contract, shall mean only that Contractor shall follow the direction of City concerning the end results of the performance.

13.4 Subcontractors. All persons assigned to perform any work related to this Contract, including any subcontractors, are deemed to be employees of Contractor, and Contractor shall be directly responsible for their work.

13.5 Covenants and Conditions. All provisions of this Contract expressed as either covenants or conditions on the part of City or Contractor shall be deemed to be both covenants and conditions.

13.6 Compliance with Controlling Law. Contractor shall comply with all applicable local, state, and federal laws, regulations, and policies. Contractor's act or omission in violation of applicable local, state, and federal laws, regulations, and policies is grounds for contract

termination. In addition to all other remedies or damages allowed by law, Contractor is liable to City for all damages, including costs for substitute performance, sustained as a result of the violation. In addition, Contractor may be subject to suspension, debarment, or both.

13.7 Governing Law. The Contract shall be deemed to be made under, construed in accordance with, and governed by the laws of the State of California without regard to the conflicts or choice of law provisions thereof.

13.8 Venue. The venue for any suit concerning solicitations or the Contract, the interpretation of application of any of its terms and conditions, or any related disputes shall be in the County of San Diego, State of California.

13.9 Successors in Interest. This Contract and all rights and obligations created by this Contract shall be in force and effect whether or not any parties to the Contract have been succeeded by another entity, and all rights and obligations created by this Contract shall be vested and binding on any party's successor in interest.

13.10 No Waiver. No failure of either City or Contractor to insist upon the strict performance by the other of any covenant, term or condition of this Contract, nor any failure to exercise any right or remedy consequent upon a breach of any covenant, term, or condition of this Contract, shall constitute a waiver of any such breach of such covenant, term or condition. No waiver of any breach shall affect or alter this Contract, and each and every covenant, condition, and term hereof shall continue in full force and effect without respect to any existing or subsequent breach.

13.11 Severability. The unenforceability, invalidity, or illegality of any provision of this Contract shall not render any other provision of this Contract unenforceable, invalid, or illegal.

13.12 Drafting Ambiguities. The parties acknowledge that they have the right to be advised by legal counsel with respect to the negotiations, terms and conditions of this Contract, and the decision of whether to seek advice of legal counsel with respect to this Contract is the sole responsibility of each party. This Contract shall not be construed in favor of or against either party by reason of the extent to which each party participated in the drafting of the Contract.

13.13 Amendments. Neither this Contract nor any provision hereof may be changed, modified, amended or waived except by a written agreement executed by duly authorized representatives of City and Contractor. Any alleged oral amendments have no force or effect. The Purchasing Agent must sign all Contract amendments.

13.14 Conflicts Between Terms. If this Contract conflicts with an applicable local, state, or federal law, regulation, or court order, applicable local, state, or federal law, regulation, or court order shall control. Varying degrees of stringency among the main body of this Contract, the exhibits or attachments, and laws, regulations, or orders are not deemed conflicts, and the most stringent requirement shall control. Each party shall notify the other immediately upon the identification of any apparent conflict or inconsistency concerning this Contract.

13.15 Survival of Obligations. All representations, indemnifications, warranties, and guarantees made in, required by, or given in accordance with this Contract, as well as all continuing obligations indicated in this Contract, shall survive, completion and acceptance of performance and termination, expiration or completion of the Contract.

13.16 Confidentiality of Services. All services performed by Contractor, and any sub-contractor(s) if applicable, including but not limited to all drafts, data, information, correspondence, proposals, reports of any nature, estimates compiled or composed by Contractor, are for the sole use of City, its agents, and employees. Neither the documents nor their contents shall be released by Contractor or any subcontractor to any third party without the prior written consent of City. This provision does not apply to information that: (1) was publicly known, or otherwise known to Contractor, at the time it was disclosed to Contractor by City; (2) subsequently becomes publicly known through no act or omission of Contractor; or (3) otherwise becomes known to Contractor other than through disclosure by City.

13.17 Insolvency. If Contractor enters into proceedings relating to bankruptcy, whether voluntary or involuntary, Contractor agrees to furnish, by certified mail or electronic commerce method authorized by the Contract, written notification of the bankruptcy to the Purchasing Agent and the Contract Administrator responsible for administering the Contract. This notification shall be furnished within five (5) days of the initiation of the proceedings relating to bankruptcy filing. This notification shall include the date on which the bankruptcy petition was filed, the identity of the court in which the bankruptcy petition was filed, and a listing of City contract numbers and contracting offices for all City contracts against which final payment has not been made. This obligation remains in effect until final payment is made under this Contract.

13.18 No Third Party Beneficiaries. Except as may be specifically set forth in this Contract, none of the provisions of this Contract are intended to benefit any third party not specifically referenced herein. No party other than City and Contractor shall have the right to enforce any of the provisions of this Contract.

13.19 Actions of City in its Governmental Capacity. Nothing in this Contract shall be interpreted as limiting the rights and obligations of City in its governmental or regulatory capacity.

Armor | City of San Diego – Response File

May 2024

Prepared by Armor
(US) +1 877 262 3473
(UK) +44 800 500 3167
www.armor.com

Armor Legal Notice

This document is disclosed only to the recipient to whom this document is addressed and is pursuant to a relationship of confidentiality under which the recipient has obligations to confidentiality. The recipient, by its receipt of this document, acknowledges that this document is confidential information and contains proprietary information belonging to Armor Defense Inc. and Armor Defense Ltd. ("Armor") and further acknowledges its obligation to comply with the provisions of this notice.

This proposal and the information contained herein is to be used by the recipient only for the purpose for which this document is supplied. The recipient must obtain Armor's written consent before the recipient or any other person acting on its behalf, communicate any information on the contents or the subject matter of this document or part thereof to any third party. The third party to whom the communication is made includes individual, firm or company or an employee or employees of such a firm and company.

Due to the dynamic nature of the industry and the technology that it depends upon, Armor makes no warranty as to the long-term accuracy of the assessments made herein. OTHER THAN THE WARRANTIES EXPRESSLY SET FORTH IN THE AGREEMENT BETWEEN YOU AND ARMOR FOR THE ARMOR SERVICES, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ARMOR DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, CONCERNING OR RELATED TO THIS PROPOSAL, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, PERFORMANCE, RESULTS, TITLE, NON-INFRINGEMENT AND THOSE ARISING BY STATUTE OR OTHERWISE IN LAW OR FROM A COURSE OF DEALING OR USAGE OF TRADE.

Executive Summary

Armor, the leading Cloud Security-as-a-Service (SECaaS) provider for public, private, and hybrid cloud solutions presents a comprehensive proposal for the protection of City of San Diego's systems, applications, and critical information assets. Armor's comprehensive approach to cloud and hybrid-based cybersecurity provides a full stack of security capabilities backed by a world-class security operations center (SOC). Armor's comprehensive SOC provides real-time security analysis and detection as well as advanced capabilities including monitoring, threat hunting, threat intelligence, and incident response services.

Designed for resilience, Armor Enterprise Cloud provides continuous compliance, active protection, and fast remediation to cybersecurity risks. Includes a unified self-service portal and APIs make integration easy with your service. In the rare event of a compromise, our cyber-insured solution mitigates and isolates the threat in less than one (1) day on average, minimizing data loss, theft, and preventing lateral movement. Additionally, we include our 24/7/365 Armor Enterprise Support and Security Response Teams.

Armor has been City of San Diego's valued partner for four (4) years and currently provides City of San Diego with our fully managed, turnkey PCI compliant cloud hosting solution. Armor team respectfully submits our response to bid for Payment Card Industry (PCI) Compliant Cloud Hosting Services 10090089-24-S.

Solution includes Armor GRC|P team to assist with PCI Compliance. City of San Diego inherits controls from Armor PCI DSS 4.0 Report on Compliance (ROC). Armor has over 15 years of experience delivering solutions to customers that have significant security and compliance requirements.

About Armor

WE HELP COMPANIES AROUND THE GLOBE FAST-TRACK THEIR CLOUD SECURITY

By taking a proactive approach to cybersecurity in cloud, hybrid, and on-premise environments, we protect data workloads, applications, and critical information assets. We do this by integrating hard-to-find security talent, best-of-breed security technologies and proven battle-tested cybersecurity techniques. Armor's unique value is how we abstract tools into capabilities – letting the client focus on what's important rather than managing tools, licenses, features, and security infrastructure – to deliver an effective fast-track to addressing cloud security needs.

Our unique, full-stack SECaaS approach is powered by our proprietary threat prevention and response platform and backed by decades of cyber threat intelligence and research by our highly experienced security teams. Security leaders suffer from tool fatigue, so Armor bundles critical security capabilities with advanced services your business needs to deliver a truly industry-unique experience. Armor's solution is natively built to protect, detect, and respond to threats both in real-time and as new threats are identified over time.

As a born-in-the-cloud cybersecurity services company, we provide the services, talent and visibility needed to protect you in any environment. And the standard we've set for managed cloud security is simply unmatched.

Armor Defense Inc.
7700 Windrose Ave. #G300
Plano, TX 75024

Armor Service Level Agreement

This Service Level Agreement ("SLA") outlines Armor's commitments ("Service Commitment") for (i) the end-to-end uptime for the Armor Enterprise Cloud Services ("Armor Enterprise Cloud") and (ii) critical security incident notifications for both the Armor Anywhere Services ("Anywhere Services") and Armor Enterprise Cloud Services, and sets forth the respective remedies available if Armor fails to meet these Service Commitments. This SLA and the credits provided for below ("Service Credits") are Armor's only obligation and customer's only remedy for Armor's failure to meet Service Commitments. Capitalized terms not defined herein will have the same meaning as in the applicable regional Terms of Services Agreement between customer and Armor (the "Agreement").

The Service Commitments under this SLA are:

1. SECURITY INCIDENT NOTIFICATION GUARANTEE

This guarantee is only applicable to customers who utilize either the Complete Services or Anywhere Services (collectively, the "Services").

Armor guarantees that customers will be notified of a Critical Security Incident within fifteen (15) minutes of Armor's knowledge of a security incident ("Critical Incident Notification Time" or "CINT"). "CINT" is defined as the time period between Armor identifying a Critical Security Incident and the time stamp associated with Armor's initial notification to the customer of the Critical Security Incident.

A "Critical Security Incident" occurs when Armor has positively identified a security incident within the scope of the Services that may have a significant impact to the environment protected by Armor. Examples of Critical Security Incidents include, but are not limited to:

Successful brute force logins

Detection of threat escalation of root privileges or lateral movement

Post compromise activity such as outbound remote shell commands, attack tool downloads

Armor will initially notify the customer of a Critical Security Incident via a ticket in the Armor Management Portal. If Armor receives no response, it will use its best efforts to

notify customer's primary point of contact by telephone. Customer is responsible for ensuring that its contact information is up to date in the Armor Management Portal.

CINT Credits

If Armor does not meet the CINT, the customer will receive a credit equal to five percent (5%) of the applicable monthly service Fees for the applicable Services for the impacted account(s). Armor will apply the CINT Credits only against future payments otherwise payable by the customer for the applicable Services. The total cumulative CINT Credits claimed by the customer in any given month shall not exceed the amount owed by the customer for the applicable Services during that month.

CINT Credit Claims

All CINT Credit claims should be communicated via a ticket in the Armor Management Portal within seven (7) calendar days of the incident giving rise to the claim. The ticket must include all relevant information, including, but not limited to the impacted server(s), the date, time and full description of the incident and any logs (if applicable). The customer's failure to provide the request and other information as required above will disqualify the customer from receiving a CINT Credit.

To be eligible to make a CINT Credit claim, customer must use its best efforts to maintain a secure environment with hardened and patched applications and configurations, and to follow best security practices as recommended by Armor. Customer is expected to be responsive to the Armor Management Portal and phone notifications, and to take immediate action as required to bring a Critical Security incident to closure.

To qualify for CINT Credit(s), customer (i) must be a Complete Services or Anywhere Services customer, (ii) cannot be ninety (90) or more days past due on payment to Armor, and (iii) must be in compliance with the Agreement for the Services and with Armor's Acceptable Use Policy.

2. 'END-TO-END' INFRASTRUCTURE UPTIME GUARANTEE

This guarantee is only applicable to customers who utilize the Armor Enterprise Cloud Services.

Armor guarantees an end-to-end uptime availability of 99.99% for the Armor Enterprise Cloud Services. The "layers" and services needed to ensure the uptime of the Armor Enterprise Cloud Services are:

Physical Infrastructure (all power and HVAC infrastructure, including UPS, PDU and cabling)

Armor Infrastructure (the Armor Network, firewalls, virtual firewall platform and infrastructure log collection devices)

Storage Platform (includes all LUN(s), SAN Fabric, SAN Switches, and SAN Data drive availability)

Compute Platform (includes all physical hosts and virtualization software)

Operations within the Armor Enterprise Cloud Services (e.g., operating system and customer provided software) or within other services offered by Armor are excluded from this guarantee. For purposes of this SLA, the "Armor Network" is defined as the provision of access by Armor to the Armor internal boundary to the Internet, as well as the internal network serving the front-end secure cloud hosting environment.

The following are excluded from this guarantee:

The backend Armor-only management network;

Routing anomalies, asymmetries, inconsistencies and failures of the Internet outside of Armor's control;

Maintenance events as defined below;

Customer instructed or requested actions, whether performed by the customer, Armor, or a third party, that impacts the availability of the Services

Armor proactively monitors infrastructure uptime. The results of these monitoring systems are the exclusive determination of Armor Enterprise Cloud Services uptime. Not more than once a month and upon request via the Armor Management Portal, Armor will provide customer with these results.

Service Credits

If Armor does not meet the "End to End Infrastructure Uptime Guarantee" (excluding Scheduled and Emergency maintenance as defined below), Armor will provide the following Service Credits:

Length of Downtime	Payment of Applicable Monthly Service Fees Impacted Services
>5 minutes – 45 minutes	10%
>45 minutes – 7 hours	20%
>7hours	50%

The payment of Service Credits will be based solely on the Fees for the Armor Enterprise Cloud Services for the month in which the claim arises and only for the impacted account(s) for the Armor Enterprise Cloud Services. Armor will only apply the Service Credits against future Armor Enterprise Cloud Services payments otherwise payable by the customer. The payment for any single failure shall not exceed fifty percent (50%) of the monthly service Fees for the impacted components of the Armor Enterprise Cloud Services. The total cumulative Service Credits claimed by the customer in any given month shall not exceed the amount owed by the customer for the Armor Enterprise Cloud Services during that month.

No Service Credits will be given for service interruptions: (i) caused by the action or failure to act by customer, customer's personnel, or any of customer's Users, (ii) due to failure of any equipment or software provided by customer, (iii) which are the result of Scheduled or Emergency Maintenance, (iv) due to a force majeure event, (v) for which customer is entitled to a Service Credit for the same or contemporaneous Service Commitment failure, (vi) for downtime or other problems that may result from customer's use of the Beta Services, as defined in customer's Agreement with Armor, (vii) to the extent Armor offers customer a Self-Service Option and that results from customer's use of a Self-Service Option, or (viii) that occurs while customer is subject to any suspension action taken by Armor pursuant to customer's Agreement with Armor.

Service Credit Claims

All Service Credit claims should be communicated via a ticket in the Armor Management Portal within seven (7) calendar days of the incident giving rise to the claim. The ticket must include all relevant information, including but not limited to the impacted server(s), the date, time and full description of the incident and any logs (if applicable).

To be eligible to make a Service Credit claim, customer must use its best efforts to maintain a secure environment with hardened and patched applications and configurations, and to follow best security practices as recommended by Armor. Customer is expected to be responsive to the Armor Management Portal and phone notifications, and to take immediate action as required.

(V) To qualify for Service Credit(s), customer (i) must be a Armor Enterprise Cloud Services customer, (ii) cannot be ninety (90) or more days past due on payment to Armor, and (iii) must be in compliance with its Agreement for the Armor Enterprise Cloud Services and Armor's Acceptable Use Policy.

Maintenance Exceptions

Scheduled Maintenance

Armor may from time to time conduct routine tests, maintenance, upgrades or repairs on any part of its networks, infrastructure, or the Services ("Scheduled Maintenance") and will use commercially reasonable efforts to provide prior notice (including at least fourteen (14) days' prior notice for customer-impacting maintenance). Armor will seek to perform scheduled maintenance outside of the business hours of the relevant data center (defined as Monday to Friday 09:00 to 18:00 of the time zone of the relevant datacenter).

Emergency Maintenance

In some instances, it may not be practical for Armor to give advance notice of maintenance, for example, in the event of an unforeseen disruption of service ("Emergency maintenance"). In these cases, Armor has the right to disrupt Services without prior notice.

"Maximum Time to Resolution" means the time span listed in the table below under the heading "Maximum Time to Resolution".

"Service Credit" means the monetary credit that Armor will credit to a Customer's eligible account, the calculation of which is provided in the tables below for each of the following scenarios:

the Actual Monthly Uptime Percentage is less than the Monthly Uptime Percentage Threshold;

the Actual Time to Resolution for any incident is greater than the Maximum Response Time value corresponding to the priority of that incident; or

the Actual Initial Response Time for any incident is greater than the Maximum Initial Response Time value corresponding to the priority of that incident.

For any and all scenarios, the total Service Credit amount shall not exceed the price paid by you for the Services. Service Credit amounts will be the lesser of the calculated amount based on the calculations provided below or the invoiced amount of the affected Services for the service period in which the SLA claim is being made.

"Business Days" means Monday through Friday in Central Standard/Daylight Time.

"Service Level Objective" (or "SLO") means a performance target which Armor strives to satisfy, but for which no Service Credit is payable should it be breached.

Service Availability

Applicable Services	Monthly Uptime Percentage Threshold	Service Credit
Armor Service Management APIs	99.99%	10% credit equivalent
Armor Service Management Console	99.99%	10% credit equivalent

Incident Response

Incident Priority	Maximum Initial Response Time	Maximum Update Interval	Maximum Time to Resolution[1]	Service Credit
Critical	15 minutes	30 minutes	8 hours	10% credit equivalent
High	1 hour	4 hours	1 day	10% credit equivalent
Medium	8 hours	1 day	2 days	SLO-only (0%)
Low	24 hours	As needed (∞)	7 days	SLO-only (0%)

[1] In the context of this SLA, an incident is considered as having a resolution when the priority of the incident has been downgraded because there is no longer an active threat, or it has been resolved.

3. Service Commitments

If, during any month throughout the Term, the Actual Monthly Uptime Percentage falls below the Monthly Uptime Percentage Threshold, then Customer will be eligible to receive a Service Credit, subject to Customer's compliance with Section 4 below.

If, at any time throughout the Term, any of the Customer's incidents' Actual Time to Resolution exceeds the Maximum Time to Resolution, then Customer will be eligible to receive a Service Credit, subject to Customer's compliance with Section 4 below.

If, at any time throughout the Term, any of the Customer's incidents' Actual Update Interval exceeds the Maximum Update Interval, then Customer will be eligible to receive a Service Credit, subject to Customer's compliance with Section 4 below.

If, at any time throughout the Term, any of the Customer's incidents' Actual Initial Response Time exceeds the Maximum Initial Response Time, then Customer will be eligible to receive a Service Credit, subject to Customer's compliance with Section 4 below.

4. Credit Request and Payment Procedures

To receive a Service Credit for Services, Customer must submit a request to Armor through the Armor Management Portal, available at https://amp.armor.com/, within thirty (30) days from the last day of the calendar month in which Customer claims Armor failed to meet or exceed any Service Commitments. Availability of Armor's Services are measured by a third party provider of performance and monitoring services (the "Monitoring Service"), that issues uptime reports, available at https://status.armor.com/. Armor will adjust the Monitoring Service's uptime results as necessary to account for any Excluded Monthly Times. All submissions must include:

"SLA Claim" as the subject of the ticket;

the dates and times of Unavailable Monthly Time (for service availability claims)

the incident ID for which a claim is being made (for incident response claims)

Each Service Credit will be applied to future amounts payable by Customer to Armor for the Services. No refunds or cash value will be given. Should an SLA claim be made after the Term of the Customer's contract, but otherwise in compliance with the other requirements listed in this section, a credit balance will be kept for the Customer for any subsequent contract terms.

5. Planned and Emergency Maintenance

From time to time, Armor may be required to perform periodic planned or emergency maintenance including, without limitation, feature updates, bug fixes, and security patches. Armor will notify you of any maintenance period in which interruptions of Services are expected. Notifications will be based on the preferences you've configured and are additionally available at https://status.armor.com/.

Armor will strive to provide notifications to Customers with sufficient advanced warning on an SLO-only basis, with the following targets:

Maintenance Type	Notification Target
Planned Maintenance	3 Business Days
Emergency Maintenance	1 Business Day
Unplanned Fault Notification	2 hours

6. Excluded Monthly Times

Notwithstanding any provision in this Agreement to the contrary, no Unavailable Monthly Time will be deemed to have occurred if downtime:

is caused by factors outside of Armor's reasonable control, including, without limitation, telecommunications provider-related problems or issues, Internet access or related problems occurring beyond the point in the network where Armor maintains access and control over the Services, or cloud service provider-related problems or issues;

results from any actions or inactions of Customer or any third party (except for Armor's agents and subcontractors);

is caused by applications, equipment, or other technology provided by the Customer or any third party;

occurs during any maintenance period described in Section 5;

results from the use of alpha, beta, developer preview, or otherwise non-production features of the Services; or

periods of Unavailable Monthly Time that are less than five (5) minutes of continuous unavailability in duration; collectively, the "Excluded Monthly Times".

