PROFESSIONAL CONSULTANT SERVICES AGREEMENT

SECURICON, LLC

Vulnerability Assessment Report for Riverside Public Utilities

THIS PROFESSIONAL CONSULTANT SERVICES AGREEMENT ("Agreement") is made and entered into this _____ day of _____, 20_____ ("Effective Date"), by and between the CITY OF RIVERSIDE ("City"), a California charter city and municipal corporation and SECURICON, LLC, a Virginia limited liability company authorized to do business in California ("Consultant").

1. **Scope of Services**. City agrees to retain and does hereby retain Consultant and Consultant agrees to provide the services more particularly described in Exhibit "A," "Scope of Services" ("Services"), attached hereto and incorporated herein by reference, in conjunction with the Vulnerability Assessment Report for Riverside Public Utilities ("Project").

2. **Term**. This Agreement shall be effective on the date first written above and shall remain in effect until September 30, 2016, unless otherwise terminated pursuant to the provisions herein.

3. **Compensation/Payment**. Consultant shall perform the Services under this Agreement for the total sum not to exceed Three Hundred Forty-Two Thousand Dollars ($342,000) payable in accordance with the terms set forth in Exhibit "B." Said payment shall be made in accordance with City's usual accounting procedures upon receipt and approval of an itemized invoice setting forth the services performed. The invoices shall be delivered to City at the address set forth in Section 4 hereof.

4. **Notices**. Any notices required to be given, hereunder shall be in writing and shall be personally served or given by mail. Any notice given by mail shall be deemed given when deposited in the United States Mail, certified and postage prepaid, addressed to the party to be served as follows:

To City	To Consultant
Riverside Public Utilities	Securicon, LLC
City of Riverside	Attn: Paul Hurley
Attn: Jennifer Tavaglione	5400 Shawnee Road, Suite 206
3750 University Avenue	Alexandria, VA 22312
Riverside, CA 92501	

5. **Prevailing Wage**. If applicable, Consultant and all subcontractors are required to pay the general prevailing wage rates of per diem wages and overtime and holiday wages determined by the Director of the Department of Industrial Relations under Section 1720 et seq. of the California Labor Code and implemented by Resolution No. 13346 of the City Council of the City of Riverside. The Director's determination is available on-line at: www.dir.ca.gov/dlsr/DPreWageDetermination.htm and is referred to and made a part hereof; the

wage rates therein ascertained, determined, and specified are referred to and made a part hereof as though fully set forth herein.

6. **Contract Administration**. A designee of the City will be appointed in writing by the City Manager or Department Director to administer this Agreement on behalf of City and shall be referred to herein as Contract Administrator.

7. **Standard of Performance**. While performing the Services, Consultant shall exercise the reasonable professional care and skill customarily exercised by reputable members of Consultant's profession practicing in the Metropolitan Southern California Area, and shall use reasonable diligence and best judgment while exercising its professional skill and expertise.

8. **Personnel**. Consultant shall furnish all personnel necessary to perform the Services and shall be responsible for their performance and compensation. Consultant recognizes that the qualifications and experience of the personnel to be used are vital to professional and timely completion of the Services. The key personnel listed in Exhibit "C" attached hereto and incorporated herein by this reference and assigned to perform portions of the Services shall remain assigned through completion of the Services, unless otherwise mutually agreed by the parties in writing, or caused by hardship or resignation in which case substitutes shall be subject to City approval.

9. **Assignment and Subcontracting**. Neither party shall assign any right, interest, or obligation in or under this Agreement to any other entity without prior written consent of the other party. In any event, no assignment shall be made unless the assignee expressly assumes the obligations of assignor under this Agreement, in a writing satisfactory to the parties. Consultant acknowledges that any assignment may, at the City's sole discretion, require City Manager and/or City Council approval. Consultant shall not subcontract any portion of the work required by this Agreement without prior written approval by the responsible City Contract Administrator. Subcontracts, if any, shall contain a provision making them subject to all provisions stipulated in this Agreement, including without limitation, the insurance obligations set forth in Section 12. The Consultant acknowledges and agrees that the City is an intended beneficiary of any work performed by any subcontractor for purposes of establishing a duty of care between any subcontractor and the City.