EXHIBIT D: Price Proposal

The City of SAN DIEGO

	One-Time	Monthly Fee per Unit	Unit Quantity	Year 1	Year 2	Year 3	Option Year 4	Option Year 5	Proposer Comments *(highlight assumptions if any)*
Armor Defense Inc.									
Section 1: Licensing and Maintenance Costs									
Windows Servers									
Windows 2022, 2 CPUs, 8GB RAM, 60GB Storage (Total Cost based on 2 servers*)	$0.00	$300.00	2	$7,200.00	$7,200.00	$7,200.00	$7,200.00	$7,200.00	All storage utilizes SSD in HA configuration
Windows 2022, 4 CPUs, 16GB RAM, 160GB Storage (Total Cost based on 1 server)	$0.00	$725.00	1	$8,700.00	$8,700.00	$8,700.00	$8,700.00	$8,700.00	All storage utilizes SSD in HA configuration
Windows 2022, 4 CPUs, 16GB RAM, 110GB Storage (Total Cost based on 1 server)	$0.00	$640.00	1	$7,680.00	$7,680.00	$7,680.00	$7,680.00	$7,680.00	All storage utilizes SSD in HA configuration
Option A Total Costs	**$0.00**			**$23,580.00**	**$23,580.00**	**$23,580.00**	**$23,580.00**	**$23,580.00**	
Linux Servers									
Red Hat Enterprise Linux 7, 2 CPUs, 8 GB RAM, 30GB Storage (Total Cost based on 2 servers*)	$0.00	$170.00	2	$4,080.00	$4,080.00	$4,080.00	$4,080.00	$4,080.00	All storage utilizes SSD in HA configuration
Red Hat Enterprise Linux 7, 2 CPUs, 16 GB RAM, 30GB Storage (Total Cost based on 1 server)	$0.00	$290.00	1	$3,480.00	$3,480.00	$3,480.00	$3,480.00	$3,480.00	All storage utilizes SSD in HA configuration
Red Hat Enterprise Linux 7, 4 CPUs, 8 GB RAM, 30GB Storage (Total Cost based on 4 servers*)	$0.00	$190.00	4	$9,120.00	$9,120.00	$9,120.00	$9,120.00	$9,120.00	All storage utilizes SSD in HA configuration
Option B Total Costs	**$0.00**			**$16,680.00**	**$16,680.00**	**$16,680.00**	**$16,680.00**	**$16,680.00**	
Section 2: Implementation and Transition Costs									
Implementation and Transition Costs									
Cost	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	No additional costs associated to these services
Total Implementation and Training Costs	**$0.00**			**$0.00**	**$0.00**	**$0.00**	**$0.00**	**$0.00**	No additional costs associated to these services
Section 3: Other Additional Costs									
Backup Services	$0.00	$15.00	11	$1,980.00	$1,980.00	$1,980.00	$1,980.00	$1,980.00	
Recovery Services	$0.00	$190.91	11	$25,200.00	$25,200.00	$25,200.00	$25,200.00	$25,200.00	Note that the per unit cost is the average monthly fee for Replication Service
Log Management/Retention (13-month Retention)	$0.00	$100.00	11	$13,200.00	$13,200.00	$13,200.00	$13,200.00	$13,200.00	
PCI Vulnerability Scanning Services	$0.00	$150.00	1	$1,800.00	$1,800.00	$1,800.00	$1,800.00	$1,800.00	
IP Allocations (Total Cost based on 13 IP Allocations*)	$0.00	$5.00	12	$720.00	$720.00	$720.00	$720.00	$720.00	Note that the first public IP is provided at no charge
Misc. Premium Support	$0.00	$3,000.00	1	$36,000.00	$45,000.00	$54,000.00	$63,000.00	$72,000.00	Support fee to increase each year by 25% (No other line item fee changes)
Load Balancing	$0.00	$1,000.00	1	$12,000.00	$12,000.00	$12,000.00	$12,000.00	$12,000.00	
SSL VPN Accounts (Total Cost based on 10 Accounts*)	$0.00	$25.00	9	$2,700.00	$2,700.00	$2,700.00	$2,700.00	$2,700.00	Note that the first SSL VPN account is provided at no charge

EXHIBIT D: Price Proposal

	One-Time	Monthly Fee per Unit	Unit Quantity	Year 1	Year 2	Year 3	Option Year 4	Option Year 5	Proposer Comments *(highlight assumptions if any)*
Intelligent Security Model Per VM Fee to include the following services: File Integrity Monitoring Malware Host based IDS/IPS Patch Management IP Reputation Management Network Firewall DDoS Mitigation Multi Authentication Management Disk Encryption at the SAN Storage Layer Vulnerability Monitoring and Reporting Security Operations Center 24/7 Monitoring and Incident Response VMs deployed with Hardened OS using CIS Benchmarks Reporting and Dashboards provided via Armor Managment Portal	$0.00	$600.00	11	$79,200.00	$79,200.00	$79,200.00	$79,200.00	$79,200.00	
Other (please describe)	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	
Other (please describe)	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	
Other (please describe)	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	
Other (please describe)	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	
Other (please describe)	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	
Other (please describe)	$0.00			$0.00	$0.00	$0.00	$0.00	$0.00	
Other Additional Costs Total	$0.00			$172,800.00	$181,800.00	$190,800.00	$199,800.00	$208,800.00	Support fee increase will result in a YoY increase of total fees of approximately 5.2%
Sum for Summary Sheet	**$0.00**			**$213,060.00**	**$222,060.00**	**$231,060.00**	**$240,060.00**	**$249,060.00**	0.052083333
									$17,755.00
Total Contract Cost of Ownership					**$1,155,300.00**				

Contract Term:

As may be required for a period of three (3) years from the Effective Date, with an option to renew of up to two (2) additional one (1) year periods.

EXHIBIT D: Optional Services

	One-Time	Year 1	Year 2	Year 3	Year 4 (Option Year 1)	Year 5 (Option Year 2)	Proposer Comments
Optional Services (will not be included in cost evaluation)							
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Optional Module/Service (provide description and details)	$ -	$ -	$ -	$ -	$ -	$ -	
Other	$ -	$ -	$ -	$ -	$ -	$ -	

Hourly Rates for Additional Service Requests (will not be included in cost evaluation)		
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*
Title 1 (*e.g. Consultant, Project Manager, Developer, Teste* r)	$0.00	*Please include title and responsibilities*

1	Go to the "IT City Standards" tab and choose "Fully Compliant", "Partially Compliant", "Not Compliant", or "NA" for each line item.
2	Provide a complete explanation of how, specifically, the solution does (or does not) comply. Please describe, in detail, how solution does (or does not) comply.
3	If not fully compliant, please provide proposed workarounds, planned updates (with timelines), or alternatives, as available (and associated costs, as applicable). For non-applicability of a standard, please provide explanation / justification.
4	If there are any additional costs associated w/ proposed workarounds or alternatives, they must be explicity provided herein, and they must be provided in the Pricing Pages, as well.
5	Next, go to the "Technical Alignment" tab and answer each question.

*** * * Requests for exceptions to IT City Standards must be listed as exceptions (as outlined in Exhibit A of the RFP) * * ***
*** * Exceptions to IT City Standards will require approval by the City's Department of Information Technology * ***

City of San Diego - Armor Defense Inc.

IT City Standards for Solicitations - Rev. 2024.01 (reflects Governance Rev. 2023.06)

ID	City Requirement	Level of Compliance *(select in the dropdown)*	*Describe, in detail, how solution does (or does not) comply. If not fully compliant, please provide proposed workarounds, planned updates (with timelines) or alternatives, as available (and associated costs, as applicable). If you believe this City standard requirement to be non-applicable, provide explanation / justification.*
AS	**Application Security**		
The following Application Security requirements shall apply:			
AS-1	**System User Authentication.** Web authentication must be integrated into City's OKTA SSO via Security Assertion Markup Language (SAML) 2.0 and OpenID Connect (OIDC). Application must ensure user session automatically logs out upon twenty (20) minutes of user inactivity.	***Partially Compliant***	***Armor's Management Portal utilizes OKTA and automatically logs out upon ten (10) minutes of user inactivity. Due to the Secure nature of the platform, integration into City's OKTA SSO is not available at the time of writing.***
AS-2	**Secure Authentication.** All authentication activity occurring over the network must be encrypted using industry best practices to ensure that logins and passwords are not transmitted in clear text. This includes System User and administrator authentication activity.	***Fully Compliant***	***The solution uses secure authentication with encryption and enhances security with Multi-factor User/Group Admin Management, seamlessly integrated into the Armor Management Portal. This feature ensures an added layer of protection by requiring multi-factor authentication for user and group administration, contributing to a resilient cybersecurity posture.***
AS-3	**Encryption.** Application must support industry standard methods, and at a minimum secure, modern algorithm for the encryption of Sensitive Data in transit to/from the host/server system, at rest within storage subsystem(s), and client computer(s), and must use most recent secure versions of encryption protocols such as SSL, TLS, or Secure FTP.	***Fully Compliant***	***Data is encrypted at rest and in motion and meets HIPAA standards. Armor maintains HITRUST r2 certifications as evidence of HIPAA compliance.***
AS-4	**System Sharing**. Application must not permit the transmission of City data beyond the approved City domains sandiego.gov and sannet.gov.	***Fully Compliant***	***Armor Enterprise Cloud is independent of City domains sandiego.gov and sannet.gov***
AS-5	Protection of Sensitive Information and Data. Proposer, its agents, employees, contractors and any other person or entity working on behalf of Proposer to provide services under this proposal must at all times comply with City of San Diego Administrative Regulation (A.R. 90.64) “Protection of Sensitive Information and Data”.	***Fully Compliant***	***See attached signed Exhibit I***
AS-6	**Auditing and Logging.** Application must support interoperability with, and stream logs to the City’s centralized Sumo Logic Security Information and Event Management (SIEM) platform for, at a minimum, all security related events including logon, logoff, data modification, data deletion, change in rights or permission levels, and the addition of data/information to the application. Logs must include user ID generating the transaction, time of the transaction and details regarding the activity (e.g. logon, logoff or data details).	***Partially Compliant***	***Armor Enterprise Cloud includes a Log Management and a SIEM within the Platform, which actively gathers, analyzes, and responds to log data from servers and networks. Within the service Armor provides continuous monitoring and customizable alerts, with Armor's Log Management ensuring a comprehensive and proactive approach to handling security incidents, reinforcing a robust cybersecurity framework for hosted infrastructure and data. Streaming logs to the City's SIEM is not supported at this time.***
AS-7	Compliance with Organization’s Security Policy, Standards and Procedures. Solution Proposer working directly on City-owned applications or from City facilities are subject to and required to follow all City policies, standards and guidelines. Proposer must also follow FIPS 140-2 standards which can be viewed at https://csrc.nist.gov/publications/detail/fips/140/2/final. For FIPS-140-2 the City requires Level 2 compliance; the City requires at least role based authentication for access to this application.	***Fully Compliant***	***Solution provides for identity and role-based operator authentication. Cryptography options.***

AS-8	**Data Integrity.** The Solution must ensure the integrity of all the data collected, stored and processed. Interruptions in processing due to incidents such as aborted transactions, hardware failures, or network unavailability must not result in inaccurate or inconsistent data stored and/or processed in the Application. If data transfers occur, the Application must provide a method of audit validation to ensure that all data sent to it was received and processed correctly.	***Fully Compliant***	***Armor Enterprise Cloud can provide Data Integrity with Armor Encryption Options. The basic model consists of an agent and a provisioned key management system (Data Security Manager). The Data Security Manager is a virtual appliance that provides centralized encryption key and policy management for all Encryption Expert Agents installed on servers across the customers infrastructure. The Data Security Manager can also provide enterprise data security and encryption management for Transparent Data Encryption from Oracle and Microsoft SQL Server databases as well as providing storage for any other encryption keys.***
AS-9	**Error Messages.** Errors must be handled in an appropriate manner. Failed login attempts to the Application must not display detailed information about the failed login attempt (e.g. incorrect password or unknown System User account). Other security related errors (e.g. file not found or permission denied) must generate generic error responses. Detailed error information must be written to secure logs so that developers and system administrators have access to error details required to address the error.	***Fully Compliant***	***Security Logs are ingested into Armor Cloud Security Platform which backed by Armor's 24/7 Security Operations Center. Error Messages from any Applications deployed / developed by City onto instances within Armor Enterprise Cloud will be the responsibility of City to ensure generation of generic error responses and detailed error information is written.***
AS-10	**Logical Data Separation**. In the instances of a shared-hosting environment, including, but not limited to, shared hardware, processing, platform, application instance, software code and architecture, and security controls, Vendor must ensure that City data is logically separated from third-parties to ensure no leakage of City data occurs.	***Fully Compliant***	***Armor Enterprise Cloud provides logical separation within the platform. Firewall Rules within Armor Enterprise Cloud can be added / deleted / modified by the first City Administrator deployed and any subsequent Users setup by the first Administrator and provided that permission. Armor Encryption can also be deployed to safeguard data at rest within the virtual hosting infrastructure. This offering encompasses file and folder encryption as well as a centralized key management system. The solution can be deployed as a FIPS level 1 virtual machine, or a hardware appliance co-located within a Armor Datacenter to obtain both FIPS level 2 and FIPS level 3 encryption standards.***
AS-11	**Sensitive Data**. Applications containing or hosting sensitive data, as defined by State or Federal law, must encrypt data at rest, data in motion over the network and all authentication activity. Encryption algorithm used to encrypt data and authorization activity must meet HIPAA standards and be encrypted as NIST FIPS 140-2 compliant.	***Fully Compliant***	***Data is encrypted at rest and in motion and meets HIPAA standards. Armor maintains HITRUST r2 certifications as evidence of HIPAA compliance.***
AS-12	**Patching.** Application/Systems must be patched on, at a minimum, a monthly basis.	***Fully Compliant***	***Armor Enterprise Cloud Complies with the requirement providing Patch Monitoring and Patch Management as part of the service.***
AS-13	**Vulnerability Management**. Prior to product deployment into a production environment and/or external exposure, all Application, Service and Systems must be scanned, with an established industry-recognized tool and security vulnerability remediated. Vulnerabilities discovered on existing systems must be remediated within at least 30 days of discovery. Discovered vulnerabilities shall be assigned a risk ranking. High-rated vulnerabilities must be patched/remediated within 24 hours.	***Fully Compliant***	***Armor Enterprise Cloud Complies with the requirement providing Vulnerability and Policy Recommended Scanning as well as providing base OS image and subsequent vendor provided patches and updates.***
AS-14	**Mobile Device Management (MDM).** Mobile Devices e.g. tablets and mobile phones must be registered through DoIT's Security Team and Microsoft Intune MDM must be installed on those devices	***N/A***	Not applicable to Armor as proposed hosting vendor. (Mobile Devices are not part of Armor Enterprise Cloud)
AD	**Application Data**		
The following Application Data requirements shall apply:			

AD-1	**Ownership of Data**. All data collected on behalf of the City of San Diego is the property of the City. None of the data will be used for any other purpose. Upon termination or, expiration of any contractual agreement, the Proposer will retain the City's data for a minimum of ninety (90) days and will transfer City data in its possession to the City at no cost by using a method that protects the confidentiality of the information being exchanged and as agreed upon by the City but, at a minimum, data records will be provided in ASCII comma, separated value (CSV) format, with binary images in TIFF, JPG, or PDF format.	***Partially Compliant***	Please see Armor's Privacy Policy for details on data collected and purposes that may fall outside these expectations. https://www.armor.com/legal/privacy-policy
AD-2	**Personal Data.** Proposer agrees that it will comply with all applicable federal, state and local data protection laws and regulations in any relevant jurisdiction with respect to dealing with, disclosing and exchanging any Personal Data in connection with this Agreement. For the purpose of this Agreement, "Personal Data" means any personal identifying information including, but not limited to, customer's name, address, telephone number, social security number, and financial account numbers (including credit or debit card numbers and any related security codes or passwords).	***Fully Compliant***	Armor agrees to comply with all applicable federal, state and local data protection laws and regulations in any relevant jurisdiction with respect to dealing with, disclosing and exchanging any Personal Data in connection with this Agreement.
AD-3	**City Data Access.** If proposed Solution is sub-contracted and hosted by a third party, City owned data must be available to the City of San Diego. System User access and authorizations must be provided as directed by the City of San Diego.	***Fully Compliant***	Armor agrees that City owned data must be available to the City of San Diego.
AD-4	**Third Party Requirements**. Proposer will cause any third party sub-contractor to adhere to all data privacy and security requirements no less rigorous than those set forth in this RFP.	***Fully Compliant***	Armor will cause any third party sub-contractor to adhere to all data privacy and security requirements no less rigorous than those set forth in this RFP.
AD-5	**State Requirements.** Proposer is compliant with the California Consumer Privacy Act (CCPA).	***Partially Compliant***	Armor aligns with the California Consumer Privacy Act (CCPA), but has not undergone a compliance audit for validated assurance.
D	**Design**		
The following Design requirements shall apply:			
DD-1	**Design Documentation.** Proposer will provide design documentation, including but not limited to Process diagram, Interface/Integration diagram, and Infrastructure diagram.	***Fully Compliant***	Armor will provide topology and architecture diagram.
DD-2	**Architecture Documentation.** Proposer will provide architecture documentation, including but not limited to data flow diagram, data models, database schema and Entity-Relationship diagram.	***Fully Compliant***	Armor will provide topology and architecture diagram.
DHW	**Desktop Hardware**		
The following Desktop requirements shall apply:			
HWD-1	**System.** Compatible with 64 bit systems.	***N/A***	Not applicable to Armor as proposed hosting vendor.
HWD-2	**Desktop/Laptop Hardware**. Hewlett-Packard (HP) brand business-class.	***N/A***	Not applicable to Armor as proposed hosting vendor.
HWD-3	**Tablets**. HP ELITE X2 G4	***N/A***	Not applicable to Armor as proposed hosting vendor.
HWD-4	**Tablet/Laptop Combos**. MS Surface Pro 7, MS Surface Pro 7+	***N/A***	Not applicable to Armor as proposed hosting vendor.
DSW	**Desktop Software**		
The following Desktop requirements shall apply:			
SWD-1	**Desktop Operating System.** Microsoft Windows 10 Enterprise, or the most current version of this Operating System to within an n-1 standard.	***N/A***	Not applicable to Armor as proposed hosting vendor. (Desktop's are not part of Armor Enterprise Cloud)
SWD-2	**Desktop Software.** The proposed system must not conflict with, or modify standard desktop software. Other standard software includes: ESET Antivirus, Adobe Creative Cloud; SAPGUI. The City targets n-1 if not the latest updates.	***N/A***	Not applicable to Armor as proposed hosting vendor. (Desktop's are not part of Armor Enterprise Cloud)
SWD-3	**Office Productivity.** Microsoft Office Suite, Teams, Visio, Project	***N/A***	Not applicable to Armor as proposed hosting vendor. (Desktop's are not part of Armor Enterprise Cloud)

SWD-4	**Web Browser.** Google Chrome and Microsoft Edge Chromium or the current manufacturer's version to within an n-1 standard.	***N/A***	Not applicable to Armor as proposed hosting vendor. (Desktop's are not part of Armor Enterprise Cloud)
O-STD	**Other Applications Standards**		
The following Applications requirements shall apply:			
OSTD-1	**Programming Language Standards.** HTML5 (Web Presentment); Python (ESRI ArcGIS Script); ASP.net (Dynamic Web Pages); PHP; PowerShell (Windows Automation Scripting); Microsoft SQL Server Reporting Services (SSRS); Transact T-SQL (Database Programming Language); Microsoft .Net Responsive design.	***N/A***	Not applicable to Armor as proposed hosting vendor. (Any application deployments / development by City on the Armor Enterprise Cloud hardened Microsoft / Linux based OS's deployed will be City's responsibility to adhere to Programming Language Standards).
OSTD-2	**Data Transport Protocol Standards.** XML (includes JXDM); JSON; SOAP / HTTP / RESTful (web services); EDI; ACH; ESRI - File GeoDatabase; GeoJSON, DWG, DGN (CADD)	***N/A***	Not applicable to Armor as proposed hosting vendor. (Any application deployments / development by City on the Armor Enterprise Cloud hardened Microsoft / Linux based OS's deployed will be City's responsibility to adhere to Data Transport Protocol Standards).
OSTD-3	**Desktop Configuration.** Desktop components for any solution must be able to be pushed to the user via the City's Service Center Configuration Manager (SCCM) platform.	***N/A***	Not applicable to Armor as proposed hosting vendor. (Desktop's are not part of the Armor Enterprise Cloud Solution)
OSTD-4	**Reporting Tool Integration Standards.** SAP Crystal Reports; Microsoft SQL Server Reporting Services.	***N/A***	Not applicable to Armor as proposed hosting vendor. (City are able to adhere to the Reporting Tool Integration Standards and deploy SAP Crystal Reports / Microsoft SQL Server Reporting Services. if required)
OSTD-5	**Web Content Management System.** Drupal	***N/A***	Not applicable to Armor as proposed hosting vendor.
OSTD-6	**Document Management Integration.** OpenText.	***N/A***	Not applicable to Armor as proposed hosting vendor.
OSTD-7	**Geographic Information System and Integration Standards.** ESRI - ArcGIS Desktop; RouteSmart / ArcGIS Network Analyst.	***N/A***	Not applicable to Armor as proposed hosting vendor.
HSTD	**Hosting Standards**		
The following Hosting requirements shall apply:			
HSTD-1	**City Hyper Converged Infrastructure.** If solution is proposed as 'On Premise', it must support either:	***N/A***	Not applicable to Armor as proposed hosting vendor. Armor Enterprise Cloud is not 'On Premise'
HSTD-2	**Hyper Converged Infrastructure:** server, shared-storage, networking equipment, and software for infrastructure management. The City's standard Integrated Infrastructure Model is the VMWare Virtual Cloud Foundation.	***N/A***	Not applicable to Armor as proposed hosting vendor. Armor Enterprise Cloud is not 'On Premise'
HSTD-3	**Standalone server** – HP ProLiant Generation 10 or higher.	***N/A***	Not applicable to Armor as proposed hosting vendor. Armor Enterprise Cloud is not 'On Premise'
HSTD-4	**Server OS.** Solution must support Server Operating System – Microsoft Windows Server, SuSe Linux versions must be within N-1.	***Partially Compliant***	Windows, Ubuntu and RHEL OS's are supported within Armor Enterprise Cloud
HSTD-5	**Web Servers.** If proposed system is locally hosted, it must support web servers – Microsoft IIS and Apache to an n-1 standard.	***Fully Compliant***	Web Servers are supported and supports Microsoft IIS and Apache.
HSTD-6	**Virtual Servers.** Solution must support virtual server hosting – VMware ESX (to an n-1 standard).	***Fully Compliant***	Armor Enterprise Cloud supports Virtual Server Hosting (utilizing VMware)
HSTD-7	**Relational Database Management Systems.** If solution is proposed as 'On Premise', it must support Relational Database Management Systems (RDBMS) – Microsoft SQL Server version within N-1.	***Fully Compliant***	Microsoft SQL Server is supported within Armor's Enterprise Cloud
HSTD-8	**Cloud.** Providers are Amazon Web Services (AWS) , Microsoft Azure, and Google Cloud platform (GCP) with AWS being the preferred public cloud platform. Current services provided include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Microservices, Storage and Archiving. **Public Cloud** solutions must reside within the borders of the United States and support either Microsoft Azure, AWS or GCP. Private Cloud using Virtual Cloud Foundation or VMC on AWS are the Standards.	***Partially Compliant***	Armor is proposing Armor's Enterprise Cloud, which is a secure private cloud supporting Virtual Server Hosting (utilizing VMware) and Infrastructure as a Service (IaaS). Designed for resilience, Armor Enterprise Cloud provides continuous compliance, active protection, and fast remediation to cybersecurity risks, as well as adherence to Major Compliance Frameworks (including HIPPAA, PCI, SOC2 etc.).
END OF REQUIREMENTS			

City of San Diego - Armor Defense Inc.