10. **Independent Contractor**. In the performance of this Agreement, Consultant, and Consultant's employees, subcontractors and agents, shall act in an independent capacity as independent contractors, and not as officers or employees of the City of Riverside. Consultant acknowledges and agrees that the City has no obligation to pay or withhold state or federal taxes or to provide workers' compensation or unemployment insurance to Consultant, or to Consultant's employees, subcontractors and agents. Consultant, as an independent contractor, shall be responsible for any and all taxes that apply to Consultant as an employer.

11. **Indemnification**.

11.1 **Design Professional Defined**. For purposes of this Agreement, "Design Professional" includes the following:

A. An individual licensed as an architect pursuant to Chapter 3 (commencing with Section 5500) of Division 3 of the Business and Professions Code, and a business entity offering architectural services in accordance with that chapter.

B. An individual licensed as a landscape architect pursuant to Chapter 3.5 (commencing with Section 5615) of Division 3 of the Business and Professions Code, and a business entity offering landscape architectural services in accordance with that chapter.

C. An individual registered as a professional engineer pursuant to Chapter 7 (commencing with Section 6700) of Division 3 of the Business and Professions Code, and a business entity offering professional engineering services in accordance with that chapter.

D. An individual licensed as a professional land surveyor pursuant to Chapter 15 (commencing with Section 8700) of Division 3 of the Business and Professions Code, and a business entity offering professional land surveying services in accordance with that chapter.

11.2 **Defense Obligation for Design Professional Liability**. Consultant agrees, at its cost and expense, to promptly defend the City, and the City's employees, officers, managers, agents and council members (collectively the "Parties to be Defended") from and against any and all claims, allegations, lawsuits, arbitration proceedings, administrative proceedings, regulatory proceedings, or other legal proceedings to the extent the same arise out of, pertain to, or relate to the negligence, recklessness or willful misconduct of Consultant, or anyone employed by or working under the Consultant or for services rendered to the Consultant in the performance of the Agreement, notwithstanding that the City may have benefited from its work or services and whether or not caused in part by the negligence of an Indemnified Party. Consultant agrees to provide this defense immediately upon written notice from the City, and with well qualified, adequately insured and experienced legal counsel acceptable to City. This obligation to defend as set forth herein is binding on the successors, assigns and heirs of Consultant and shall survive the termination of Consultant's Services under this Agreement.

11.3 **Indemnity for Design Professional Liability**. When the law establishes a professional standard of care for Consultant's services, to the fullest extent permitted by law, Consultant shall indemnify, protect and hold harmless the City and the City's employees, officers, managers, agents, and Council Members ("Indemnified Parties") from and against any and all claim for damage, charge, lawsuit, action, judicial, administrative, regulatory or arbitration proceeding, damage, cost, expense (including counsel and expert fees), judgment, civil fines and penalties, liabilities or losses of any kind or nature whatsoever to the extent the same arise out of, pertain to, or relate to the negligence, recklessness or willful misconduct of Consultant, or anyone employed by or working under the Consultant or for services rendered to the Consultant in the performance of the Agreement, notwithstanding that the City may have benefited from its work or services and whether or not caused in part by the negligence of an Indemnified Party.

11.4 **Defense Obligation for Other than Design Professional Liability**. Consultant agrees, at its cost and expense, to promptly defend the City, and the City's employees, officers, managers, agents and council members (collectively the "Parties to be Defended") from and against any and all claims, allegations, lawsuits, arbitration proceedings, administrative proceedings, regulatory proceedings, or other legal proceedings which arise out of, or relate to, or are in any way connected with: 1) the Services, work, activities, operations, or duties of the Consultant, or of anyone employed by or working under the Consultant, or 2) any breach of the Agreement by the Consultant. This duty to defend shall apply whether or not such claims, allegations, lawsuits or proceedings have merit or are meritless, or which involve claims or allegations that any or all of the Parties to be Defended were actively, passively, or concurrently negligent, or which otherwise assert that the Parties to be Defended are responsible, in whole or in part, for any loss, damage or injury. Consultant agrees to provide this defense immediately upon written notice from the City, and with well qualified, adequately insured and experienced legal counsel acceptable to City. This obligation to defend as set forth herein is binding on the successors, assigns and heirs of Consultant and shall survive the termination of Consultant's Services under this Agreement.

11.5 **Indemnity for Other than Design Professional Liability**. Except as to the sole negligence or willful misconduct of the City, Consultant agrees to indemnify, protect and hold harmless the Indemnified Parties from and against any claim for damage, charge, lawsuit, action, judicial, administrative, regulatory or arbitration proceeding, damage, cost, expense (including counsel and expert fees), judgment, civil fine and penalties, liabilities or losses of any kind or nature whatsoever whether actual, threatened or alleged, which arise out of, pertain to, or relate to, or are a consequence of, or are attributable to, or are in any manner connected with the performance of the Services, work, activities, operations or duties of the Consultant, or anyone employed by or working under the Consultant or for services rendered to Consultant in the performance of this Agreement, notwithstanding that the City may have benefited from its work or services. This indemnification provision shall apply to any acts, omissions, negligence, recklessness, or willful misconduct, whether active or passive, on the part of the Consultant or anyone employed or working under the Consultant.

12. **Insurance**.

12.1 **General Provisions**. Prior to the City's execution of this Agreement, Consultant shall provide satisfactory evidence of, and shall thereafter maintain during the term of this Agreement, such insurance policies and coverages in the types, limits, forms and ratings required herein. The rating and required insurance policies and coverages may be modified in writing by the City's Risk Manager or City Attorney, or a designee, unless such modification is prohibited by law.

12.1.1 **Limitations**. These minimum amounts of coverage shall not constitute any limitation or cap on Consultant's indemnification obligations under Section 11 hereof.

12.1.2 **Ratings**. Any insurance policy or coverage provided by Consultant or subcontractors as required by this Agreement shall be deemed inadequate and a material breach of this Agreement, unless such policy or coverage is issued by insurance companies authorized to transact insurance business in the State of California with a policy holder's rating of A or higher and a Financial Class of VII or higher.

12.1.3 **Cancellation**. The policies shall not be canceled unless thirty (30) days prior written notification of intended cancellation has been given to City by certified or registered mail, postage prepaid.

12.1.4 **Adequacy**. The City, its officers, employees and agents make no representation that the types or limits of insurance specified to be carried by Consultant pursuant to this Agreement are adequate to protect Consultant. If Consultant believes that any required insurance coverage is inadequate, Consultant will obtain such additional insurance coverage as Consultant deems adequate, at Consultant's sole expense.

12.2 **Workers' Compensation Insurance**. By executing this Agreement, Consultant certifies that Consultant is aware of and will comply with Section 3700 of the Labor Code of the State of California requiring every employer to be insured against liability for workers' compensation, or to undertake self-insurance before commencing any of the work. Consultant shall carry the insurance or provide for self-insurance required by California law to protect said Consultant from claims under the Workers' Compensation Act. Prior to City's execution of this Agreement, Consultant shall file with City either 1) a certificate of insurance showing that such insurance is in effect, or that Consultant is self-insured for such coverage, or 2) a certified statement that Consultant has no employees, and acknowledging that if Consultant does employ any person, the necessary certificate of insurance will immediately be filed with City. Any certificate filed with City shall provide that City will be given ten (10) days prior written notice before modification or cancellation thereof.

12.3 **Commercial General Liability and Automobile Insurance**. Prior to City's execution of this Agreement, Consultant shall obtain, and shall thereafter maintain during the term of this Agreement, commercial general liability insurance and automobile liability insurance as required to insure Consultant against damages for personal injury, including accidental death, as well as from claims for property damage, which may arise from or which may concern operations by anyone directly or indirectly employed by, connected with, or acting for or on behalf of Consultant. The City, and its officers, employees and agents, shall be named as additional insureds under the Consultant's insurance policies.