IT Technical Alignment for Solicitations - Rev. 2023.11 (reflects Governance Rev. 2023.06)

Questions	Required Responses	Guidance/Instructions	Discipline
Is there any equipment being installed?	Not applicable to Armor as proposed hosting vendor.	If so, please include any network, infrastructure, or appliances equipment (including manufacture model, servers, etc.).	General
Will City need to receive GIS data?	No - This is not a requirement for Armor Enterprise Cloud	If ***yes*** , vendor will need to provide metadata to GIS team.	General
Who will be administrator of the application-Vendor or City?	The Armor Enterprise Cloud Platform is managed and maintained by Armor. During onboarding, a named user for City of San Diego will be added as the initial Armor Management Portal (AMP) with full administrative rights. The Administrative user may add or remove Users / Administrators, modify roles etc. All virtual machines deployed will have two local administrative accounts: Customer Admin Account - provided to customer to access the server. Customer is responsible for the logical access to its designated Secure Virtual Machine(s) and for managing access to the Customer Admin Account. • Armor Admin Account – assigned to Armor Support for the purposes of accessing servers upon customer request. The credentials for this account are maintained in the Armor Privileged Access Management (PAM) system. The PAM system fully records and stores Armor's access to the Secure Virtual Machine. This account cannot be disabled	If application is hosted, a City Department of IT Security Team Member must be included as one of the administrators.	Information and Data Security
Who owns the data in the system?	Data ownership is fully retained by the customer.		Information and Data Security
Will this solution have the capability to accept credit card information now or in the future?	While the application stack hosted in the Armor environment may be capable of transacting e-commerce utilizing credit cards, Armor does not provide or maintain any such application. Therefore, the ability to create, maintain and ensure PCI compliance with the application is the responsibility of the customer.	If ***yes*** , an approval will be required by DoIT PCI team. See PCI compliance requirements.	Information and Data Security
Will any protected data be stored in the system (PCI, HIPAA, Financial, PII)?	While the application stack hosted in the Armor environment may be capable of transacting storing credit card data, Armor does not provide or maintain any such application. Therefore, the ability to create, maintain and ensure PCI compliance with the application is the responsibility of the customer.	For PCI data, see PCI compliance requirements.	Information and Data Security
Will any protected data be stored OUTSIDE the City's network or datacenter (PCI, HIPAA, Financial, PII)?	As part of the Armor Enterprise Cloud, attached storage to each VM will house data. The classification of the data is to be determined by the customer. Consider the nature of the application, it is expected that the associated data processing and storage will be subject to PCI compliance.		Information and Data Security
Will the vendor or application need access to the City's internal systems to do development or for operational use of the new system?	Armor will not require access to the City's internal systems. The City will determine any necessary connectivity from the Armor environment to the City's internal systems.		Information and Data Security
Does the application have any connections to systems outside of the City's firewall?	Yes as the application stack will be hosted in the Armor data center.		Information and Data Security
If hosted outside of the City's internal network, does the application need a connection inside of our firewall?	Armor will not require a connection inside of the City's firewall. The City will determine any necessary connectivity from the Armor environment to the City's internal systems which may require a connection inside the City's firewall.	If yes, the source and destination IP addresses and ports will be required.	Information and Data Security

How will the system be kept current with patches and upgrades?	Armor Enterprise Cloud provides initial virtual server with an OS hardened images with the latest patches. As an ongoing and included service, Armor will coordinate the applying of critical OS patches on a regular schedule.	If the solution is hosted, the contract needs to state the upgrade and patch processes.	Information and Data Security
Does the system utilize Generative Artificial Intelligence (AI)? If so, what LLM or technology is used (ChatGPT, Bard, etc.?)	Armor does not use Generative AI in Armor Enterprise Cloud solution.	If yes, please explain what input data will be used, if it will be publicly accessible, and what acceptable use and data loss protection policies will be applied.	Information and Data Security
Is the solution: on premise, hosted solution, software as a service (SaaS), or hybrid?	Armor Enterprise Cloud is a Secure Cloud Hosting Solution		Data Center
If the solution is hosted, who is subcontracted to host the data (e.g. AWS, Google Cloud Platform (GCP), Microsoft Azure)?	Armor's Enterprise Cloud incorporates hosting of the data within the platform		Data Center
If the solution is hosted, where will the City's data reside geographically?	Geographically the City's data will reside in Armor Dallas, Texas data center with disaster recovery services provided in our Chicago, Illinois data center.		Data Center
If the solution is hosted, what type of disaster recovery policy or plan does the vendor who is hosting the data have?	Armor's Enterprise Cloud architecture is highly available and highly resilient. Armor also maintains and regularly exercises a Disaster Recovery Plan. Customers are able to utilize our Continuous Data Replication which fully replicates servers and data along with critical networking and security policies to a geographically independent data center. It allows for recovery from a complete datacenter disaster with minimal RTO/RPO and minimal effort.		Data Center
If the solution is hosted, what is the backup policy in place by the vendor?	As an add on service, Armor offers our Advanced Backup Solution with the ability to define custom back up policies and retention periods.		Data Center
If the solution is hosted, what access rights does the City have to the data through the course of the subscription? In what format will the data be provided to the City?	The City will have full access to the Data in Armor Enterprise Cloud through SSL VPN and / or L2L VPN. In terms of format of the data, this will be based on the City's requirements and deployment.		Data Center
If the solution is hosted, what access rights does the City have to the data upon conclusion of the contract? In what format will the data be returned to the City?	The City will have full access to the Data in Armor Enterprise Cloud through SSL VPN and / or L2L VPN. Upon notice of conclusion on the contract the City have the ability to move / transfer any data required. In terms of format of the data, this will be based on the City's requirements and deployment. Post conclusion of the contract any data will be destroyed. Armor will also provide Certificate of Destruction (CoD).		Data Center
If the solution is on premise, how many IP addresses and network connections will be needed?	N/A - The Solution is not on premise		Data Center
If the solution is on premise: How many servers are required?	N/A - The Solution is not on premise		Data Center
If the solution is on premise, what are the source and destination IP addresses and ports?	N/A - The Solution is not on premise		Network
If the solution is on premise, how will it physically connect to the internal network?	N/A - The Solution is not on premise	If this is not clearly outlined in the architecture diagram, please explain and include any relevant hardware required (e.g. switches, routers, etc.).	Network
What are the hours of support of the application?	Armor Enterprise Cloud includes 24/7 support via phone or ticket.		Service Desk
Who does the user call if they have a problem with the system?	Armor's Response / Support Team is available 24/7. Additionally, the City will have a named Client Engagement Manager available for coordination of regular cadence interaction.		Service Desk
Can SCCM (System Center Configuration Manager) be used to push the required desktop components?	N/A - Desktop devices are not in scope for this project.		Service Desk
What other services does the product integrate with?	A number of Hosting services are available in the Armor Enterprise Cloud Platform including Data Encryption, Advanced WAF, Backup and Recovery Options, Continuous Server Replication, Resource Monitoring, Log Search and Visualizations of Security Logs etc.		Service Desk

What software is required on the desktop?	N/A - Desktop devices are not in scope for this project.		Service Desk
Is the system ADA Compliant (WCAG 2.0 as a guideline? Vpat?)	To date, Armor has not been assessed for ADA compliance.		Service Desk

INSTRUCTIONS

Functional Requirements Tab:
The City has provided a list of solution features and designated each of them as either "Mandatory" or "Highly Desirable". Proposers are required to indicate in the "Solution Compliance" drop down box whether their Solution is:

- Fully Compliant
- Partially Compliant
- Not Compliant

All Requirements that are identified by the proposer with a “Fully Compliant” or “Partially Compliant” response shall require further explanation from the Proposer in the “Comments” section.

- Fully Compliant responses require comments decribing how the solution is fully compliant
- Partially Compliant response require comments describing to what extent it meets City requirements, and to what extent modifications or customizations are required. Any additonal cost needed to make a Mandatory Requirement fully compliant shall be included in the proposed Pricing Schedule (Exhibit D).

If the Proposer fails to provide an accompanying elaboration, the City shall consider the requirement to be “Not Compliant”.

Any “Not Compliant” responses or responses considered not compliant for failure to provide accompanying elaboration for requirements specifically designated as “Mandatory” may be declared non-responsive and rejected.

General Requirements Tab:
The City has provided a list of solution general requirements. Proposers are required to describe how their solution meets these requirements. If the requirement requests specific details on what the proposer is offering (i.e. SLA's, compliance documentation) then proposer shall provide the requested information as decribed.

Proposer should be prepared to possibly demonstrate these features during the Product Evaluations.

EXHIBIT F: FUNCTIONAL REQUIREMENTS RESPONSE TEMPLATE - Armor Defense Inc.				Proposer Completes (note: Proposers should not alter the format of this response sheet)
ID	City Requirement			
1	**Functionality**	**Requirement is Mandatory (M) or Highly Desirable (HD)**	**Solution Compliance**	**Proposer Comments - Proposers must describe, in detail, exactly how the solution does, or does not comply.**
	The following Functionality requirements shall apply:			
1.1	**Secure Cloud Environment**: Creating and maintaining a PCI DSS 4.0-compliant cloud hosting environment.	M	Partially Compliant	Compliant against PCI v3.2.1 (ROC dated 9/30/2023). PCI 4.0 Readiness Assessment completed in March 2024. PCI 4.0 Type 1 Service Provider assessment underway. ROC anticipated completion date is 6/30/2024.
1.2	**Four 9's (99.99%) Uptime**: Ensuring a minimum of 99.99% uptime for the hosting environment.	M	Fully Compliant	A full description of Armor's SLA's can be found at: https://www.armor.com/legal/sla
1.3	Comprehensive Security Measures: Implementing encryption, multi-factor authentication, firewalls, intrusion detection, and ongoing vulnerability assessments.	M	Fully Compliant	Armor maintains compliance certifications against PCI DSS, HITRUST (HIPAA/NIST 800-53), ISO27001, SOC2 Type II, TX-RAMP, and Data Privacy Framework, all of which address these comprehensive security measures. These assessments are performed by independent audit firms and are certified annually.
1.4	**Incident Response and Recovery**: Providing 24/7 monitoring and rapid response to security incidents, with well-defined incident response procedures.	M	Fully Compliant	A full description of Armor's Incident Response and Recovery procedures can be found at: https://kb.armor.com/kb/incident-response-plan
1.5	**Backup and Recovery Services**: Establishing regular backup procedures and efficient data recovery protocols to minimize data loss.	M	Fully Compliant	A full description of Armor's Backup and Recovery procedures can be found at: https://kb.armor.com/kb/business-continuity
1.6	**Load Balancers for High Availability**: Implementing load balancers to ensure continuous service availability, particularly during patching windows, to avoid service downtime.	M	Fully Compliant	A full description of Armor's load balancers can be found at: https://kb.armor.com/kb/networking
1.7	**File Integrity Monitoring**: Implementing file integrity monitoring to detect unauthorized changes to critical system files.	M	Fully Compliant	A full description of Armor's file integrity monitoring capabilities can be found at: https://kb.armor.com/kb/file-integrity-monitoring
1.8	**Endpoint Detection and Response**: Implementing endpoint detection and response mechanisms, including antivirus, behavioral anomaly detection, and containment.	M	Fully Compliant	A full description of Armor's EDR capabilities can be found at: https://kb.armor.com/kb/endpoint-detection-and-response-edr
1.9	**Host-based IDS and IPS**: Implementing host-based intrusion detection and prevention systems to monitor and block malicious activities.	M	Fully Compliant	A full description of Armor's HIDS/HIPS capabilities can be found at: https://kb.armor.com/kb/intrusion-detection
1.10	**Malware Protection**: Deploying malware protection mechanisms to safeguard against malicious software.	M	Fully Compliant	A full description of Armor's Malware Protection capabilities can be found at: https://kb.armor.com/kb/malware-protection
1.11	**Vulnerability Scanning and Remediation**: Conducting regular vulnerability scans and performing remediation without patching window downtime, using load balancers.	M	Fully Compliant	A full description of Armor's Vulnerability Scanning capabilities can be found at: https://kb.armor.com/kb/vulnerability-scanning. Vulnerability Remediation details can be found at: https://kb.armor.com/kb/vulnerability-remediation.
1.12	**IPRM (Internet Protocol Reputation Management) Services**: Managing and monitoring Internet Protocol reputations to mitigate potential threats.	M	Fully Compliant	A full description of Armor's Threat Hunting capabilities can be found at: https://kb.armor.com/kb/threat-hunting
1.13	**Web Application Firewall (WAF) Services**: Deploying and managing a WAF to protect against web-based attacks.	M	Fully Compliant	A full description of Armor's WAF services can be found at: https://kb.armor.com/kb/network-security-services
1.14	**Log Management and Retention**: Implementing a robust log management system with retention policies for compliance and security analysis.	M	Fully Compliant	A full description of Armor's Log Management and Retention capabilities can be found at: https://kb.armor.com/kb/log-management-home

EXHIBIT F: FUNCTIONAL REQUIREMENTS RESPONSE TEMPLATE - Armor Defense Inc.			Proposer Completes (note: Proposers should not alter the format of this response sheet)	
ID	City Requirement			
1.15	**Firewall Port Administration**: Providing an interface within the management portal for firewall port administration.	M	Fully Compliant	A full description of Armor's Firewall Port Administration capabilities can be found at: https://kb.armor.com/kb/firewall-rules
1.16	**ASV Scanning Solution**: List of the service provider's Approved Scanning Vendor solution for vulnerability assessment and compliance scanning.	M	Fully Compliant	A full description of Armor's ASV Scanning Solutions can be found at: https://kb.armor.com/kb/vulnerability-scanning-qualys-asv
1.17	**Business Continuity**: Deploying high-availability and disaster recovery solutions.	M	Fully Compliant	A full description of Armor's Business Continuity capabilities can be found at: https://kb.armor.com/kb/business-continuity
1.18	**Custom Reporting and Dashboarding**: Description of availability of custom reports and dashboards.	HD	Fully Compliant	A full description of Armor's Customer Reporting and Dashboarding capabilities can be found at: https://kb.armor.com/kb/dashboards-reporting
2	**Technical**			
	The following Functionality requirements shall apply:			
2.1	**Troubleshooting and Remediation Coordination**: Coordinating troubleshooting and remediation efforts for the general infrastructure within the hosting environment.	HD	Fully Compliant	A full description of Armor's Troubleshooting and Remediation Coordination capabilities can be found at: https://kb.armor.com/kb/armor-support
2.2	**Continuous Compliance Oversight**: Monitoring and reporting on PCI DSS compliance status, including the transition to DSS 4.0 if that level of compliance has yet to be achieved.	M	Fully Compliant	The same process would be followed as above with Armor Support. Escalations would progress up through the GRC|P organization, as high as the Chief Risk Officer/Data Privacy Officer (Dept Head).
3	**System User Authentication**			
	The following Functionality requirements shall apply:			
3.1	**Active Directory.** Solution should offer integration with City's Active Directory to authenticate System Users.	HD	Fully Compliant	A full description of Armor's Integration capabilities can be found at: https://kb.armor.com/kb/cloud-connectors
3.2	**Multi-factor Authentication.** Solution must support various methods of multi-factor authentication for internal and external parties (within diverse authentication settings such as knowledge-based or credential-based) included but not limited to PIN code, third party authentication like OATH/SAML, phone #, email, etc.	M	Fully Compliant	A full description of Armor's MFA setup instructions can be found at: https://kb.armor.com/kb/user-accounts#UserAccounts-Configuremulti-factorauthenticationasacurrentuser
3.3	**System Administration.** Hosting solution must provide the ability for system administers to maintain System Users and permissions without technical assistance.	M	Fully Compliant	A full description of System Administration capabilities can be found at: https://kb.armor.com/kb/user-accounts#UserAccounts-Configuremulti-factorauthenticationasacurrentuser

	EXHIBIT F: General Requirements Response Template - Armor Defense Inc.	Proposer shall describe how their proposed solution meets these requirements.
ID	City Requirement	Proposer Response
		Proposers must provide detailed responses for each of these requirements
4.1	**Technical Solution**: Detailed architecture, security measures, network configuration, and data protection plans to reflect all applicable services in the scope of work.	General details can be identified at docs.armor.com. For specific information, Armor's direct POCs will work with City to provide all required documentation.
4.2	**Compliance Documentation**: Evidence of PCI DSS compliance and industry certifications.	Able to provide evidence of PCI DSS compliance and industry certifications under MNDA.
4.3	**PCI DSS 4.0 Compliance Approach**: Clear outline of steps to achieve compliance with PCI DSS 4.0 standards.	PCI DSS 4.0 Readiness Assessment completed in April 2024. Level 1 Service Provider assessment underway. ROC anticipated by 6/30/2024.
4.4	**Supported Operating Systems List**: Comprehensive list of supported operating systems.	Information on supported operating systems can be found at: https://kb.armor.com/kb/pre-installation-and-deployment-options
4.5	**Vendor Lock-In and Data Portability Strategy**: Explanation of handling data portability and migration.	City would be locked in with Armor to the extent of the contracts executed between both parties. In terms of data portability/migration, City can announce their intent to churn when contractually appropriate and begin exporting their own data offsite or to wherever they've chosen. Alternatively, Armor Support can perform a data export for them and provide a Certificate of Destruction upon completion.
4.6	**Continuous Improvement and Innovation**: Explain how hosting provider ensures ongoing innovation and improvement in security practices to stay ahead of emerging threats.	Armor has documented their Threat Intelligence practices here: https://kb.armor.com/kb/threat-intelligence, and their Threat Hunting practices here: https://kb.armor.com/kb/threat-hunting. In combination, these describe some of the continuous improvement and innovation methods used to stay ahead of emerging threats.
4.7	**Regulatory Compliance Expertise**: Company's expertise in other relevant regulations and standards, such as GDPR or HIPAA, depending on your use case.	Armor maintains annual certifications against PCI DSS, HITRUST (HIPAA/NIST 800-53), ISO-27001, SOC2 Type II, TX-RAMP, and Data Privacy Framework. We have expertise in PDPA, GDPR, CCPA/CPRA, Sarbanes-Oxley, and others.
4.8	**Service Level Agreements (SLAs)**: Proposed SLAs for uptime, response times, and issue resolution.	SLA information is posted on Armor's website: https://www.armor.com/legal/sla
4.9	**Data Center Location**: The provider's data center must be located within the continental United States.	Armor has data centers located in DFW Texas and Chicago Illinois, as well as in Slough England and in Frankfurt Germany.
4.10	**Vendor Lock-In and Data Portability**: Discuss how the hosting provider handles data portability and migration should one choose to switch providers in the future.	With respect to Armor's vendors, we are locked in only to the extent of the contractual agreements we've entered. Any decision made to change a vendor could require any number of actions, including: risk assessments, vendor due diligence processes, privacy impact assessments, customer notification and approval (in limited cases), etc., depending on the criticality of the vendor and/or the data type(s) they may store or process for us.