12.3.1 Consultant's commercial general liability insurance policy shall cover both bodily injury (including death) and property damage (including, but not limited to, premises operations liability, products-completed operations liability, independent contractor's liability, personal injury liability, and contractual liability) in an amount not less than $1,000,000 per occurrence and a general aggregate limit in the amount of not less than $2,000,000.

12.3.2 Consultant's automobile liability policy shall cover both bodily injury and property damage in an amount not less than $1,000,000 per occurrence and an aggregate limit of not less than $1,000,000. All of Consultant's automobile and/or commercial general liability insurance policies shall cover all vehicles used in connection with Consultant's performance of this Agreement, which vehicles shall include, but are not limited to, Consultant owned vehicles,

Consultant leased vehicles, Consultant's employee vehicles, non-Consultant owned vehicles and hired vehicles.

12.3.3 Prior to City's execution of this Agreement, copies of insurance policies or original certificates along with additional insured endorsements acceptable to the City evidencing the coverage required by this Agreement, for both commercial general and automobile liability insurance, shall be filed with City and shall include the City and its officers, employees and agents, as additional insureds. Said policies shall be in the usual form of commercial general and automobile liability insurance policies, but shall include the following provisions:

> It is agreed that the City of Riverside, and its officers, employees and agents, are added as additional insureds under this policy, solely for work done by and on behalf of the named insured for the City of Riverside.

12.3.4 The insurance policy or policies shall also comply with the following provisions:

a. The policy shall be endorsed to waive any right of subrogation against the City and its sub-consultants, employees, officers and agents for services performed under this Agreement.

b. If the policy is written on a claims-made basis, the certificate should so specify and the policy must continue in force for one year after completion of the services. The retroactive date of coverage must also be listed.

c. The policy shall specify that the insurance provided by Consultant will be considered primary and not contributory to any other insurance available to the City and Endorsement No. CG 20010413 shall be provided to the City.

12.4 **Errors and Omissions Insurance.** Prior to City's execution of this Agreement, Consultant shall obtain, and shall thereafter maintain during the term of this Agreement, errors and omissions professional liability insurance in the minimum amount of $1,000,000 to protect the City from claims resulting from the Consultant's activities.

12.5 **Subcontractors' Insurance.** Consultant shall require all of its subcontractors to carry insurance, in an amount sufficient to cover the risk of injury, damage or loss that may be caused by the subcontractors' scope of work and activities provided in furtherance of this Agreement, including, but without limitation, the following coverages: Workers Compensation, Commercial General Liability, Errors and Omissions, and Automobile liability. Upon City's request, Consultant shall provide City with satisfactory evidence that Subcontractors have obtained insurance policies and coverages required by this section.

13. **Business Tax**. Consultant understands that the Services performed under this Agreement constitutes doing business in the City of Riverside, and Consultant agrees that Consultant will register for and pay a business tax pursuant to Chapter 5.04 of the Riverside Municipal Code and keep such tax certificate current during the term of this Agreement.

14. **Time of Essence**. Time is of the essence for each and every provision of this Agreement.

15. **City's Right to Employ Other Consultants**. City reserves the right to employ other Consultants in connection with the Project. If the City is required to employ another consultant to complete Consultant's work, due to the failure of the Consultant to perform, or due to the breach of any of the provisions of this Agreement, the City reserves the right to seek reimbursement from Consultant.

16. **Accounting Records**. Consultant shall maintain complete and accurate records with respect to costs incurred under this Agreement. All such records shall be clearly identifiable. Consultant shall allow a representative of City during normal business hours to examine, audit, and make transcripts or copies of such records and any other documents created pursuant to this Agreement. Consultant shall allow inspection of all work, data, documents, proceedings, and activities related to the Agreement for a period of three (3) years from the date of final payment under this Agreement.

17. **Confidentiality**. All ideas, memoranda, specifications, plans, procedures, drawings, descriptions, computer program data, input record data, written information, and other materials either created by or provided to Consultant in connection with the performance of this Agreement shall be held confidential by Consultant, except as otherwise directed by City's Contract Administrator. Nothing furnished to Consultant which is otherwise known to the Consultant or is generally known, or has become known, to the related industry shall be deemed confidential. Consultant shall not use City's name or insignia, photographs of the Project, or any publicity pertaining to the Services or the Project in any magazine, trade paper, newspaper, television or radio production, website, or other similar medium without the prior written consent of the City.

18. **Ownership of Documents**. All reports, maps, drawings and other contract deliverables prepared under this Agreement by Consultant shall be and remain the property of City. Consultant shall not release to others information furnished by City without prior express written approval of City.

19. **Copyrights.** Consultant agrees that any work prepared for City which is eligible for copyright protection in the United States or elsewhere shall be a work made for hire. If any such work is deemed for any reason not to be a work made for hire, Consultant assigns all right, title and interest in the copyright in such work, and all extensions and renewals thereof, to City, and agrees to provide all assistance reasonably requested by City in the establishment, preservation and enforcement of its copyright in such work, such assistance to be provided at City's expense but without any additional compensation to Consultant. Consultant agrees to waive all moral rights relating to the work developed or produced, including without limitation any and all rights of

identification of authorship and any and all rights of approval, restriction or limitation on use or subsequent modifications.

20. **Conflict of Interest**. Consultant, for itself and on behalf of the individuals listed in Exhibit "C," represents and warrants that by the execution of this Agreement, they have no interest, present or contemplated, in the Project affected by the above-described Services. Consultant further warrants that neither Consultant, nor the individuals listed in Exhibit "C" have any real property, business interests or income interests that will be affected by this project or, alternatively, that Consultant will file with the City an affidavit disclosing any such interest.

21. **Solicitation**. Consultant warrants that Consultant has not employed or retained any person or agency to solicit or secure this Agreement, nor has it entered into any agreement or understanding for a commission, percentage, brokerage, or contingent fee to be paid to secure this Agreement. For breach of this warranty, City shall have the right to terminate this Agreement without liability and pay Consultant only for the value of work Consultant has actually performed, or, in its sole discretion, to deduct from the Agreement price or otherwise recover from Consultant the full amount of such commission, percentage, brokerage or commission fee. The remedies specified in this section shall be in addition to and not in lieu of those remedies otherwise specified in this Agreement.

22. **General Compliance with Laws**. Consultant shall keep fully informed of federal, state and local laws and ordinances and regulations which in any manner affect those employed by Consultant, or in any way affect the performance of services by Consultant pursuant to this Agreement. Consultant shall at all times observe and comply with all such laws, ordinances and regulations, and shall be solely responsible for any failure to comply with all applicable laws, ordinances and regulations. Consultant represents and warrants that Consultant has obtained all necessary licenses to perform the Scope of Services and that such licenses are in good standing. Consultant further represents and warrants that the services provided herein shall conform to all ordinances, policies and practices of the City of Riverside.

23. **Waiver**. No action or failure to act by the City shall constitute a waiver of any right or duty afforded City under this Agreement, nor shall any such action or failure to act constitute approval of or acquiescence in any breach thereunder, except as may be specifically, provided in this Agreement or as may be otherwise agreed in writing.

24. **Amendments**. This Agreement may be modified or amended only by a written agreement and/or change order executed by the Consultant and City.

25. **Termination**. City, by notifying Consultant in writing, shall have the right to terminate any or all of Consultant's services and work covered by this Agreement at any time. In the event of such termination, Consultant may submit Consultant's final written statement of the amount of Consultant's services as of the date of such termination based upon the ratio that the work completed bears to the total work required to make the report complete, subject to the City's rights under Sections 15 and 25 hereof. In ascertaining the work actually rendered through the termination

date, City shall consider completed work, work in progress and complete and incomplete reports and other documents only after delivered to City.