EXHIBIT G: Interrogatories Response & References Template ID	City Question	Proposer Completes (note: Proposers should not alter the format of this response sheet) Proposer Response
1	**Background and Experience**	**Armor Defense Inc.**
	Please answer the following questions:	
1.1	Provide an overview of the maturity of the Solution, inclusive of: a. Number of active paying commercial customers for the Solution b. Description of age and maturity of the Solution c. Description of update cycle for Solution d. Any relevant future enhancements or innovations for Solution e. Number of successful implementations completed within the last three years (by your organization or your proposed sub-contractor).	400+ active paying commercial customers for Armor Enterprise Cloud solution; solution has been in place since 2009; update cycles follow quarterly roadmap; large VMs, increased storage capacity, enhancements to Armor Management Portal (AMP); 100+ successful implementations completed within last three (3) years.
1.2	Provide the following information: a. Proposer must include a company overview including related experience to the services being requested in this RFP. b. Resumes: Proposer must include brief resumes for personnel that will be assigned to the implementation project, if awarded the contract. The resumes must identify expertise in the functional areas listed in the RFP. Proven work experience combined with related education will be means of substantiating expertise.	Armor Defense Inc. has provided solution to City of San Diego since September 2020 and company overview is located in response file; no implementation required as solution is currently in place; Armor team currently supporting City of San Diego team is Chris Murphy, VP Client Engagement Management, Evan Powell, Client Engagement Manager, Nancy Free, Head of Risk and PCI Compliance, Chris Stouff, Head of Security, Scott Cole, Director of Enterprise Support, and Goutam Sinha, Armor Enterprise Cloud Product Management. Additional resources that support City of San Diego include Product, Engineering, Enterprise Support, Security Operations Center (SOC), Compliance, and other Technical resources. Additional resume information for Armor team that currently serves City of San Diego team are certainly available.
2	**References**	
	Please answer the following questions:	
2.1	**Reference 1** Provide a reference for your solution (from the last five years), inclusive of: a. Company name b. Contact name and role c. Contact details (email, phone) d. Location e. Deployment size f. Description of the deployment (where possible, provide examples of clients of similar size/environment/sector to the City of San Diego). If you intend to sub-contract the implementation services, please provide the above details for both your own organization, and the sub-contractor.	ViTel Net, Keith Buck, Chief Innovation Officer, dkbuck@vitelnet.com, 410-627-5574, McLean, VA, fully managed multiple VM implementation needing high degree of security and compliance, Armor has many customers in CA, no implementation sub-contractor and no implementation required as Armor is currently providing City of San Diego's Payment Card Industry (PCI) Compliant Cloud Hosting Services/Solution.
2.2	**Reference 2** Provide a reference for your solution (from the last five years), inclusive of: a. Company name b. Contact name and role c. Contact details (email, phone) d. Location e. Deployment size f. Description of the deployment (where possible, provide examples of clients of similar size/environment/sector to the City of San Diego). If you intend to sub-contract the implementation services, please provide the above details for both your own organization, and the sub-contractor.	Devlin Consulting (Sagility), Jim Cowsert, VP Sagility Payment Integrity Services, jim.cowsert@devlinconsulting.com, 480-365-9090, Queen Creek, AZ, fully managed multiple VM implementation needing high degree of security and compliance, Armor has many customers in CA, no implementation sub-contractor and no implementation required as Armor is currently providing City of San Diego's Payment Card Industry (PCI) Compliant Cloud Hosting Services/Solution.

EXHIBIT G: Interrogatories Response & References Template ID	City Question	Proposer Completes (note: Proposers should not alter the format of this response sheet) Proposer Response
2.3	**Reference 3** Provide a reference for your solution (from the last five years), inclusive of: a. Company name b. Contact name and role c. Contact details (email, phone) d. Location e. Deployment size f. Description of the deployment (where possible, provide examples of clients of similar size/environment/sector to the City of San Diego). If you intend to sub-contract the implementation services, please provide the above details for both your own organization, and the sub-contractor.	Western Health Advantage, Eric Sibley, IT Infrastructure Director, e.sibley@westernhealth.com, 916-614-6029, Sacramento, CA, fully managed multiple VM implementation needing high degree of security and compliance, Armor has many customers in CA including this one as reference, no implementation sub-contractor and no implementation required as Armor is currently providing City of San Diego's Payment Card Industry (PCI) Compliant Cloud Hosting Services/Solution.
3	**Implementation, Planning & Training**	
	Please answer the following questions:	
3.1	Provide a project plan for a fixed-price delivery of the implementation services including the following: a. Project Timeline-High level project plan (Microsoft Project Gantt chart, or equivalent); b. Explanation of the roles of the proposed project team; c. Explanation of the role of the City (including time commitments); d. Description of a recommended team structure; and e. List of key personnel functions, staffing profiles and responsibilities to cover the implementation, training and support.	N/A as Armor is currently supporting the hosting and security of City of San Diego's PCI application stack. No further work is needed to continue with the services as currently implemented.
3.2	Provide a brief proposed plan for implementing the Solution. It must include, but not be limited to: a. High level explanation of how you plan to successfully implement the Solution requirements; b. Migration Strategy, final testing & acceptance, transition; c. Technical requirements for test, training and production environments, including equipment, as appropriate; and	***N/A as Armor is currently supporting the hosting and security of City of San Diego's PCI application stack. No further work is needed to continue with the services as currently implemented.***
3.3	Provide a brief proposed plan for providing City staff with training in the operation and maintenance of the Solution, including application functions, hardware use, and any procedures that are unique to a particular job function. a. A detailed training plan for selected City staff must be developed and implemented for the operation of all application modules and processing functions prior to implementation. b. Application manuals and procedures manuals must be provided to the City in an electronic format. The manuals must be routinely updated as policies or programs are changed. c. Training will begin no later than thirty (30) calendar days after the Solution is installed and accepted by the City. If the Go-live date is significantly delayed due to the Proposer actions or faults, any repeat training sessions as determined by the City must be performed at no cost to the City.	*N/A as Armor is currently supporting the hosting and security of City of San Diego's PCI application stack. No need for training as the team from the City of San Diego is well versed in the use and interaction with the Armor environment.*
4	**Pricing**	
	Please answer the following questions:	

EXHIBIT G: Interrogatories Response & References Template		Proposer Completes (note: Proposers should not alter the format of this response sheet)
ID	City Question	Proposer Response
4.1	Explain clearly your proposed pricing model for the solution. Ensure you cover all potential chargeable costs, and include all details pertinent to: a. Charging metrics (e.g. named user, CPU, socket, month, gigabyte etc.) b. Definitions for the charging metrics c. Unitary cost for each chargeable item d. Quantities for each unit e. SKU code for each item f. Sandboxing and dev/test licensing g. Describe what limits and additional costs (if any) might apply for bandwidth usage on transporting City data h. Under what circumstances the City may be exposed to additional overage costs i. Any other relevant payment triggers, and how the City might be notified prior to the charge being triggered	Pricing model for Armor services is such that the services are billed on a monthly basis. Each service is specifically requested by the customer and either implemented automatically (via request in the Armor Management Portal) or implemented by an Armor Support Engineer (via ticket request submitted by the customer in Armor's Ticketing Platform. Depending on the service, the applicable unit of measurement is displayed on the invoice. Please see pricing submitted in Exhibit D for detailed costs. No fees associated to bandwidth. Authorized users from the City of San Diego may request additional services at any time. Fees for additional services will be clearly indicated prior to submitting the request. The City of San Diego my limit purchasing rights via Armor's Management Portal, however, at least one user must retain purchase rights. For authorized users with purchasing rights, Armor will not restrict any request for additional services. Therefore, additional services requested by an authorized user and the associated fees for those services will be applicable.
4.2	The City's PCI environment outlined within the language of this RFP is based on the environment at time of the release of this RFP, however this is expected to change (likely decrease). Please provide specific details as to how the pricing provided in the Pricing Schedule (Exhibit D) would change based on your pricing model for the solution with changes to the environment.	Armor services and the associated fees for the services are specific to what is assigned to the account during the monthly billing period. Services may increase or decrease as determined by the City of San Diego and indicated with requests to increase or decrease via the Armor Management Portal.
5	**Minimum Service Level Requirements**	
	Please answer the following questions:	
5.1	Explain clearly your proposed solution meets the following minimum service level requirements: a. Hours of Operation (details) b. Uptime Availability including the following: - remuneration - service credits and service credits calculations - scheduled maintenance	Please see the Armor Service Leval Agreement Attached as separate PDF document.
6	**City Tech Alignment**	
	Please answer the following questions:	
6.1	Will the Proposer or application need access to the City's internal systems to do development or for operational use of the new system?	No
6.2	Will the Solution require any connections to systems outside of the City's firewall?	Yes
6.3	How many IP's will the Proposer require for both the outbound connections and authentication to the app via the City's LDAP? (there are typically IP's identified by the vendor as the IP's that point to the externally hosted application).	IP requirements are determined by the customer
6.4	Does access to the application need to be restricted inside the City network to certain IP addresses or subnets?	Not applicable to Armor Services
6.5	What restrictions (if any) will be placed on the City's third party Applications Maintenance provider in terms of accessing the Solution to make changes to the configuration for enhancements on behalf of the City?	Requests for new user accounts are at the exclusive request made by a current authorized user through the Armor Management Portal
6.6	Please describe how will the system be kept current with patches and upgrades?	Critical security patches as defined and provided by the manufacturer of Operating System software will be applied by Armor as part of our Patch Management Service at a regularly scheduled time mutually agreed to by Armor and the City of San Diego.
6.7	What software (if any) is required on a City desktop?	None

EXHIBIT G: Interrogatories Response & References Template		Proposer Completes (note: Proposers should not alter the format of this response sheet)
ID	City Question	Proposer Response
6.8	Are there any desktop components required to be installed?	None
6.9	If the solution is to be linked or jumped off from the City's website, then what is the domain name/URL going to be and whose responsibility is it to get it?	Application related access is the responsibility of the customer
6.10	Is the hosting component expected to be sub-contracted to a provider? If so, who?	Armor utilizes a sub-contractor to provide the data center and physical hardware associated to the services
6.11	Where are the hosting sites located?	Current solution hosted in our Dallas, Texas data center with replication services located in Chicago, Illinois. Armor has additional data centers in Frankford, Germany and London, England.
6.12	Where are backup sites located?	Backup services are available via the primary data center with an option to extend the backups to a secondary data center.
6.13	Would City data be made available for use or access by a third party? Please describe to what extent.	Armor does not access customer data during typical operations. On occasion, Armor may be required to access server environments which contain customer data. In those cases, Armor will only access customer environments through a Privileged Access Management System where all sessions are fully recorded and stored for audit purposes.

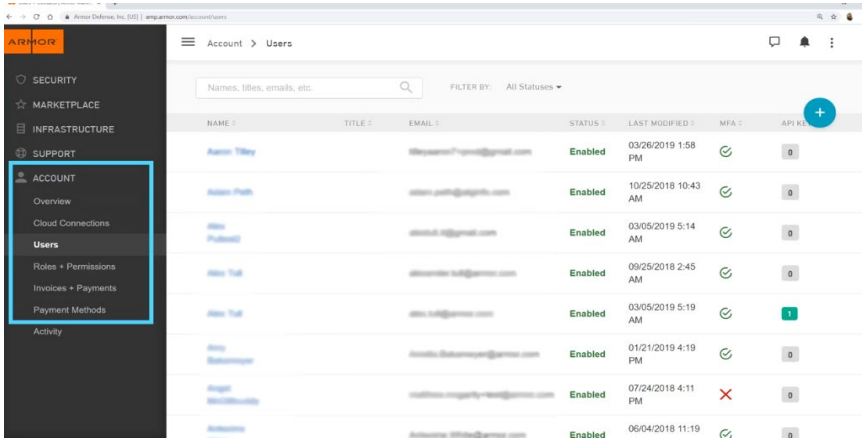
EXHIBIT H: Screenshots Response Template

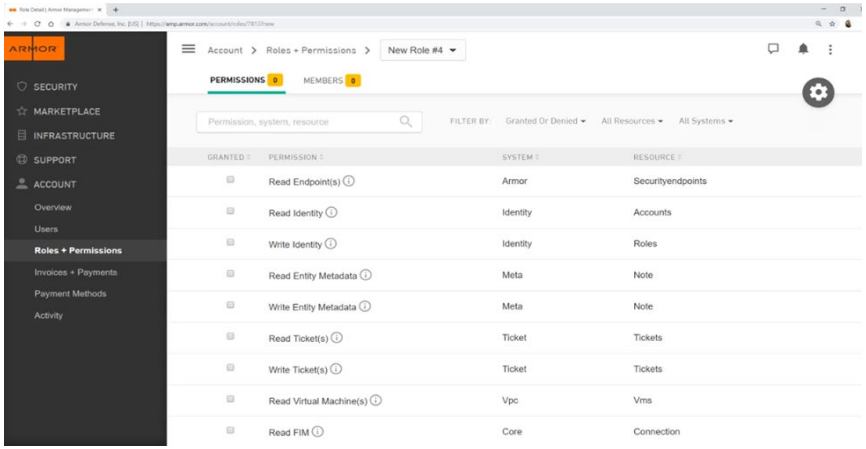
The City of SAN DIEGO

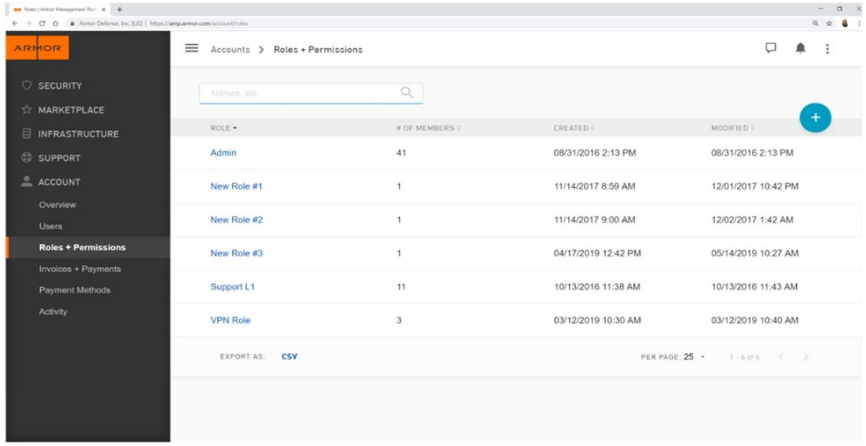
Armor Defense Inc.

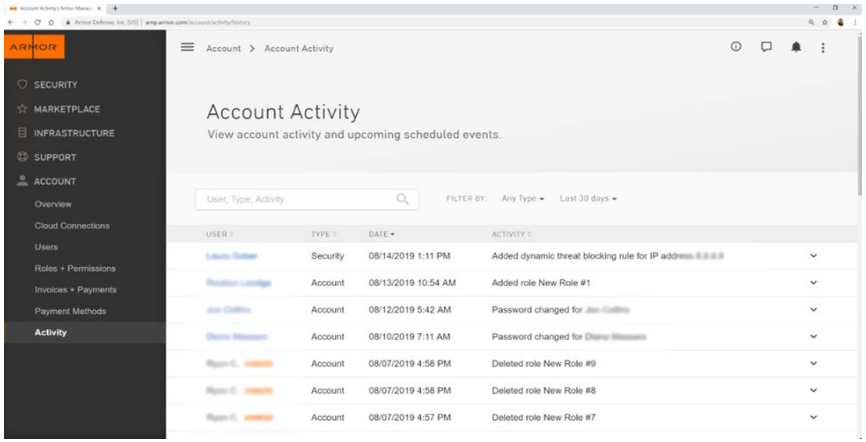
Please provide GUI and dashboard screenshots (examples below) for frequent operations, reporting and analytics on this worksheet.

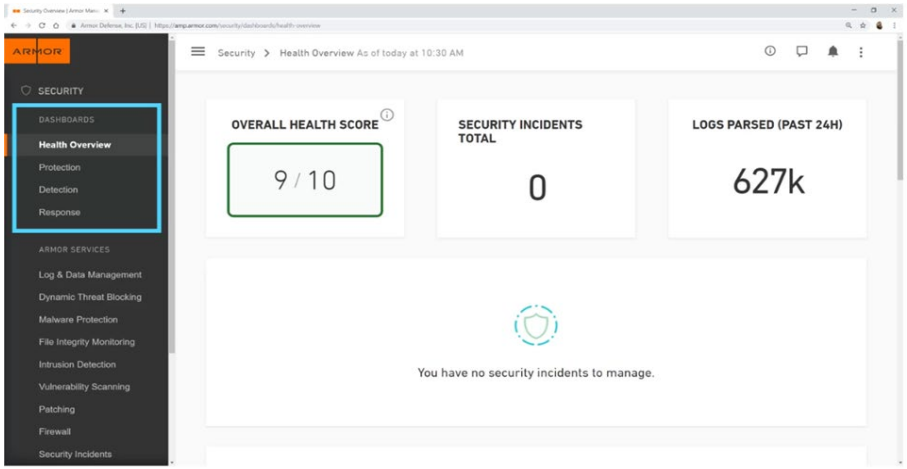
Examples:
User setup
Account administration
Main dashboard
Reporting and analytics
SLA reports
Any useful functions that differentiate your product from competition

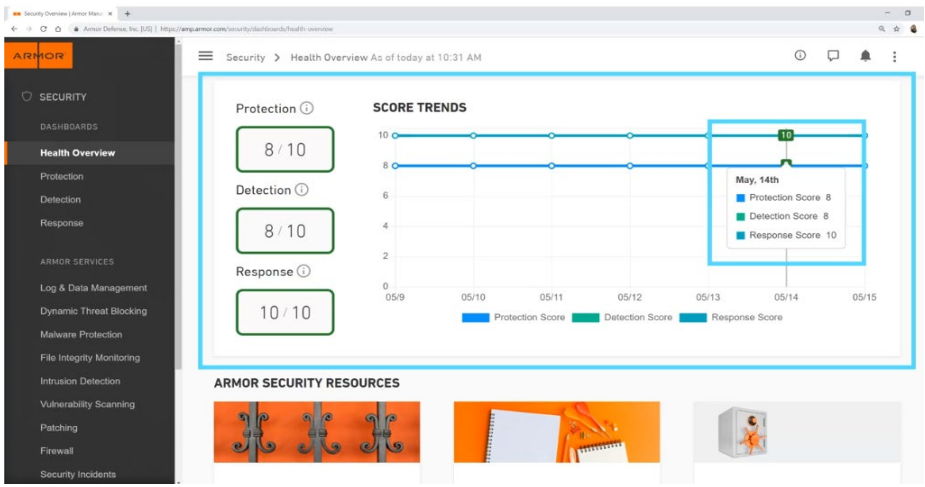

ARMOR
Account > Users
SECURITY
MARKETPLACE
INFRASTRUCTURE
SUPPORT
ACCOUNT
Overview
Cloud Connections
Users
Roles + Permissions
Invoices + Payments
Payment Methods
Activity
Names, titles, emails, etc.
FILTER BY: All Statuses
NAME
TITLE
EMAIL
STATUS
LAST MODIFIED
MFA
Enabled
03/26/2019 1:58 PM
10/25/2018 10:43 AM
03/05/2019 5:14 AM
09/25/2018 2:45 AM
03/05/2019 5:19 AM
01/21/2019 4:19 PM
07/24/2018 4:11 PM
06/04/2018 11:19

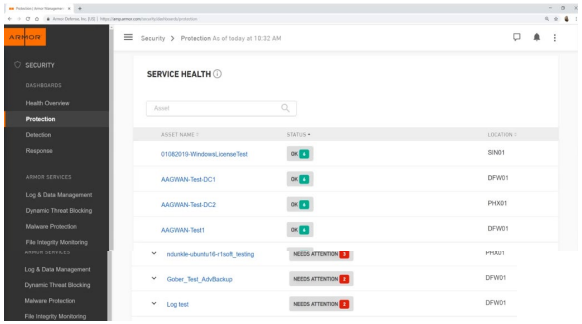

ARMOR
Account > Roles + Permissions > New Role #4
PERMISSIONS 9
MEMBERS 8
Permission, system, resource
FILTER BY: Granted Or Denied All Resources All Systems
GRANTED
PERMISSION
SYSTEM
RESOURCE
Read Endpoint(s) Armor Securityendpoints
Read Identity Identity Accounts
Write Identity Identity Roles
Read Entity Metadata Meta Note
Write Entity Metadata Meta Note
Read Ticket(s) Ticket Tickets
Write Ticket(s) Ticket Tickets
Read Virtual Machine(s) Vpc Vms
Read FIM Core Connection

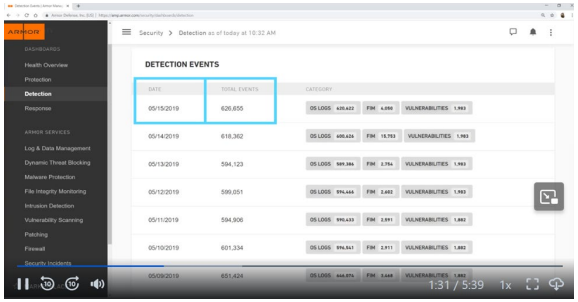

ARMOR
Accounts > Roles + Permissions
Names, etc.
ROLE
OF MEMBERS
CREATED
MODIFIED
Admin 41 08/31/2016 2:13 PM 08/31/2016 2:13 PM
New Role #1 1 11/14/2017 8:59 AM 12/01/2017 10:42 PM
New Role #2 1 11/14/2017 9:00 AM 12/02/2017 1:42 AM
New Role #3 1 04/17/2019 12:42 PM 05/14/2019 10:27 AM
Support L1 11 10/13/2016 11:38 AM 10/13/2016 11:43 AM
VPN Role 3 03/12/2019 10:30 AM 03/12/2019 10:40 AM
EXPORT AS: CSV
PER PAGE: 25

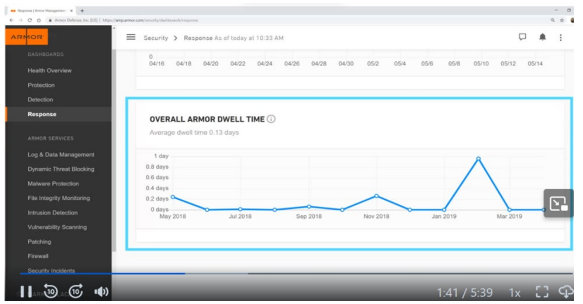

ARMOR
Account > Account Activity
Account Activity
View account activity and upcoming scheduled events.
User, Type, Activity
FILTER BY: Any Type Last 30 days
USER
TYPE
DATE
ACTIVITY
Security 08/14/2019 1:11 PM Added dynamic threat blocking rule for IP address
Account 08/13/2019 10:54 AM Added role New Role #1
Account 08/12/2019 5:42 AM Password changed for
Account 08/10/2019 7:11 AM Password changed for
Account 08/07/2019 4:58 PM Deleted role New Role #9
Account 08/07/2019 4:58 PM Deleted role New Role #8
Account 08/07/2019 4:57 PM Deleted role New Role #7

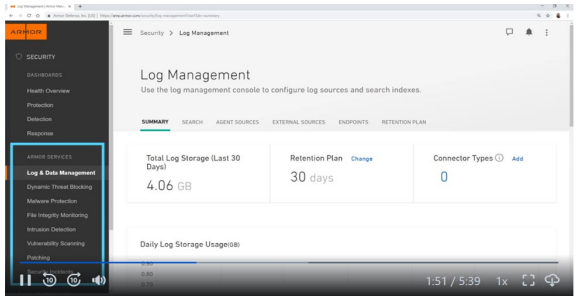

ARMOR
SECURITY
DASHBOARDS
Health Overview
Protection
Detection
Response
ARMOR SERVICES
Log & Data Management
Dynamic Threat Blocking
Malware Protection
File Integrity Monitoring
Intrusion Detection
Vulnerability Scanning
Patching
Firewall
Security Incidents
Security > Health Overview As of today at 10:30 AM
OVERALL HEALTH SCORE
9 / 10
SECURITY INCIDENTS TOTAL
0
LOGS PARSED (PAST 24H)
627k
You have no security incidents to manage.