25.1 Other than as stated below, City shall give Consultant thirty (30) days prior written notice prior to termination.

25.2 City may terminate this Agreement upon fifteen (15) days written notice to Consultant, in the event:

25.2.1 Consultant substantially fails to perform or materially breaches the Agreement; or

25.2.2 City decides to abandon or postpone the Project.

26. **Offsets**. Consultant acknowledges and agrees that with respect to any business tax or penalties thereon, utility charges, invoiced fee or other debt which Consultant owes or may owe to the City, City reserves the right to withhold and offset said amounts from payments or refunds or reimbursements owed by City to Consultant. Notice of such withholding and offset, shall promptly be given to Consultant by City in writing. In the event of a dispute as to the amount owed or whether such amount is owed to the City, City will hold such disputed amount until either the appropriate appeal process has been completed or until the dispute has been resolved.

27. **Successors and Assigns**. This Agreement shall be binding upon City and its successors and assigns, and upon Consultant and its permitted successors and assigns, and shall not be assigned by Consultant, either in whole or in part, except as otherwise provided in paragraph 9 of this Agreement.

28. **Venue and Attorneys' Fees**. Any action at law or in equity brought by either of the parties hereto for the purpose of enforcing a right or rights provided for by this Agreement shall be tried in a court of competent jurisdiction in the County of Riverside, State of California, and the parties hereby waive all provisions of law providing for a change of venue in such proceedings to any other county. In the event either party hereto shall bring suit to enforce any term of this Agreement or to recover any damages for and on account of the breach of any term or condition of this Agreement, it is mutually agreed that the prevailing party in such action shall recover all costs thereof, including reasonable attorneys' fees. However, the recovery of attorneys' fees by the prevailing party is limited to individual actions or proceedings in which the City elects, at the initiation of that individual action or proceeding, to seek recovery of its own attorneys' fee. In no action shall an award of attorneys' fees to the prevailing party exceed the amount of reasonable attorneys' fees incurred by the City in the action or proceeding.

29. **Nondiscrimination**. During Consultant's performance of this Agreement, Consultant shall not discriminate on the grounds of race, religious creed, color, national origin, ancestry, age, physical disability, mental disability, medical condition, including the medical condition of Acquired Immune Deficiency Syndrome (AIDS) or any condition related thereto, marital status, sex, genetic information, gender, gender identity, gender expression, or sexual orientation, in the selection and retention of employees and subcontractors and the procurement of materials and equipment, except

as provided in Section 12940 of the California Government Code. Further, Consultant agrees to conform to the requirements of the Americans with Disabilities Act in the performance of this Agreement.

30. **Severability**. Each provision, term, condition, covenant and/or restriction, in whole and in part, of this Agreement shall be considered severable. In the event any provision, term, condition, covenant and/or restriction, in whole and/or in part, of this Agreement is declared invalid, unconstitutional, or void for any reason, such provision or part thereof shall be severed from this Agreement and shall not affect any other provision, term, condition, covenant and/or restriction of this Agreement, and the remainder of the Agreement shall continue in full force and effect.

31. **Authority**. The individuals executing this Agreement and the instruments referenced herein on behalf of Consultant each represent and warrant that they have the legal power, right and actual authority to bind Consultant to the terms and conditions hereof and thereof.

32. **Entire Agreement**. This Agreement constitutes the final, complete, and exclusive statement of the terms of the agreement between the parties pertaining to the subject matter of this Agreement, and supersedes all prior and contemporaneous understandings or agreements of the parties. Neither party has been induced to enter into this Agreement by and neither party is relying on, any representation or warranty outside those expressly set forth in this Agreement.

33. **Interpretation**. City and Consultant acknowledge and agree that this Agreement is the product of mutual arms-length negotiations and accordingly, the rule of construction, which provides that the ambiguities in a document shall be construed against the drafter of that document, shall have no application to the interpretation and enforcement of this Agreement.

33.1 Titles and captions are for convenience of reference only and do not define, describe or limit the scope or the intent of the Agreement or any of its terms. Reference to section numbers, are to sections in the Agreement unless expressly stated otherwise.

33.2 This Agreement shall be governed by and construed in accordance with the laws of the State of California in effect at the time of the execution of this Agreement.

33.3 In the event of a conflict between the body of this Agreement and Exhibit "A" attached hereto, the terms contained in Exhibit "A" shall be controlling.

34. **Exhibits**. The following exhibits attached hereto are incorporated herein to this Agreement by this reference:

Exhibit "A" - Scope of Services
Exhibit "B" - Compensation
Exhibit "C" - Key Personnel

(Signatures on Next Page)

IN WITNESS WHEREOF, City and Consultant have caused this Agreement to be duly executed the day and year first above written.

CITY OF RIVERSIDE, a California charter city and municipal corporation

By: _____
City Manager

Attest: _____
City Clerk

Approved as to Form:

By: _____
Assistant City Attorney

CERTIFIED AS TO FUNDS AVAILABILITY:

By: _____
Finance Director

CA #15-2280 SW 12/15/15
O:\Cycom\Wpdocs\D015\P023\00265752.Doc

SECURICON, LLC, a Virginia limited liability Company authorized to do business in California

By: _____

Paul W. Hurley
Printed Name

CEO
Title

By: _____

_____
Printed Name

_____
Title

EXHIBIT "A"

SCOPE OF SERVICES

PROPOSAL TO DEVELOP PHYSICAL SECURITY AND CYBER SECURITY GUIDELINES AND CONDUCT A VULNERABILITY ASSESSMENT

Prepared for

City of Riverside, California
Habib R. Hariri, P.E.
2911 Adams Street
Riverside, CA 92504
951-826-5304

Submitted by

Securicon, LLC
5400 Shawnee Road, Suite 206
Alexandria, Virginia 22312
703-914-2780
www.securicon.com

*** PROPRIETARY & CONFIDENTIAL INFORMATION IS CONTAINED WITHIN ***

October 26, 2015

STATEMENT OF CONFIDENTIALITY

This Confidential Memorandum is being delivered to a select number of parties who are believed to have interest in entering into a transaction with Securicon, LLC (identified throughout this document as "Securicon"). The sole purpose of this Memorandum is to assist the recipient in deciding whether to proceed into a contractual agreement with Securicon. Each recipient agrees that, prior to reading this Memorandum, it shall not distribute or use the information marked as propriety herein for any purpose other than those stated.

The pages marked as proprietary shall remain the sole property of Securicon and may not be copied, reproduced, or distributed without the prior written consent of Securicon. In general, these are the pages that describe specific methodologies, name our staff and the logic employed to arrive at the schedule and thereby, the costs.

In furnishing this Memorandum, Securicon undertakes no obligations. This Memorandum states general intent and agreement to perform services contingent upon a formal written agreement between both parties.

POINTS OF CONTACT

Contractual:
Paul W. Hurley
CEO & General Manager
Phone: 703-914-2780 ext. 101
Fax: 703-914-2785
Email: Paul.Hurley@Securicon.com

Technical/Service Delivery:
Harry Regan
VP, Security Services
Phone: 703-914-2780 ext. 104
Fax: 703-914-2785
Email: Harry.Regan@securicon.com

INTRODUCTION

Securicon, LLC (Securicon) is pleased to present this proposal to The City of Riverside (City) to develop Physical Security and Cyber Security Guidelines and to conduct a Vulnerability Assessment. This engagement will provide a standardized and accepted guidelines for the City's physical and cyber security environments and provides a gap analysis of deviations of the current implementation against the guidelines. Securicon will identify and document vulnerabilities that could lead to reduced integrity, confidentiality, or availability of your critical data. In addition, where reviews of security practices and where trends in technical vulnerability data can be analyzed and root causes identified, Securicon will also offer recommendations to address the root causes of any identified vulnerabilities to prevent them from reoccurring in the future.

Cyber threats are increasing at an unprecedented rate. Furthermore, the increased complexity of stealth, malicious network and web application attacks challenges the abilities of many information security professionals and the intrusion detection and related devices they often rely upon to stay one step ahead of the latest malware or virus incarnations. For these reasons many companies seek not only to meet the network security compliance requirements they are mandated to uphold by regulators, but to strive for a higher level of information security in an effort to thwart both malicious and accidental data breaches.