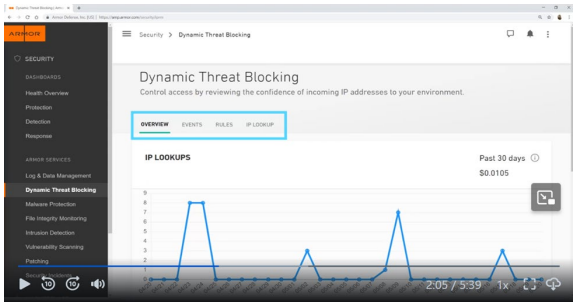

ARMOR
SECURITY
DASHBOARDS
Health Overview
Protection
Detection
Response
ARMOR SERVICES
Log & Data Management
Dynamic Threat Blocking
Malware Protection
File Integrity Monitoring
Intrusion Detection
Vulnerability Scanning
Patching
Firewall
Security Incidents
Security > Health Overview As of today at 10:31 AM
Protection
8 / 10
Detection
8 / 10
Response
10 / 10
SCORE TRENDS
10
8
6
4
2
0
05/9
05/10
05/11
05/12
05/13
05/14
05/15
May, 14th
Protection Score 8
Detection Score 8
Response Score 10
Protection Score
Detection Score
Response Score
ARMOR SECURITY RESOURCES

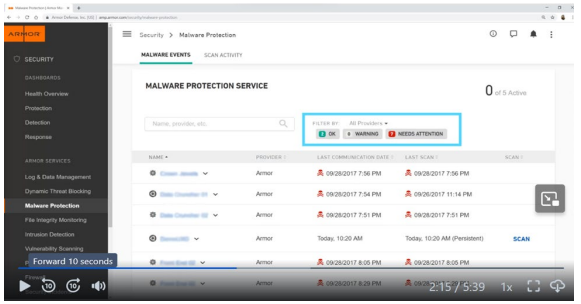

SERVICE HEALTH

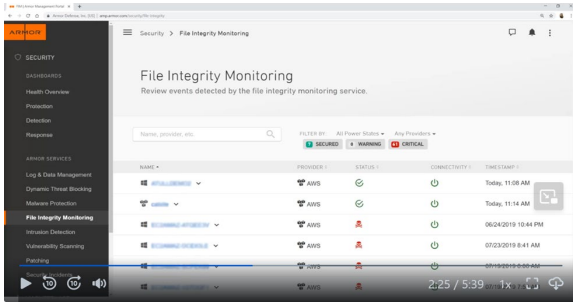

DETECTION EVENTS
1:31 / 5:39

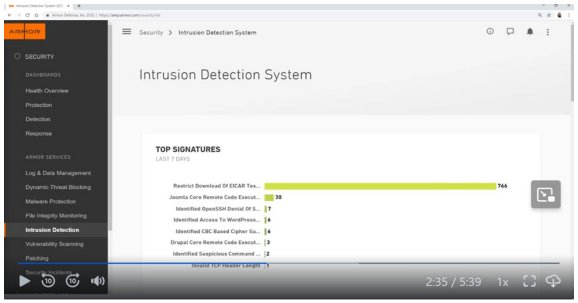

OVERALL ARMOR DWELL TIME
1:41 / 5:39

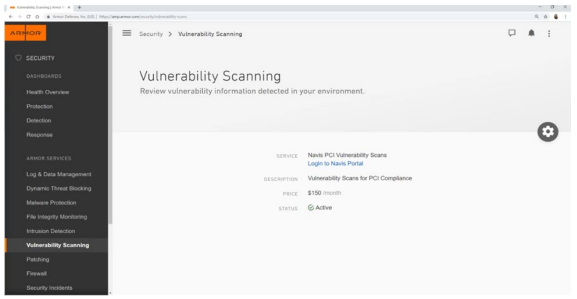

Log Management
1:51 / 5:39

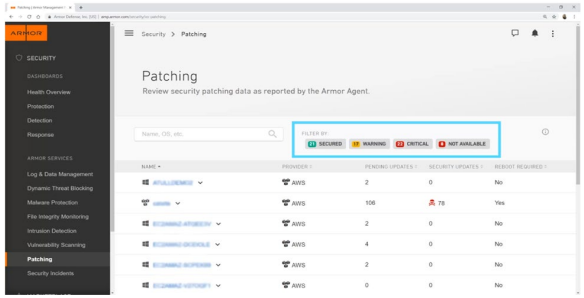

Dynamic Threat Blocking
2:05 / 5:39

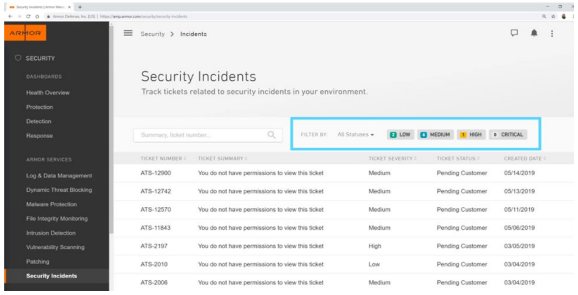

MALWARE PROTECTION SERVICE
Forward 10 seconds
2:15 / 5:39

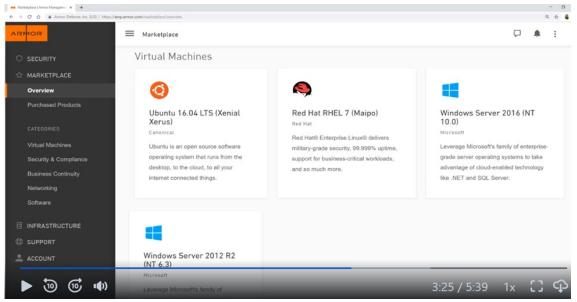

File Integrity Monitoring
Review events detected by the file integrity monitoring service.
2:25 / 5:39 1x

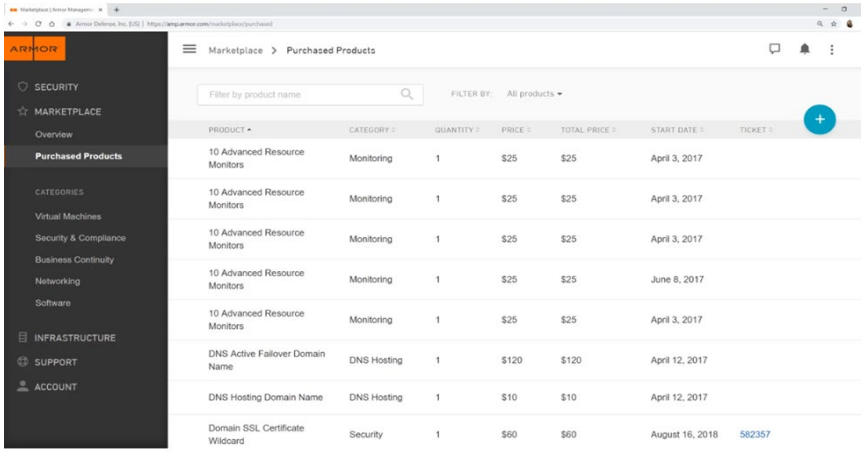

Intrusion Detection System
TOP SIGNATURES
2:35 / 5:39 1x

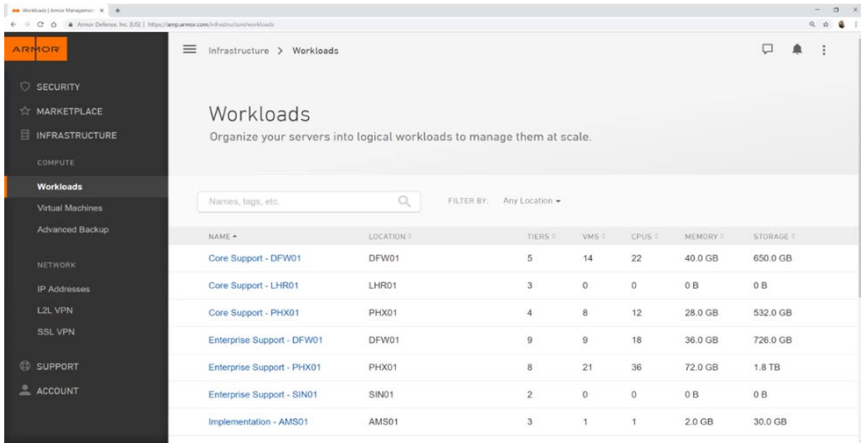

Vulnerability Scanning
Review vulnerability information detected in your environment.

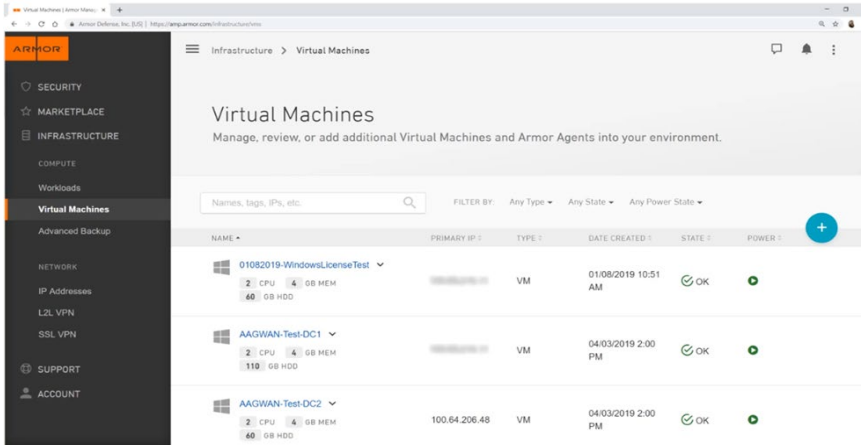

Patching
Review security patching data as reported by the Armor Agent.

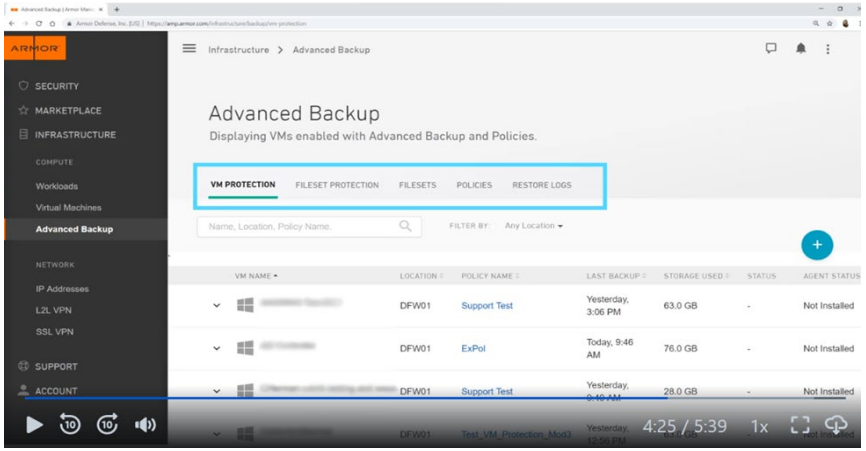

Security Incidents
Track tickets related to security incidents in your environment.


Virtual Machines
Ubuntu 16.04 LTS (Xenial Xerus)
Red Hat RHEL 7 (Maipo)
Windows Server 2016 (NT 10.0)
Windows Server 2012 R2 (NT 6.3)
3:25 / 5:39 1x


ARMOR
Marketplace > Purchased Products
SECURITY
MARKETPLACE
Overview
Purchased Products
CATEGORIES
Virtual Machines
Security & Compliance
Business Continuity
Networking
Software
INFRASTRUCTURE
SUPPORT
ACCOUNT
Filter by product name
FILTER BY: All products
PRODUCT | CATEGORY | QUANTITY | PRICE | TOTAL PRICE | START DATE | TICKET
10 Advanced Resource Monitors | Monitoring | 1 | $25 | $25 | April 3, 2017
10 Advanced Resource Monitors | Monitoring | 1 | $25 | $25 | April 3, 2017
10 Advanced Resource Monitors | Monitoring | 1 | $25 | $25 | April 3, 2017
10 Advanced Resource Monitors | Monitoring | 1 | $25 | $25 | June 8, 2017
10 Advanced Resource Monitors | Monitoring | 1 | $25 | $25 | April 3, 2017
DNS Active Failover Domain Name | DNS Hosting | 1 | $120 | $120 | April 12, 2017
DNS Hosting Domain Name | DNS Hosting | 1 | $10 | $10 | April 12, 2017
Domain SSL Certificate Wildcard | Security | 1 | $60 | $60 | August 16, 2018 | 582357


ARMOR
Infrastructure > Workloads
SECURITY
MARKETPLACE
INFRASTRUCTURE
COMPUTE
Workloads
Virtual Machines
Advanced Backup
NETWORK
IP Addresses
L2L VPN
SSL VPN
SUPPORT
ACCOUNT
Workloads
Organize your servers into logical workloads to manage them at scale.
Names, tags, etc.
FILTER BY: Any Location
NAME | LOCATION | TIERS | VMS | CPUS | MEMORY | STORAGE
Core Support - DFW01 | DFW01 | 5 | 14 | 22 | 40.0 GB | 650.0 GB
Core Support - LHR01 | LHR01 | 3 | 0 | 0 | 0 B | 0 B
Core Support - PHX01 | PHX01 | 4 | 8 | 12 | 28.0 GB | 532.0 GB
Enterprise Support - DFW01 | DFW01 | 9 | 9 | 18 | 36.0 GB | 726.0 GB
Enterprise Support - PHX01 | PHX01 | 8 | 21 | 36 | 72.0 GB | 1.8 TB
Enterprise Support - SIN01 | SIN01 | 2 | 0 | 0 | 0 B | 0 B
Implementation - AMS01 | AMS01 | 3 | 1 | 1 | 2.0 GB | 30.0 GB


ARMOR
Infrastructure > Virtual Machines
SECURITY
MARKETPLACE
INFRASTRUCTURE
COMPUTE
Workloads
Virtual Machines
Advanced Backup
NETWORK
IP Addresses
L2L VPN
SSL VPN
SUPPORT
ACCOUNT
Virtual Machines
Manage, review, or add additional Virtual Machines and Armor Agents into your environment.
Names, tags, IPs, etc.
FILTER BY: Any Type Any State Any Power State
NAME | PRIMARY IP | TYPE | DATE CREATED | STATE | POWER
01082019-WindowsLicenseTest
2 CPU 4 GB MEM 60 GB HDD
VM | 01/08/2019 10:51 AM | OK
AAGWAN-Test-DC1
2 CPU 4 GB MEM 110 GB HDD
VM | 04/03/2019 2:00 PM | OK
AAGWAN-Test-DC2
2 CPU 4 GB MEM 60 GB HDD
100.64.206.48 | VM | 04/03/2019 2:00 PM | OK


ARMOR
Infrastructure > Advanced Backup
SECURITY
MARKETPLACE
INFRASTRUCTURE
COMPUTE
Workloads
Virtual Machines
Advanced Backup
NETWORK
IP Addresses
L2L VPN
SSL VPN
SUPPORT
ACCOUNT
Advanced Backup
Displaying VMs enabled with Advanced Backup and Policies.
VM PROTECTION | FILESET PROTECTION | FILESETS | POLICIES | RESTORE LOGS
Name, Location, Policy Name.
FILTER BY: Any Location
VM NAME | LOCATION | POLICY NAME | LAST BACKUP | STORAGE USED | STATUS | AGENT STATUS
DFW01 | Support Test | Yesterday, 3:06 PM | 63.0 GB | - | Not Installed
DFW01 | ExPol | Today, 9:46 AM | 76.0 GB | - | Not Installed
DFW01 | Support Test | Yesterday, 9:46 AM | 28.0 GB | - | Not Installed
DFW01 | Test_VM_Protection_Mod3 | Yesterday, 12:56 PM
4:25 / 5:39 1x

PST ARMOR HOME SUBSCRIBE

42
UP

0
AFFECTED

0
DOWN

Armor's intuitive status dashboard provides real-time visibility into the health of our infrastructure and security solutions. Leverage the interactive tool to confirm service availability based on geography, and also the status for storage, security controls, hosts, management portals, APIs, or Armor Anywhere services. To receive instant notifications via email, SMS or Web hooks for maintenance events, or changes in status to individual services, click "Subscribe" at the top of the page.

Notifications

No Current Events

Maintenance

No Planned Maintenances

Service History

LIST CALENDAR

EXHIBIT I

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 90.64	Issue 2	Page 1 of 8
PROTECTION OF SENSITIVE INFORMATION AND DATA	Effective Date May 5, 2017		

1. PURPOSE

1.1. To establish a policy to ensure the confidentiality and protection of *Sensitive Information* against unauthorized use; to establish procedures to control access to *Sensitive Information* so that it is only accessible by *Authorized Persons*; and to establish safeguards to ensure the appropriate use of *Sensitive Information* by *Authorized Persons*.

1.2. To define responsibility and procedures for granting *Authorized Persons* access to *Sensitive Information*.

1.3. To define processes by which access to *Sensitive Information* is administered and to develop control points in compliance with City policy.

2. SCOPE

2.1. This policy applies to all City employees in all City departments, including independent departments as authorized by the signing authorities below; and to City volunteers, contractors, vendors, and other individuals granted access to *Sensitive Information* under the City's control by the nature of their support or service functions.

2.2. This policy and procedures apply to all Sensitive Information created, owned, stored, managed or under the control of the City of San Diego, regardless of the media which contains the Sensitive Information, including but not limited to paper, microfilm, microfiche or any analog or digital format.

2.3. Nothing in this Administrative Regulation supersedes any stricter requirement(s) set by other authorities (i.e., local, state, and/or federal laws, rules or regulations), such as obtaining or retaining employment in a law enforcement agency; nor does this Administrative Regulation supersede any applicable, stricter rules, regulations or policies that affect access to or use of *Sensitive Information*. In such cases, the department head must ensure implementation or application of any such superseding rules, regulations or policies include adequately strong internal controls over *Sensitive Information*.

(Supersedes Administrative Regulation 90.64, Issue 1, effective July 1, 2009)

Authorized

(*Signature on File*)

CHIEF OPERATING OFFICER

3. DEFINITIONS

3.1. *Appointing Authority* - An unclassified, management-level position designated by the department head or higher who has the authority to grant permission for an employee or individual to be authorized for access to *Sensitive Information*.

3.2. *Authorized Person* - An employee or other individual who is granted permission to access or use *Sensitive Information* by an *Appointing Authority*, as approved by the *Information/Data Owner*, at the type and the *Level of Access* to the specific information required for the performance of his or her job duties.

3.3. *Authorization Acknowledgment Form* - The City's official form used to request and authorize an individual's access to or use of *Sensitive Information* (see Appendix). This form will be available on the City's Intranet site (CityNet) on the 'Forms' page.

3.4. *Information/Data Owner* - The department head or designee who is the primary recipient or manager of particular *Sensitive Information* or who has the responsibility to oversee the collection, maintenance or management of such information or data. There will only be one defined *Information/Data Owner* for any particular source of data; although other departments may collect and/or access the data. An *Information/Data Owner* may also be an *Appointing Authority*, as defined in Section 3.1 above.

3.5. *Level of Access* - The amount of *Sensitive Information* for which access is granted for any specific category or type of *Sensitive Information*, such as full access to all information related to a particular category or document, or limited access to only specific pieces of information (i.e., certain fields in a database) required for the performance of valid job duties.

3.6. *Personal Identifying Information* - Shall include information listed in California Penal Code Section 530.55(b), as amended (Sept. 2006), which reads, in pertinent part:

3.6.1. *Person* - A natural *Person*, living or deceased, firm, association, organization, partnership, business trust, company, corporation, limited liability company, or public entity, or any other legal entity.

3.6.2. *Personal Identifying Information* - Any name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license or identification number, social security number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN (personal identification number) or password, alien registration number, government passport number, date of birth, unique biometric data including fingerprint, facial scan identifiers, voiceprint, retina or iris image, or other unique physical representation, unique electronic data including information identification number assigned to the *Person*, address or routing code, telecommunication identifying

information or access device, information contained in a birth or death certificate, credit card number of an individual *Person*, or an equivalent form of identification.

3.7. For the purpose of this policy, *Sensitive Information* shall mean:

3.7.1. *Personal Identifying Information* (as defined above), also including debit card number of an individual *Person*, and where home/personal address and telephone number are included and work/office address and telephone number are excluded (i.e., the City Directory is not considered *Sensitive Information*); and

3.7.2. Any information that is possessed by the City of San Diego which is not subject to the California Public Records Act (refer to Administrative Regulation 95.20), and which may be used for other than the intended purpose of such information, to cause harm to or otherwise jeopardize the City of San Diego or any individual, or used in violation of any local, state or federal law (for example the Health Insurance Portability and Accountability Act of 1996 (HIPAA)).

3.8. *Sensitive Information Custodian* - The *Person* who manages the physical or computer-based access to *Sensitive Information*; for example an office manager or records manager who controls access to locked file rooms/cabinets, or a computer systems administrator who manages the creation of user accounts and passwords to provide specific access to particular data. A *Sensitive Information Custodian* may also be an *Information/Data Owner*, as defined in Section 3.4. above.

3.9. *Type of Access* - Refers to Read Only, Write/Create, Edit/Modify, and Delete.

4. POLICY

4.1. *Sensitive Information* shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her *Appointing Authority* and approved by the *Information/Data Owner*, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.2. Contractors and vendors or other non-City employees who are authorized to access or use *Sensitive Information*, shall be required to enter into agreements stating that the individuals specified for this access and their employing Contractor/Vendor agree to be contractually bound by the terms and conditions of this policy, including personal liability, as part of their contract or agreement prior to being granted access to *Sensitive Information*.

4.3. Authorization to access or use *Sensitive Information* shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an *Authorized Person's* job duties no longer require access to or use of *Sensitive Information*, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to *Sensitive Information* extend beyond the termination of the authorizing

contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.4. The *Information/Data Owner* shall specify the type and the *Level of Access* that should be assigned to various functional roles that require access to the *Sensitive Information* based on an employee's or individual's job requirements.

4.5. *Authorized Persons* shall access or use *Sensitive Information* only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use *Sensitive Information* shall sign an *Authorization Acknowledgement Form* stating he or she has read, understands, and agrees to abide by this policy.

4.6. As a standard IT security measure, *Authorized Persons* shall not share their User ID and/or password with anyone else, and shall not have their User ID and/or password written down in any unsecured location (e.g., anywhere around their work location). "Generic" User IDs shall not be used for system access to *Sensitive Information*; each *Authorized Person* must use an assigned, unique User ID that is directly linked with the user's name. As a standard physical security measure, *Authorized Person*s shall not share their building or facility access key card or key(s) with anyone else, nor shall they allow access into secured areas by unauthorized *Persons*.

4.7. Violation of this policy, either by unauthorized *Persons* accessing or attempting to access *Sensitive Information*, or by *Authorized Persons* accessing or using *Sensitive Information* for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

4.8. Appointing Authorities shall review the list of their employees, contractors or other individuals who they have designated as *Authorized Persons* with access to *Sensitive Information*, at least semi-annually, to ensure continued authorization is warranted and to update (add, delete or modify) the authorization list appropriately.

4.9. *Information/Data Owners* shall verify and document semi-annually that the Appointing Authorities performed a thorough review of authorized users in compliance with this policy (Section 4.8.), by comparing the *Appointing Authority's* report with a list of individuals currently authorized to access the *Sensitive Information* over which the Information/Data Owner has control and authority. For internal control purposes, to maintain segregation of duties, this verification must be performed by someone other than the *Appointing Authority* who submitted the semi-annual review of *Authorized Persons*. All discrepancies shall be reported back to the impacted *Appointing Authority* for

appropriate corrective action. *Information/Data Owners* shall retain records of such reviews and actions for the period of time set within the citywide or departmental Records Retention Schedule as approved by the City Clerk.

4.10. *Sensitive Information* stored in City computer systems shall be secured and maintained in accordance with applicable provisions of the Information Security Guidelines and Standards, as amended.

4.11. *Sensitive Information* stored in paper or other non-digital formats shall have appropriate physical security, and access to such information shall also comply with Administrative Regulation 95.10 for validating the identity of the individual requesting authorized access.

4.12. Upon the discovery of any breach of the protection of *Sensitive Information* through the accidental, inadvertent or purposeful release of such information to any unauthorized *Persons*, the *Person* discovering such breach should immediately notify the *Information/Data Owner* or their *Appointing Authority*, and, if the information was stored on City computer systems, also notify the Chief Information Security Officer in the Department of Information Technology.

4.12.1. Depending on the nature and scope of such breach and release of information, additional notifications must comply with applicable state and federal regulations.

4.12.2. The Information/Data Owner, in coordination with the Chief Information Security Officer from the Department of Information Technology (if applicable), should immediately take whatever steps are deemed necessary to stop any further breach of the protected information and to minimize any potential or actual losses or damages to the City of San Diego.

5. RESPONSIBILITY

5.1. Supervisor

5.1.1. When an employee's, volunteer's or contractor's job duties require access to or use of *Sensitive Information*, the immediate supervisor will complete an Authorization Acknowledgment Form. In addition, the supervisor must ensure that the proper system access/account request form and process is followed for the specific computer system where the *Authorized Person* needs access, specifying the nature of the job duties and the level and *Type of Access* or use requested. The supervisor will ensure the accuracy and completeness of information on the forms. After obtaining the employee's signature, the acknowledgement and request forms will be routed to the *Appointing Authority* for approval. Likewise, when an employee's, volunteer's or contractor's job duties change such that access to or use of *Sensitive Information* is no longer needed, the immediate supervisor will notify both the

Appointing Authority and the *Information/Data Owner*, as soon as possible (no more than five (5) business days).

5.2. *Authorized Person* (employee, volunteer, contractor, vendor or other individual being authorized for access).

5.2.1. Any *Person* being given access to *Sensitive Information* must sign the *Authorization Acknowledgement Form* stating he or she has read, understands, and agrees to comply with this policy for access or use and protection of such information. A copy of the final, approved form shall be kept in the employee's departmental personnel file, as the *Appointing Authority's* record; or for volunteers, on file with the department where assigned; or for a contractor, on file with the contract manager.

5.3. Department *Appointing Authority*

5.3.1. The Department *Appointing Authority* having management control over the employee, volunteer, contractor Vendor or other individual seeking authorization to access *Sensitive Information*, shall review the Authorization Acknowledgement and system access/account request forms for appropriateness of the job functions for the type and *Level of Access* requested while considering appropriate segregation of duties, and ensure the forms are signed by both the individual and supervisor.

5.3.2. The Department *Appointing Authority* will sign either approval or denial of the request, providing the reasons for any denial, and route the approved request form to the appropriate *Information/Data Owner*(s), or route a denied form back to the supervisor. Appointing Authorities shall maintain a copy of all authorization forms they approve, including those for non-City employees (i.e., volunteers and contractors). Any changes reported in the job duties of *Authorized Persons* which require a change in the access to or use of *Sensitive Information* must be immediately communicated to the *Information/Data Owner* to initiate the appropriate change in access. The semi-annual reviews should take place in May and November each year. The *Appointing Authority* will submit documentation of each review to the *Information/Data Owner* and these records will be retained by the department for the period of time set by the citywide or departmental Records Retention Schedule as approved by the City Clerk.

5.4. Information/Data Owner (owner of the information, regardless of its format or mechanism of access, [i.e., computerized system, hard copy file, etc.])

5.4.1. The Information/Data Owner for each different source of *Sensitive Information* covered by an approved access request form will review each request to ensure the type and *Level of Access* requested is appropriate for the job functions of the individual seeking access. Upon confirmation of the business need to have access

to *Sensitive Information*, the Information/Data Owner will sign approval to grant access, and may modify the type or *Level of Access* granted, as he or she deems necessary and appropriate, in consultation with the requesting *Appointing Authority*. The Information/Data Owner will initiate any further actions necessary to grant access to the *Authorized Person* (such as any computer system access processes). *Information/Data Owners* will maintain a list of individuals currently authorized access to their *Sensitive Information* and provide such list to the appropriate *Appointing Authority* for semi-annual review at the end of April and October each year

5.5. *Sensitive Information Custodian* (Administrator of the format and/or mechanism of access [i.e., computerized system or hard copy file] for the given information)

5.5.1. The *Authorized Person's* access to the identified *Sensitive Information* will be set up following the established procedures either in the IT Security Guidelines and Standards for access to electronic or digital data or following departmental internal controls for paper or physical records, based on the nature (media/format) of the *Sensitive Information*.

5.6. Department of Information Technology

5.6.1. Annually review this policy for any necessary updates or revisions, taking into account changes in City organization and IT systems. Maintain the list of *Information/Data Owner*s and update it annually. Maintain the necessary correlation between this policy and other IT security policies and/or regulations. Ensure City third-party vendors who have access to this data comply with this and other IT security policies. The Department of Information Technology is also responsible for ensuring that the requirements of this policy are communicated to all employees at least annually, using citywide and/or departmental training or communication channels.

5.7. Purchasing & Contracting Department

5.7.1. Ensure that this policy is included as an Addendum to or within the Terms and Conditions of signed contracts or agreements, for all contracts and/or agreements that include a contractor's or vendor's need to access or use the City's *Sensitive Information*.

SUBJECT	Number 90.64	Issue 2	Page 8 of 8
PROTECTION OF SENSITIVE INFORMATION AND DATA	Effective Date May 5, 2017		

APPENDIX

Legal References

Civil Service Rules and City Personnel Manual
Civil Service Rules, Definitions (p.l), "Appointing Authority"
Civil Service Rule XI, "Resignation, Removal, Suspension, Reduction in Compensation, Demotion"
Personnel Manual, Index Code A-3, "Improper Use of City Resources"
Personnel Manual, Index Code G-1, "Code of Ethics and Conduct"
Administrative Regulation 45.50 - Private Use of City Labor, Materials, Equipment and Supplies Prohibited
Administrative Regulation 90.63 - Information Security Policy
Administrative Regulation 95.10 - Identification of City Employees and Controlled Access to City Facilities
Administrative Regulation 95.20 - Public Records Act Requests and Civil Subpoenas; Procedures for Furnishing Documents and Recovering Costs
Administrative Regulation 95.60 - Conflict of Interest and Employee Conduct
IT Security Guidelines and Standards
Employee Performance Plans, Ethics and Integrity Section
Applicable California State Laws
Applicable Federal Laws

Forms Involved

Form DoIT-010A, "*Sensitive Information* Authorization Acknowledgement-City Employees"
Form DoIT-010B, "*Sensitive Information* Authorization Acknowledgement-City Volunteers"
Form DoIT-010C, "*Sensitive Information* Authorization Acknowledgement-City Contractors/Vendors"

Subject Index

Sensitive Information
Sensitive Data Information Security
Protection of *Sensitive Information*

Distribution

All Departments (Mayoral and Non-Mayoral)

Administering Department

Department of Information Technology

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form - City Employees

Authorized Person (City Employee requesting authorized access to Sensitive Information):

Name (Printed)	*Job Classification*	*Network (AD) Login/User ID*
Department / Division		
Mail Station	*Office Phone*	*Office FAX*
Supervisor's Name (Printed)	*Supervisors Phone*	

Policy Summary (pertinent excerpts from Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. [...]

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above employee acknowledges the he or she has been provided a full copy of A.R. 90.64 ("Protection of Sensitive Information and Data"), which has been discussed with his or her supervisor, and further acknowledges that he or she has read, understands, and agrees to comply with the provisions of the policy. Employee understands that this form will be kept as part of his or her permanent employee file, and that he or she may receive a copy, if requested. The supervisor acknowledges that he or she has discussed the policy with the above employee and understands the supervisor's obligations regarding employee's access to Sensitive Information under this policy.

_____ _____

Employee's Signature Date Signed

_____ _____

Supervisor's Signature Date Signed

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form- City Volunteers

Authorized Person (City Volunteer requesting authorized access to Sensitive Information):

Name (Printed)	*Volunteer Assignment*	*Network (AD} Login/User ID*
City Department / Division (where assigned as volunteer)		
Work Location		*Contact Phone*
City Supervisor's Name (Printed)	*City Supervisor's Phone*	*City Supervisor's Mail Station*

Policy Summary (pertinent excerpts from Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role Job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to Sensitive Information extend beyond the termination of the authorizing contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above City Volunteer acknowledges the he or she has been provided a full copy of A.R. 90.64 ("Protection of Sensitive Information and Data"), which has been discussed with the City Supervisor, and further acknowledges that he or she has read, understands, and agrees to comply with the provisions of the policy. City Volunteer understands that this form will be kept on file with the City Department, and that he or she may receive a copy, if requested. The City Supervisor acknowledges that he or she has discussed the policy with the above volunteer and understands the supervisor's obligations regarding the volunteer's access to Sensitive Information under this policy.

_____ _____

Volunteer's Signature Date Signed

_____ _____

City Supervisor's Signature Date Signed

CITY OF SAN DIEGO

Sensitive Information Authorization Acknowledgement Form- City Contractors/Vendors

Authorized Person (City Contractor/Vendor requesting authorized access to Sensitive Information):

Name (Printed)	*eMail Address*	*Network (AD) Login/User ID*
Nancy Free	nancy.free@armor.com	
Company/Organization		*Contractor/Vendor Office Phone*
Armor Defense Inc.		469-480-2414
City Department (managing contract)		*Contractor/Vendor Office FAX*
Information Technology		
City Contract Manager's Name (Printed)	*City Contract Manager'8 Phone*	*City Contract Manager's Mail Sta.*
Ian Brazill	6195334812	

Policy Summary (pertinent excerpts from City Administrative Regulation 90.64):

4.1. Sensitive Information shall be maintained in a confidential manner and access restricted to only employees or individuals properly authorized by his or her Appointing Authority and approved by the Information/Data Owner, based on verified business needs to have access to such information and/or in compliance with specific legal requirements.

4.3. Authorization to access or use Sensitive Information shall be based on a functional role (job duties) and not linked directly with a specific individual, such that when an authorized person's job duties no longer require access to or use of Sensitive Information, the ability to access or use such information shall be revoked. At no time shall a contractor's or vendor's access to Sensitive Information extend beyond the termination of the authorizing contract, and such access shall be revoked as soon as the duties requiring access or use have ended, regardless of the end date of the contract.

4.5. Authorized Persons shall access or use Sensitive Information only for its intended purpose for which it was obtained and maintained by the City of San Diego. An employee or individual authorized to access or use Sensitive Information shall sign an Authorization Acknowledgement Form stating he or she has read, understands, and agrees to abide by this policy.

4.7. Violation of this policy, either by unauthorized persons accessing or attempting to access Sensitive Information, or by Authorized Persons accessing or using Sensitive Information for other than its intended purpose or beyond the scope of their duties, may result in disciplinary action, up to and including termination of employment, and also subject the violating individual(s) to personal liability without the option of City legal defense. In the case of contractors or vendors, violation of this policy will be considered a breach of contract and appropriate actions taken on that basis. If deemed necessary, information regarding employee, volunteer, contractor or vendor violation of this policy may be referred to the appropriate agency for any civil and/or criminal action, as applicable.

Acknowledgement

By signing below, the above City Contractor/Vendor acknowledges the he or she understands that the Terms and Conditions of the underlying City Contract contain the provisions of the full policy stated above, and he or she agrees to comply with such contract provisions. City Contractor/Vendor understands that this form will be kept on file with the underlying contract documents in the City Purchasing & Contracting Department, and that he or she may receive a copy, if requested. The City Contract Manager acknowledges that he or she has discussed the contract Terms and Conditions related to this policy with the above Contractor/Vendor and understands the supervisor's obligations regarding the Contractor's/Vendor's access to the City's Sensitive Information under this policy.

Nancy Free
Nancy Free (May 21, 2024 15:28 CDT)

Contractor's/Vendor's Signature — Date Signed: 05/21/2024

Ian Brazill

City Contract Manager's Signature — Date Signed: 10/28/2024

Exhibit I - AR 90.64 (2)

Final Audit Report 2024-05-21

Created:	2024-05-21
By:	Nakia Shields (nshields@armor.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA9dHQ_TW84oFMvD8QAOLVIcgrX4c_joCI

"Exhibit I - AR 90.64 (2)" History

Document created by Nakia Shields (nshields@armor.com)
2024-05-21 - 8:00:39 PM GMT

Document emailed to Nancy Free (nancy.free@armor.com) for signature
2024-05-21 - 8:00:43 PM GMT

Email viewed by Nancy Free (nancy.free@armor.com)
2024-05-21 - 8:27:44 PM GMT

Document e-signed by Nancy Free (nancy.free@armor.com)
Signature Date: 2024-05-21 - 8:28:32 PM GMT - Time Source: server

Agreement completed.
2024-05-21 - 8:28:32 PM GMT

EXHIBIT J

Payment Card Industry Data Security Standards (PCI DSS):

__✓__**.01 PCI Compliance.** Contractor acknowledges and agrees that to the extent that credit card data is collected, processed, stored or transmitted, Contractor must adhere to the Payment Card Industry Data Security Standards (PCI DSS) and must specifically comply with the City PCI requirements described in this Section __I__.

__✓__**.02 Contractor Compliance with Payment Card Industry Security Standards Council Standards.** Contractor must maintain full compliance with all current and applicable Payment Card Industry Security Standards Council Standards (PCI SSC), for all Services performed under this Contract or other contracts managed by Contractor. Contractor acknowledges and agrees that it will ensure that any subcontractors or other service providers that it uses to assist with performance of this Contract will also maintain full compliance with all current and applicable PCI SSC standards.

__✓__**.03 Attestation of PCI Compliance.** Contractor must, upon request of the City annually on the anniversary of the Effective Date, provide the City with a copy of the Level 1 Service Provider attestation of compliance which must be approved and signed by a qualified security assessor (QSA) company recognized by the PCI SSC. Any deficiencies noted in an annual assessment must be communicated to City, in writing, within thirty (30) days of the report, and include a remediation date in accordance with the PCI SSC's prioritized approach. Any deficiencies noted in an annual assessment must be remediated at Contractor's sole cost and expense.

__✓__**.04 Contractor Remediation.** Contractor must remediate, in a timely manner and at Contractor's sole cost and expense, any outstanding audit finding by Contractor or City's QSA as it relates to Contractor's provision of PCI related hardware or services in compliance with the most current PCI DSS and PCI SSC.

__✓__**.05 Service Provider Responsibility Matrix.** Contractor must complete a Service Provider Responsibility Matrix (Matrix) in either the form provided by City, or in a format approved by City, and account for all management services that will be supplied to the City as they relate to cardholder data that is stored, processed, or transmitted on behalf of City. The Matrix shall be updated in regularly and in a timely manner to reflect any changes in the provision of such management services. Upon its completion, the Matrix is hereby incorporated into the Contract and any updates or revisions to the Matrix will also be incorporated into this Contract without need for an amendment.

__N/A__**.06 Contractor Hardware Inspections, Checklist and Notice of Unauthorized Access**. Contractor must physically inspect all kiosk devices, merchant terminals, and related payment hardware, accessible to Contractor, used in the acceptance, transmission, or storage of credit card data, at a frequency determined by the City. Contractor must document all hardware inspections using a checklist in accordance with PCI DSS requirement 9.9 (Checklist), located at

https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

or located at such other website as the PCI SSC may describe from time to time.

N/A **.06.01** Contractor must report immediately to the City, via email and phone call, any known device tampering or other breach, intrusion, or unauthorized access to cardholder data stored by or on behalf of Contractor. For purposes of this subsection a, reporting to the City's Information Security Officer (CISO) and the Office of the City Treasurer will be deemed sufficient for notifying the City. Contractor also agrees to assume responsibility for informing all affected individuals in accordance with applicable law.

N/A **.06.02** Upon the City's request, Contractor must provide to City a copy of the Checklist.

City of San Diego

CONTRACTOR STANDARDS

Pledge of Compliance

The City of San Diego has adopted a Contractor Standards Ordinance (CSO) codified in section 22.3004 of the San Diego Municipal Code (SDMC). The City of San Diego uses the criteria set forth in the CSO to determine whether a contractor (bidder or proposer) has the capacity to fully perform the contract requirements and the business integrity to justify the award of public funds. This completed Pledge of Compliance signed under penalty of perjury must be submitted with each bid and proposal. If an informal solicitation process is used, the bidder must submit this completed Pledge of Compliance to the City prior to execution of the contract. All responses must be typewritten or printed in ink. If an explanation is requested or additional space is required, Contractors must provide responses on Attachment A to the Pledge of Compliance and sign each page. Failure to submit a signed and completed Pledge of Compliance may render a bid or proposal non-responsive. In the case of an informal solicitation or cooperative procurement, the contract will not be awarded unless a signed and completed Pledge of Compliance is submitted. A submitted Pledge of Compliance is a public record and information contained within will be available for public review except to the extent that such information is exempt from disclosure pursuant to applicable law.

By signing and submitting this form, the contractor is certifying, to the best of their knowledge, that the contractor and any of its Principals have not within a five (5) year period – preceding this offer, been convicted of or had a civil judgement rendered against them for commission of a fraud or a criminal offense in connection with obtaining, attempting to obtain or performing a public (Federal, State or local) contract or subcontract.

"Principal" means an officer, director, owner, partner or a person having primary management or supervisory responsibilities within the firm. The Contractor shall provide immediate written notice to the Procurement Contracting Officer handling the solicitation, at any time prior to award should they learn that this Representations and Certifications was inaccurate or incomplete.

This form contains 10 pages, additional information may be submitted as part of *Attachment A.*

A. BID/PROPOSAL/SOLICITATION TITLE:

Payment Card Industry (PCI) Compliant Cloud Hosting Services

B. BIDDER/PROPOSER INFORMATION:

Armor Defense, Inc.			
Legal Name		DBA	
7700 Windrose Ave. #G300	Plano	TX	75024
Street Address	City	State	Zip
Evan Powell, Client Engagement Manager	(469) 480-2299		
Contact Person, Title	Phone	Fax	

Provide the name, identity, and precise nature of the interest* of all persons who are directly or indirectly involved** in this proposed transaction (SDMC § 21.0103). Use additional pages if necessary.

* The precise nature of the interest includes:

- the percentage ownership interest in a party to the transaction,
- the percentage ownership interest in any firm, corporation, or partnership that will receive funds from the transaction,
- the value of any financial interest in the transaction,
- any contingent interest in the transaction and the value of such interest should the contingency be satisfied, and
- any philanthropic, scientific, artistic, or property interest in the transaction.

** Directly or indirectly involved means pursuing the transaction by:

- communicating or negotiating with City officers or employees,
- submitting or preparing applications, bids, proposals or other documents for purposes of contracting with the City, or
- directing or supervising the actions of persons engaged in the above activity.

Evan Powell	Client Engagement Manager
Name	Title/Position
Dallas, TX	
City and State of Residence	Employer (if different than Bidder/Proposer)
20%	
Interest in the transaction	

Christopher Murphy	VP, Client Engagement
Name	Title/Position
Dallas, TX	
City and State of Residence	Employer (if different than Bidder/Proposer)
20%	
Interest in the transaction	

Nancy Free	Chief Risk Officer
Name	Title/Position
Dallas, TX	
City and State of Residence	Employer (if different than Bidder/Proposer)
20%	
Interest in the transaction	

Tony Taylor	GRC|P Program Manager
Name	Title/Position
Seattle, Washington	
City and State of Residence	Employer (if different than Bidder/Proposer)
15%	
Interest in the transaction	

Anubhav Kela	Head of Finance and Operations
Name	Title/Position
Seattle, Washington	
City and State of Residence	Employer (if different than Bidder/Proposer)
10%	
Interest in the transaction	

Nakia Shields	Contracts Administrator
Name	Title/Position
Dallas, TX	
City and State of Residence	Employer (if different than Bidder/Proposer)
5%	
Interest in the transaction	

Ricky Endres	Assistant Controller
Name	Title/Position
Dallas, TX	
City and State of Residence	Employer (if different than Bidder/Proposer)
5%	
Interest in the transaction	

Karen Wood	HR Generalist III
Name	Title/Position
Dallas, TX	
City and State of Residence	Employer (if different than Bidder/Proposer)
5%	
Interest in the transaction	

Name	Title/Position
City and State of Residence	Employer (if different than Bidder/Proposer)
Interest in the transaction	

C. OWNERSHIP AND NAME CHANGES:

1. In the past five (5) years, has your firm changed its name?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to list all prior legal and DBA names, addresses, and dates each firm name was used. Explain the specific reasons for each name change.

2. Is your firm a non-profit?
☐**Yes** ☑**No**

   If **Yes,** attach proof of status to this submission.

3. In the past five (5) years, has a firm owner, partner, or officer operated a similar business?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to list names and addresses of all businesses and the person who operated the business. Include information about a similar business only if an owner, partner, or officer of your firm holds or has held a similar position in another firm.

D. BUSINESS ORGANIZATION/STRUCTURE:

Indicate the organizational structure of your firm. Fill in only one section on this page. Use Attachment A if more space is required.

☑ **Corporation** Date incorporated: 12/20/2009 State of incorporation: Delaware

List corporation's current officers: President: Christopher Drake
Vice Pres: Anubhav Kela
Secretary: _____
Treasurer: _____

Type of corporation: C ☑ Subchapter S ☐

Is the corporation authorized to do business in California: ☑ **Yes** ☐ **No**

If **Yes,** after what date: 08/26/2013

Is your firm a publicly traded corporation? ☐ **Yes** ☑ **No**

If **Yes,** how and where is the stock traded? _____

If **Yes**, list the name, title and address of those who own ten percent (10 %) or more of the corporation's stocks:

_____
_____
_____
_____

Do the President, Vice President, Secretary and/or Treasurer of your corporation have a third party interest or other financial interests in a business/enterprise that performs similar work, services or provides similar goods? ☐ **Yes** ☑ **No**

If **Yes,** please use Attachment A to disclose.

Please list the following:		Authorized	Issued	Outstanding
a.	Number of voting shares:	108,073,298	41,674,429	41,674,429
b.	Number of nonvoting shares:	0	0	0
c.	Number of shareholders:			71
d.	Value per share of common stock:		Par	$ 0.01
			Book	$ 0.00
			Market	$ 1.53

Limited Liability Company Date formed: _____ State of formation: _____

List the name, title and address of members who own ten percent (10%) or more of the company:

_____
_____
_____
_____

☐ **Partnership** Date formed: _____ State of formation: _____

List names of all firm partners:

_____
_____
_____
_____

☐ **Sole Proprietorship** Date started: _____

List all firms you have been an owner, partner or officer with during the past five (5) years. Do not include ownership of stock in a publicly traded company:

_____
_____
_____
_____

☐ **Joint Venture** Date formed: _____

List each firm in the joint venture and its percentage of ownership:

_____
_____
_____
_____

Note: To be responsive, each member of a Joint Venture or Partnership must complete a separate *Contractor Standards form*.

E. FINANCIAL RESOURCES AND RESPONSIBILITY:

1. Is your firm preparing to be sold, in the process of being sold, or in negotiations to be sold?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain the circumstances, including the buyer's name and principal contact information.

2. In the past five (5) years, has your firm been denied bonding?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances; include bonding company name.

3. In the past five (5) years, has a bonding company made any payments to satisfy claims made against a bond issued on your firm's behalf or a firm where you were the principal?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

4. In the past five (5) years, has any insurance carrier, for any form of insurance, refused to renew the insurance policy for your firm?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

5. Within the last five years, has your firm filed a voluntary petition in bankruptcy, been adjudicated bankrupt, or made a general assignment for the benefit of creditors?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

6. Are there any claims, liens or judgements that are outstanding against your firm?
   ☐ **Yes** ☑ **No**

   If **Yes,** please use Attachment A to provide detailed information on the action.

7. Please provide the name of your principal financial institution for financial reference. By submitting a response to this Solicitation Contractor authorizes a release of credit information for verification of financial responsibility.

   Name of Bank: Silicon Valley Bank

   Point of Contact: Zach Martin

   Address: 3003 Tasman Drive, Santa Clara, CA 95054

   Phone Number: (408) 654-4636

8. By submitting a response to a City solicitation, Contractor certifies that he or she has sufficient operating capital and/or financial reserves to properly fund the requirements identified in the solicitation. At City's request, Contractor will promptly provide to City

a copy of Contractor's most recent balance sheet and/or other necessary financial statements to substantiate financial ability to perform.

9. In order to do business in the City of San Diego, a current Business Tax Certificate is required. Business Tax Certificates are issued by the City Treasurer's Office. If you do not have one at the time of submission, one must be obtained prior to award.

   Business Tax Certificate No.: B2021014875 Year Issued: 2022

F. PERFORMANCE HISTORY:

1. In the past five (5) years, has your firm been found civilly liable, either in a court of law or pursuant to the terms of a settlement agreement, for defaulting or breaching a contract with a government agency?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

2. In the past five (5) years, has a public entity terminated your firm's contract for cause prior to contract completion?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances and provide principal contact information.

3. In the past five (5) years, has your firm entered into any settlement agreement for any lawsuit that alleged contract default, breach of contract, or fraud with or against a public entity?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

4. Is your firm currently involved in any lawsuit with a government agency in which it is alleged that your firm has defaulted on a contract, breached a contract, or committed fraud?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances.

5. In the past five (5) years, has your firm, or any firm with which any of your firm's owners, partners, or officers is or was associated, been debarred, disqualified, removed, or otherwise prevented from bidding on or completing any government or public agency contract for any reason?
   ☐ **Yes** ☑ **No**

   If **Yes**, use *Attachment A* to explain specific circumstances.

6. In the past five (5) years, has your firm received a notice to cure or a notice of default on a contract with any public agency?

   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances and how the matter resolved.

7. Performance References:

Please provide a minimum of three (3) references familiar with work performed by your firm which was of a similar size and nature to the subject solicitation within the last five (5) years.

Please note that any references required as part of your bid/proposal submittal are in addition to those references required as part of this form.

Company Name: ViTel Net

Contact Name and Phone Number: Keith Buck, (410) 627-5574

Contact Email: dkbuck@vitelnet.com

Address: 1640 Boro Pl, ste. 505, McLean, VA 22102

Contract Date:

Contract Amount:

Requirements of Contract: proprietary: applies to contract date, amount, and this field

Company Name: Devlin Consulting (Sagility)

Contact Name and Phone Number: Jim Cowsert, (480) 365-9090

Contact Email: jim.cowsert@devlinconsulting.com

Address: 5505 W Chandler Blvd., ste. 20, Chandler, AZ 85226

Contract Date:

Contract Amount:

Requirements of Contract: proprietary: applies to contract date, amount, and this field

Company Name: Western Health Advantage

Contact Name and Phone Number: Eric Sibley, (916) 614-6029

Contact Email: esibley@westernhealth.com

Address: 2349 Gateway Oaks Dr, #100, Sacramento, CA 95833

Contract Date:

Contract Amount:

Requirements of Contract: proprietary: applies to contract date, amount, and this field

G. COMPLIANCE:

1. In the past five (5) years, has your firm or any firm owner, partner, officer, executive, or manager been criminally penalized or found civilly liable, either in a court of law or pursuant to the terms of a settlement agreement, for violating any federal, state, or local law in performance of a contract, including but not limited to, laws regarding health and safety, labor and employment, permitting, and licensing laws?
   ☐ **Yes** ☑ **No**

   If **Yes**, use Attachment A to explain specific circumstances surrounding each instance. Include the name of the entity involved, the specific infraction(s) or violation(s), dates of instances, and outcome with current status.

2. In the past five (5) years, has your firm been determined to be non-responsible by a public entity?
   ☐ **Yes** ☑ **No**

If **Yes**, use Attachment A to explain specific circumstances of each instance. Include the name of the entity involved, the specific infraction, dates, and outcome.

H. BUSINESS INTEGRITY:

1. In the past five (5) years, has your firm been convicted of or found liable in a civil suit for making a false claim or material misrepresentation to a private or public entity?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance. Include the entity involved, specific violation(s), dates, outcome and current status.

2. In the past five (5) years, has your firm or any of its executives, management personnel, or owners been convicted of a crime, including misdemeanors, or been found liable in a civil suit involving the bidding, awarding, or performance of a government contract?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance; include the entity involved, specific infraction(s), dates, outcome and current status.

3. In the past five (5) years, has your firm or any of its executives, management personnel, or owners been convicted of a federal, state, or local crime of fraud, theft, or any other act of dishonesty?
☐**Yes** ☑**No**

   If **Yes**, use Attachment A to explain specific circumstances of each instance; include the entity involved, specific infraction(s), dates, outcome and current status.

4. Do any of the Principals of your firm have relatives that are either currently employed by the City or were employed by the City in the past five (5) years?

   ☐**Yes** ☑**No**

   If **Yes,** please disclose the names of those relatives in Attachment A.

I. BUSINESS REPRESENTATION:

1. Are you a local business with a physical address within the County of San Diego?
☐**Yes** ☑**No**

2. Are you a certified Small and Local Business Enterprise certified by the City of San Diego?
☐**Yes** ☑**No**

   Certification #_____

3. Are you certified as any of the following:
   a. Disabled Veteran Business Enterprise Certification #_____
   b. Woman or Minority Owned Business Enterprise Certification # _____
   c. Disadvantaged Business Enterprise Certification #_____

J. WAGE COMPLIANCE:

In the past five (5)years, has your firm been required to pay back wages or penalties for failure to comply with the federal, state or local **prevailing, minimum, or living wage laws**? ☐**Yes** ☑**No** If **Yes**, use Attachment A to explain the specific circumstances of each instance. Include the entity involved, the specific infraction(s), dates, outcome, and current status.

By signing this Pledge of Compliance, your firm is certifying to the City that you will comply with the requirements of the Equal Pay Ordinance set forth in SDMC sections 22.4801 through 22.4809.

K. STATEMENT OF SUBCONTRACTORS & SUPPLIERS:

Please provide the names and information for all subcontractors and suppliers used in the performance of the proposed contract, and what portion of work will be assigned to each subcontractor. Subcontractors may not be substituted without the written consent of the City. Use Attachment A if additional pages are necessary. If no subcontractors or suppliers will be used, please write "Not Applicable."

Company Name: Not Applicable

Address: _____

Contact Name: _____ Phone: _____ Email: _____

Contractor License No.: _____ DIR Registration No.: _____

Sub-Contract Dollar Amount: $_____ (per year) $_____ (total contract term)

Scope of work subcontractor will perform: _____

Identify whether company is a subcontractor or supplier: _____

Certification type (check all that apply):☐DBE ☐DVBE ☐ELBE ☐MBE ☐SLBE☐WBE ☐Not Certified

Contractor must provide valid proof of certification with the response to the bid or proposal to receive participation credit.

Company Name: _____

Address: _____

Contact Name: _____ Phone: _____ Email: _____

Contractor License No.: _____ DIR Registration No.: _____

Sub-Contract Dollar Amount: $_____ (per year) $_____ (total contract term)

Scope of work subcontractor will perform: _____

Identify whether company is a subcontractor or supplier: _____

Certification type (check all that apply):☐DBE ☐DVBE ☐ELBE ☐MBE ☐SLBE☐WBE ☐Not Certified

Contractor must provide valid proof of certification with the response to the bid or proposal to receive participation credit.

L. STATEMENT OF AVAILABLE EQUIPMENT:

A full inventoried list of all necessary equipment to complete the work specified may be a requirement of the bid/proposal submission.

By signing and submitting this form, the Contractor certifies that all required equipment included in this bid or proposal will be made available one week (7 days) before work shall commence. In instances where the required equipment is not owned by the Contractor, Contractor shall explain how the equipment will be made available before the commencement of work. The City of San

Diego reserves the right to reject any response, in its opinion, if the Contractor has not demonstrated he or she will be properly equipped to perform the work in an efficient, effective matter for the duration of the contract period.

M. TYPE OF SUBMISSION: This document is submitted as:

☑ Initial submission of *Contractor Standards Pledge of Compliance*

☐ Initial submission of *Contractor Standards Pledge of Compliance* as part of a Cooperative agreement

☐ Initial submission of *Contractor Standards Pledge of Compliance* as part of a Sole Source agreement

☐ Update of prior *Contractor Standards Pledge of Compliance* dated _____.

Complete all questions and sign below.

Under penalty of perjury under the laws of the State of California, I certify that I have read and understand the questions contained in this Pledge of Compliance, that I am responsible for completeness and accuracy of the responses contained herein, and that all information provided is true, full and complete to the best of my knowledge and belief. I agree to provide written notice to the Purchasing Agent within five (5) business days if, at any time, I learn that any portion of this Pledge of Compliance is inaccurate. Failure to timely provide the Purchasing Agent with written notice is grounds for Contract termination.

I, on behalf of the firm, further certify that I and my firm will comply with the following provisions of SDMC section 22.3004:

(a) I and my firm will comply with all applicable local, State and Federal laws, including health and safety, labor and employment, and licensing laws that affect the employees, worksite or performance of the contract.

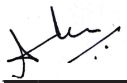
(b) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of receiving notice that a government agency has begun an investigation of me or my firm that may result in a finding that I or my firm is or was not in compliance with laws stated in paragraph (a).

(c) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of a finding by a government agency or court of competent jurisdiction of a violation by the Contractor of laws stated in paragraph (a).

(d) I and my firm will notify the Purchasing Agent in writing within fifteen (15) calendar days of becoming aware of an investigation or finding by a government agency or court of competent jurisdiction of a violation by a subcontractor of laws stated in paragraph (a).

(e) I and my firm will cooperate fully with the City during any investigation and to respond to a request for information within ten (10) working days.

Failure to sign and submit this form with the bid/proposal shall make the bid/proposal non-responsive. In the case of an informal solicitation, the contract will not be awarded unless a signed and completed *Pledge of Compliance* is submitted.

Anubhav Kela		5/21/2024
Name and Title	Signature	Date

City of San Diego
CONTRACTOR STANDARDS
Attachment "A"

Provide additional information in space below. Use additional Attachment “A” pages as needed. Each page must be signed. Print in ink or type responses and indicate question being answered.

I have read the matters and statements made in this Contractor Standards Pledge of Compliance and attachments thereto and I know the same to be true of my own knowledge, except as to those matters stated upon information or belief and as to such matters, I believe the same to be true. I certify under penalty of perjury that the foregoing is true and correct.

Print Name, Title	Signature	Date

Contractor Standard Pledge of Compliance 3 2018_Revised

Final Audit Report 2024-05-22

Created:	2024-05-21
By:	Nakia Shields (nshields@armor.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA59vrnSxcBoXTsP9kUg2JLd7L046zw1-a

"Contractor Standard Pledge of Compliance 3 2018_Revised" History

Document created by Nakia Shields (nshields@armor.com)
2024-05-21 - 10:18:38 PM GMT

Document emailed to Anubhav Kela (anubhav.kela@armor.com) for signature
2024-05-21 - 10:18:42 PM GMT

Email viewed by Anubhav Kela (anubhav.kela@armor.com)
2024-05-22 - 1:09:22 AM GMT

Document e-signed by Anubhav Kela (anubhav.kela@armor.com)
Signature Date: 2024-05-22 - 1:09:58 AM GMT - Time Source: server

Agreement completed.
2024-05-22 - 1:09:58 AM GMT

AA. CONTRACTORS CERTIFICATION OF PENDING ACTIONS

As part of this Contract, the Contractor must provide to the City a list of all instances within the past 10 years where a complaint was filed or pending against the Contractor in a legal or administrative proceeding alleging that Contractor discriminated against its employees, subcontractors, vendors or suppliers, and a description of the status or resolution of that complaint, including any remedial action taken.

CHECK ONE BOX ONLY.

☑ The undersigned certifies that within the past 10 years the Contractor has NOT been the subject of a complaint or pending action in a legal administrative proceeding alleging that Contractor discriminated against its employees, subcontractors, vendors or suppliers.

☐ The undersigned certifies that within the past 10 years the Contractor has been the subject of a complaint or pending action in a legal administrative proceeding alleging that Contractor discriminated against its employees, subcontractors, vendors or suppliers. A description of the status or resolution of that complaint, including any remedial action taken and the applicable dates is as follows:

DATE OF CLAIM	LOCATION	DESCRIPTION OF CLAIM	LITIGATION (Y/N)	STATUS	RESOLUTION/ REMEDIAL ACTION TAKEN

Contractor Name: _____

Certified By Nakia Shields Title Contracts Administrator

Name

Nakia Shields Date June 3, 2024

Signature

Certification of Pending Actions_Ready for Execution

Final Audit Report 2024-06-04

Created:	2024-06-04
By:	Nakia Shields (nshields@armor.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAA_Ccjj8SsZNgBVMV84bzsKTMhx8gzHgen

"Certification of Pending Actions_Ready for Execution" History

Document created by Nakia Shields (nshields@armor.com)
2024-06-04 - 2:44:40 AM GMT

Document emailed to Nakia Shields (nshields@armor.com) for signature
2024-06-04 - 2:44:42 AM GMT

Email viewed by Nakia Shields (nshields@armor.com)
2024-06-04 - 2:44:54 AM GMT

Document e-signed by Nakia Shields (nshields@armor.com)
Signature Date: 2024-06-04 - 2:45:09 AM GMT - Time Source: server

Agreement completed.
2024-06-04 - 2:45:09 AM GMT

EQUAL OPPORTUNITY CONTRACTING PROGRAM (EOCP)

GOODS AND SERVICES CONTRACTOR REQUIREMENTS

I. City's Equal Opportunity Contracting Commitment.

The City of San Diego (City) promotes equal employment and subcontracting opportunities. The City is committed to ensuring that taxpayer dollars spent on public contracts are not paid to businesses that practice discrimination in employment or subcontracting. The City encourages all companies seeking to do business with the City to share this commitment. Contractors are encouraged to take positive steps to diversify and expand their subcontractor and supplier solicitation base and to offer opportunities to all eligible business firms.

Contractors must submit the required EOCP documentation indicated below with their proposals. Contractors who fail to provide the required EOCP documentation are considered non-responsive.

II. Definitions.

Commercially Useful Function: a Small Local Business Enterprise or Emerging Local Business Enterprise (SLBE/ELBE) performs a commercially useful function when it is responsible for execution of the work and is carrying out its responsibilities by actually performing, managing, and supervising the work involved. To perform a commercially useful function, the SLBE/ELBE shall also be responsible, with respect to materials and supplies used on the contract, for negotiating price, determining quantity and quality, ordering the material, and installing (where applicable) and paying for the material itself.

To determine whether an SLBE/ELBE is performing a commercially useful function, an evaluation will be performed of the amount of work subcontracted, normal industry practices, whether the amount the SLBE/ELBE firm is to be paid under the contract is commensurate with the work it is actually performing and the SLBE/ELBE credit claimed for its performance of the work, and other relevant factors. Specifically, an SLBE/ELBE does not perform a commercially useful function if its role is limited to that of an extra participant in a transaction, contract, or project through which funds are passed in order to obtain the appearance of meaningful and useful SLBE/ELBE participation, when in similar transactions in which SLBE/ELBE firms do not participate, there is no such role performed.

Disadvantaged Business Enterprise (DBE): a certified business that is (1) at least fifty-one (51%) owned by socially and economically Disadvantaged Individuals, or, in the case of a publicly owned business at least fifty-one percent (51%) of the stock is owned by one or more socially and economically Disadvantaged Individuals; and (2) whose daily business operations are managed and directed by one or more socially and economically disadvantaged owners. Disadvantaged Individuals include Black Americans, Hispanic Americans, Asian Americans, and other minorities, or individual found to be disadvantaged by the Small Business Administration pursuant to Section 8 of the Small Business Reauthorization Act.

Disabled Veteran Business Enterprise (DVBE): a certified business that is (1) at least fifty-one percent (51%) owned by one or more Disabled Veterans; and (2) business operations must be managed and controlled by one or more Disabled Veterans. A Disabled Veteran is a veteran of the U.S. military, naval, or air service who resides in California and has a service-connected disability of at least 10% or more. The firm shall be certified by the State of California's Department of General Services, Office of Small and Minority Business.

Emerging Business Enterprise (EBE): a business whose gross annual receipts do not exceed the amount set by the City Manager, and which meets all other criteria set forth in the regulations implementing the City's Small and Local Business Preference Program. The City Manager shall review the threshold amount for EBEs on an annual basis, and adjust as necessary to reflect changes in the marketplace.

Emerging Local Business Enterprise (ELBE): a Local Business Enterprise that is also an Emerging Business Enterprise.

Local Business Enterprise (LBE): a business that has both a principal place of business and a significant employment presence in the County of San Diego, and that has been in operation for twelve (12) consecutive months.

Minority Business Enterprise (MBE): a certified business that is (1) at least fifty-one percent (51%) owned by one or more minority individuals, or, in the case of a publicly owned business at least fifty-one percent (51%) of the stock is owned by one or more minority individuals; and (2) whose daily business operations are managed and directed by one or more minorities owners. Minorities include the groups with the following ethnic origins: African, Asian Pacific, Asian Subcontinent, Hispanic, Native Alaskan, Native American, and Native Hawaiian.

Other Business Enterprise (OBE): any business which does not otherwise qualify as Minority, Woman, Disadvantaged, or Disabled Veteran Business Enterprise.

Principal Place of Business: a location wherein a business maintains a physical office and through which it obtains no less than fifty percent (50%) of gross annual receipts.

Significant Employee Presence: no less than twenty-five percent (25%) of a business's total number of employees.

Small Business Enterprise (SBE): a business whose gross annual receipts do not exceed the amount set by the City Manager, and that meets all other criteria set forth in regulations implementing the City's Small and Local Business Preference Program. The City Manager shall review the threshold amount for SBEs on an annual basis, and adjust as necessary to reflect changes in the marketplace. A business certified as a DVBE by the State of California, and that has provided proof of such certification to the City manager, shall be deemed to be an SBE.

Small Local Business Enterprise (SLBE): a Local Business Enterprise that is also a Small Business Enterprise.

Women Business Enterprise (WBE): a certified business that is (1) at least fifty-one percent (51 %) owned by a woman or women, or, in the case of a publicly owned business at least fifty-one percent (51%) of the stock is owned by one or more women; and (2) whose daily business operations are managed and directed by one or more women owners.

III. Disclosure of Discrimination Complaints.

As part of its proposal, Contractor shall provide to the City a list of all instances within the past ten (10) years where a complaint was filed or pending against Contractor in a legal or administrative proceeding alleging that Contractor discriminated against its employees, subcontractors, vendors, or suppliers, and a description of the status or resolution of that complaint, including any remedial action taken. (Attachment AA).

IV. Work Force Report and Equal Opportunity Outreach Plan.

A. Work Force Report. Contractors shall submit with their proposal a Work Force Report (WFR) for approval by the City. (Attachment BB). If the City determines that there are under representations when compared to County Labor Force Availability data, then the Contractor will also be required to submit an Equal Employment Opportunity Plan (EEOP) to the City for approval. Questions regarding the WFR should be directed to the Equal Opportunity Contracting Department.

B. Duty to Comply with Equal Opportunity Outreach Plan. A Contractor for whom an EEOP has been approved by the City shall use best efforts to comply with that EEOP.

V. Small and Local Business Program Requirements.

The City has adopted a Small and Local Business Enterprise program for goods, services, and consultant contracts. The SLBE requirements are set forth in Council Policy 100-10. For contracts in which the Purchasing Agent is required to advertise for sealed proposals in the City's official newspaper or consultant contracts valued over $50,000, the City shall:

A. Apply a maximum of an additional 12% of the total possible evaluation points to the Contractor's final score for SLBE or ELBE participation. Additional points will be awarded as follows:

   a. If the Contractor achieves 20% participation, apply 5% of the total possible evaluation points to the Contractor's score; or

   b. If the Contractor achieves 25% participation, apply 10% of the total possible evaluation points to the Contractor's score; or

   c. If the prime contractor is a SLBE or an ELBE, apply 12% of the total possible evaluation points to the Contractor's score.

VI. Maintaining Participation Levels.

A. Additional points are based on the Contractor's level of participation proposed prior to the award of the goods, services, or consultant contract. Contractors are required to achieve and maintain the SLBE or ELBE participation levels throughout the duration of the goods, services, or consultant contract.

B. If the City modifies the original specifications, the Contractor shall make reasonable efforts to maintain the SLBE or ELBE participation for which the additional points were awarded. The City must approve in writing a reduction in SLBE or ELBE participation levels.

C. Contractor shall notify and obtain written approval from the City in advance of any reduction in subcontract scope, termination, or substitution for a designated SLBE or ELBE subcontractor.

D. Contractor's failure to maintain SLBE or ELBE participation levels as specified in the goods, services, or consultant contract shall constitute a default and grounds for debarment under Chapter 2, Article 2, Division 8, of the San Diego Municipal Code.

E. The remedies available to the City under Council Policy 100-10 are cumulative to all other rights and remedies available to the City.

VII. Certifications.

The City accepts certifications of MBE, WBE, DBE, or DVBE from the following certifying agencies:

A. Current certification by the State of California Department of Transportation (CALTRANS) as DBE.

B. Current MBE or WBE certification from the California Public Utilities Commission.

C. DVBE certification is received from the State of California's Department of General Services, Office of Small and Minority Business.

D. Current certification by the City of Los Angles as DBE, WBE, or MBE.

Subcontractors' valid proof of certification status e.g., copy of MBE, WBE, DBE, or DVBE certification must be submitted with the proposal or contract documents. MBE, WBE, DBE, or DVBE certifications are listed for informational purposes only.

VIII. List of Attachments.

AA. Contractors Certification of Pending Actions

BB. Work Force Report

The City of SAN DIEGO

EQUAL OPPORTUNITY CONTRACTING (EOC)

1200 Third Avenue, Suite 200 • San Diego, CA 92101
Phone: (619) 236-6000 • Fax: (619) 236-5904

BB. WORK FORCE REPORT

The objective of the *Equal Employment Opportunity Outreach Program*, San Diego Municipal Code Sections 22.3501 through 22.3517, is to ensure that contractors doing business with the City, or receiving funds from the City, do not engage in unlawful discriminatory employment practices prohibited by State and Federal law. Such employment practices include, but are not limited to unlawful discrimination in the following: employment, promotion or upgrading, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rate of pay or other forms of compensation, and selection for training, including apprenticeship. Contractors are required to provide a completed *Work Force Report (WFR).*

NO OTHER FORMS WILL BE ACCEPTED

CONTRACTOR IDENTIFICATION

Type of Contractor: ☐ Construction ☐ Vendor/Supplier ☐ Financial Institution ☐ Lessee/Lessor ☐ Consultant ☐ Grant Recipient ☐ Insurance Company X Other

Name of Company: Armor Defense, Inc.

ADA/DBA: _____

Address (Corporate Headquarters, where applicable): 7700 Windrose Ave., ste. #G300

City: Plano County: Collin State: Texas Zip: 75024

Telephone Number: 877-262-3473 Fax Number: _____

Name of Company CEO: Christopher Drake

Address(es), phone and fax number(s) of company facilities located in San Diego County **(if different from above):**

Address: _____

City: _____ County: _____ State: _____ Zip: _____

Telephone Number: _____ Fax Number: _____ Email: _____

Type of Business: Corporation Type of License: _____

The Company has appointed: _____

As its Equal Employment Opportunity Officer (EEOO). The EEOO has been given authority to establish, disseminate and enforce equal employment and affirmative action policies of this company. The EEOO may be contacted at:

Address: _____

Telephone Number: _____ Fax Number: _____ Email: _____

☐ One San Diego County (or Most Local County) Work Force – Mandatory
☐ Branch Work Force *
☐ Managing Office Work Force

Check the box above that applies to this WFR.

**Submit a separate Work Force Report for all participating branches. Combine WFRs if more than one branch per county.*

I, the undersigned representative of Armor Defense, Inc. (*Firm Name*)

Collin (*County*), Texas (*State*) hereby certify that information provided herein is true and correct. This document was executed on this 21st day of May, 20 24

_____ (*Authorized Signature*)

Karen Wood (*Print Authorized Signature Name*)

WORK FORCE REPORT – Page 2

NAME OF FIRM: Armor Defense, Inc. DATE: 5/21/2024

OFFICE(S) or BRANCH(ES): COUNTY:

INSTRUCTIONS: For each occupational category, indicate number of males and females in every ethnic group. Total columns in row provided. Sum of all totals should be equal to your total work force. Include all those employed by your company on either a full or part-time basis. The following groups are to be included in ethnic categories listed in columns below:

(1) Black or African-American
(2) Hispanic or Latino
(3) Asian
(4) American Indian or Alaska Native
(5) Native Hawaiian or Pacific Islander
(6) White
(7) Other race/ethnicity; not falling into other groups

Definitions of the race and ethnicity categories can be found on Page 4

ADMINISTRATION OCCUPATIONAL CATEGORY	(1) Black or African American		(2) Hispanic or Latino		(3) Asian		(4) American Indian/ Nat. Alaskan		(5) Pacific Islander		(6) White		(7) Other Race/ Ethnicity	
	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)
Management & Financial	1				2	4	1				9	3	2	
Professional	4	4	3		6	3					17	5		
A&E, Science, Computer														
Technical														
Sales			2								3	1		
Administrative Support												1		
Services														
Crafts														
Operative Workers														
Transportation														
Laborers*														

*Construction laborers and other field employees are not to be included on this page

Totals Each Column	5	4	5		8	7	1				29	10	2	

Grand Total All Employees	71

Indicate by Gender and Ethnicity the Number of Above Employees Who Are Disabled:

Disabled														

Non-Profit Organizations Only:

Board of Directors														
Volunteers														
Artists														

WORK FORCE REPORT – Page 3

NAME OF FIRM: Armor Defense, Inc DATE: 5/21/2024

OFFICE(S) or BRANCH(ES): _____ COUNTY: _____

INSTRUCTIONS: For each occupational category, indicate number of males and females in every ethnic group. Total columns in row provided. Sum of all totals should be equal to your total work force. Include all those employed by your company on either a full or part-time basis. The following groups are to be included in ethnic categories listed in columns below:

(1) Black or African-American
(2) Hispanic or Latino
(3) Asian
(4) American Indian or Alaska Native
(5) Native Hawaiian or Pacific Islander
(6) White
(7) Other race/ethnicity; not falling into other groups

Definitions of the race and ethnicity categories can be found on Page 4

TRADE OCCUPATIONAL CATEGORY	(1) Black or African American		(2) Hispanic or Latino		(3) Asian		(4) American Indian/ Nat. Alaskan		(5) Pacific Islander		(6) White		(7) Other Race/ Ethnicity	
	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)	(M)	(F)
Brick, Block or Stone Masons														
Carpenters														
Carpet, Floor & Tile Installers Finishers														
Cement Masons, Concrete Finishers														
Construction Laborers														
Drywall Installers, Ceiling Tile Inst														
Electricians														
Elevator Installers														
First-Line Supervisors/Managers														
Glaziers														
Helpers; Construction Trade														
Millwrights														
Misc. Const. Equipment Operators														
Painters, Const. & Maintenance														
Pipelayers, Plumbers, Pipe & Steam Fitters														
Plasterers & Stucco Masons														
Roofers														
Security Guards & Surveillance Officers														
Sheet Metal Workers														
Structural Metal Fabricators & Fitters														
Welding, Soldering & Brazing Workers														
Workers, Extractive Crafts, Miners														
Totals Each Column														

Grand Total All Employees _____

Indicate By Gender and Ethnicity the Number of Above Employees Who Are Disabled:

Disabled														

The City of SAN DIEGO

Work Force Report

HISTORY

The Work Force Report (WFR) is the document that allows the City of San Diego to analyze the work forces of all firms wishing to do business with the City. We are able to compare the firm's work force data to County Labor Force Availability (CLFA) data derived from the United States Census. CLFA data is a compilation of lists of occupations and includes the percentage of each ethnicity we track (American Indian or Alaska Native, Asian, Black or African-American, Native Hawaiian or Pacific Islander, White, and Other) for each occupation. Currently, our CLFA data is taken from the 2010 Census. In order to compare one firm to another, it is important that the data we receive from the consultant firm is accurate and organized in the manner that allows for this fair comparison.

WORK FORCE & BRANCH WORK FORCE REPORTS

When submitting a WFR, especially if the WFR is for a specific project or activity, we would like to have information about the firm's work force that is actually participating in the project or activity. That is, if the project is in San Diego and the work force is from San Diego, we want a San Diego County Work Force Report[1]. By the same token, if the project is in San Diego, but the work force is from another county, such as Orange or Riverside County, we want a Work Force Report from that county[2]. If participation in a San Diego project is by work forces from San Diego County and, for example, from Los Angeles County and from Sacramento County, we ask for separate Work Force Reports representing your firm from each of the three counties.

MANAGING OFFICE WORK FORCE

Equal Opportunity Contracting may occasionally ask for a Managing Office Work Force (MOWF) Report. This may occur in an instance where the firm involved is a large national or international firm but the San Diego or other local work force is very small. In this case, we may ask for both a local and a MOWF Report[1, 3]. In another case, when work is done only by the Managing Office, only the MOWF Report may be necessary.[3]

TYPES OF WORK FORCE REPORTS:

Please note, throughout the preceding text of this page, the superscript numbers one [1], two [2] & three [3]. These numbers coincide with the types of work force report required in the example. See below:

[1] One San Diego County (or Most Local County) Work Force – Mandatory in most cases

[2] Branch Work Force *

[3] Managing Office Work Force

**Submit a separate Work Force Report for all participating branches. Combine WFRs if more than one branch per county.*

RACE/ETHNICITY CATEGORIES

American Indian or Alaska Native – A person having origins in any of the peoples of North and South America (including Central America) and who maintains tribal affiliation or community attachment.

Asian – A person having origins in any of the peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.

Black or African American – A person having origins in any of the Black racial groups of Africa.

Native Hawaiian or Pacific Islander – A person having origins in any of the peoples of Hawaii, Guam, Samoa, or other Pacific Islands.

White – A person having origins in any of the peoples of Europe, the Middle East, or North Africa.

Hispanic or Latino – A person of Cuban, Mexican, Puerto Rican, South or Central American, or other Spanish culture or origin.

Exhibit A: Work Force Report Job Categories – Administration

Refer to this table when completing your firm's Work Force Report form(s).

Management & Financial
Advertising, Marketing, Promotions, Public Relations, and Sales Managers
Business Operations Specialists
Financial Specialists
Operations Specialties Managers
Other Management Occupations
Top Executives

Professional
Art and Design Workers
Counselors, Social Workers, and Other Community and Social Service Specialists
Entertainers and Performers, Sports and Related Workers
Health Diagnosing and Treating Practitioners
Lawyers, Judges, and Related Workers
Librarians, Curators, and Archivists
Life Scientists
Media and Communication Workers
Other Teachers and Instructors
Postsecondary Teachers
Primary, Secondary, and Special Education School Teachers
Religious Workers
Social Scientists and Related Workers

Architecture & Engineering, Science, Computer
Architects, Surveyors, and Cartographers
Computer Specialists
Engineers
Mathematical Science Occupations
Physical Scientists

Technical
Drafters, Engineering, and Mapping Technicians
Health Technologists and Technicians
Life, Physical, and Social Science Technicians
Media and Communication Equipment Workers

Sales
Other Sales and Related Workers
Retail Sales Workers
Sales Representatives, Services
Sales Representatives, Wholesale and Manufacturing
Supervisors, Sales Workers

Administrative Support
Financial Clerks
Information and Record Clerks
Legal Support Workers
Material Recording, Scheduling, Dispatching, and Distributing Workers
Other Education, Training, and Library Occupations
Other Office and Administrative Support Workers
Secretaries and Administrative Assistants
Supervisors, Office and Administrative Support Workers

Services
Building Cleaning and Pest Control Workers
Cooks and Food Preparation Workers
Entertainment Attendants and Related Workers
Fire Fighting and Prevention Workers
First-Line Supervisors/Managers, Protective Service Workers
Food and Beverage Serving Workers
Funeral Service Workers
Law Enforcement Workers
Nursing, Psychiatric, and Home Health Aides
Occupational and Physical Therapist Assistants and Aides
Other Food Preparation and Serving Related Workers
Other Healthcare Support Occupations
Other Personal Care and Service Workers
Other Protective Service Workers
Personal Appearance Workers
Supervisors, Food Preparation and Serving Workers
Supervisors, Personal Care and Service Workers
Transportation, Tourism, and Lodging Attendants

Crafts
Construction Trades Workers
Electrical and Electronic Equipment Mechanics, Installers, and Repairers
Extraction Workers
Material Moving Workers
Other Construction and Related Workers
Other Installation, Maintenance, and Repair Occupations
Plant and System Operators
Supervisors of Installation, Maintenance, and Repair Workers
Supervisors, Construction and Extraction Workers
Vehicle and Mobile Equipment Mechanics,

Installers, and Repairers
Woodworkers

Operative Workers
Assemblers and Fabricators
Communications Equipment Operators
Food Processing Workers
Metal Workers and Plastic Workers
Motor Vehicle Operators
Other Production Occupations
Printing Workers
Supervisors, Production Workers
Textile, Apparel, and Furnishings Workers

Transportation
Air Transportation Workers
Other Transportation Workers
Rail Transportation Workers
Supervisors, Transportation and Material Moving Workers
Water Transportation Workers

Laborers
Agricultural Workers
Animal Care and Service Workers
Fishing and Hunting Workers
Forest, Conservation, and Logging Workers
Grounds Maintenance Workers
Helpers, Construction Trades
Supervisors, Building and Grounds Cleaning and Maintenance Workers
Supervisors, Farming, Fishing, and Forestry Workers

Exhibit B: Work Force Report Job Categories-Trade

Brick, Block or Stone Masons
Brickmasons and Blockmasons
Stonemasons

Carpenters

Carpet, floor and Tile Installers and Finishers
Carpet Installers
Floor Layers, except Carpet, Wood and Hard Tiles
Floor Sanders and Finishers
Tile and Marble Setters

Cement Masons, Concrete Finishers
Cement Masons and Concrete Finishers
Terrazzo Workers and Finishers

Construction Laborers

Drywall Installers, Ceiling Tile Inst
Drywall and Ceiling Tile Installers
Tapers

Electricians

Elevator Installers and Repairers

First-Line Supervisors/Managers
First-line Supervisors/Managers of Construction Trades and Extraction Workers

Glaziers

Helpers, Construction Trade
Brickmasons, Blockmasons, and Tile and Marble Setters
Carpenters
Electricians
Painters, Paperhangers, Plasterers and Stucco
Pipelayers, Plumbers, Pipefitters and Steamfitters
Roofers
All other Construction Trades

Millwrights
Heating, Air Conditioning and Refrigeration Mechanics and Installers
Mechanical Door Repairers

Control and Valve Installers and Repairers

Other Installation, Maintenance and Repair Occupations

Misc. Const. Equipment Operators
Paving, Surfacing and Tamping Equipment Operators
Pile-Driver Operators
Operating Engineers and Other Construction Equipment Operators

Painters, Const. Maintenance
Painters, Construction and Maintenance
Paperhangers

Pipelayers and Plumbers
Pipelayers
Plumbers, Pipefitters and Steamfitters

Plasterers and Stucco Masons

Roofers

Security Guards & Surveillance Officers

Sheet Metal Workers

Structural Iron and Steel Workers

Welding, Soldering and Brazing Workers
Welders, Cutter, Solderers and Brazers
Welding, Soldering and Brazing Machine Setter, Operators and Tenders

Workers, Extractive Crafts, Miners