Securicon recognizes the mission-critical nature of network and data security and has focused its consulting practice in that discipline for over 13 years. There are no 'staff in development' roles at Securicon – a key differentiator between our firm and others who attempt to provide similar services. All of our consultants have a decade or more experience as IT security professionals. Most are battle-tested practitioners turned consultants who come from a variety of industry backgrounds. This rich tapestry of seasoned professional resources brings a unique value to every engagement. No cookie cutter solutions, no 'check-list' mentality. Instead, each of our clients' needs, circumstances, and configurations are thoughtfully examined in the context of real-world and next generation cyber threats. Every IT network security environment and architecture is different. Without highly skilled IT security engineers of the caliber we employ at Securicon to guide a comprehensive vulnerability assessment, subtle nuances that could lead to security exploitations are routinely overlooked by lesser firms.

Securicon's long history in industrial control, SCADA and Process Control and enterprise security in regulated industries makes us uniquely qualified to address the requirements set forth in Riverside's RFP. Securicon has certified professionals in both physical and cyber security and has developed security programs encompassing both operational and programmatic solutions for industrial, commercial, municipal, state and Federal clients.

The proposal outlined in the pages that follow relies heavily on proven and, in some cases, unique and proprietary tools, techniques and methodologies used by Securicon's IT security consultants. Our vigorous testing approach to all of the elements outlined in your request for proposal (RFP) are the same strategies and tactics we successfully use to conduct assessments at some of the most recognizable organizations in the financial, stock trading platform, utility, oil/gas, grid management industries, and critical Federal government agencies.

We encourage you to carefully review the resumes of our professional IT security engineers. We are confident that your selection of a long-term, trusted advisor will be guided by what you learn about our capabilities at Securicon and your steadfast commitment to protect the sensitive and personal data your customers entrust you with.

TABLE OF CONTENTS

A. SCOPE OF WORK

Securicon understands that City's overall objective is to ensure that the security mechanisms implemented are appropriate to preserve integrity, confidentiality, and availability. An effective security controls and risk management framework will aid in the prevention of unauthorized, accidental, or deliberate disruption, disclosure, modification, and use of the City's networks, systems and applications. Securicon will work with the City to ensure that the objectives are accurate and achieve the overall security requirements. This assessment will be conducted in the following phases:

- **Task 1: Project Management Services:** This task will include all planning and assessment preparation activities as well as project management tasks through the duration of the assessment. A designated Securicon Project Manager will be responsible for all coordination details between Securicon and the City, to include but not limited to: The Kick-off meeting, development of the Written Rules of Engagement, scheduling site visits, and providing project status updates through completion of the project.

- **Task 2: Vulnerability Assessment:** This task will include the review and development of the City's physical and cyber security guidelines and policies using best management practices followed by an assessment Following the development and City's approvals of the Physical and Security Policies, Securicon will conduct a Physical and Cyber Security Assessment of the City's physical locations and cyber assets

- **Task 3: Additional Engineering Services:** This task will include a controlled allowance for additional services to be performed if desired by the City. This portion of the assessment will not exceed 10% of the total project. As requested in Addendum 01 of the RFP, Securicon has included a SCADA Penetration Test as an optional service.

B. METHODOLOGY

This section presents Securicon's proposed approach to meet the requirement outlined in the RFP. We have structured this section to follow the same order and numbering used in the Part II Scope of Work section of the RFP to allow an efficient review.

TASK 1 - PROJECT MANAGEMENT SERVICES

A. KICK OFF MEETING

The designated Securicon Project Manager will coordinate a task kickoff meeting in which any necessary scheduling details will be finalized. Securicon's Project Manager will exchange contact information so that the task team can be in communication at any day or hour, if needed. All coordination details will be reviewed and finalized at this time; such as the frequency and detail level desired for status updates. In addition, Securicon's Project Manager will work with the City's representative to establish secure channels of communication to exchange status updates (if written updates are necessary) and to exchange the eventual draft and final reports. These may include email encryption, SFTP servers or other means, based on the practicality of each method within the client's environment.

Following the kickoff meeting, Securicon's Project Manager will provide a Written Rules of Engagement which provides the City Project Manager a list of activities and a description of each activity associated with each phase to enable the City Project Manager to provide approval prior to the start of the task. The document shall also include the test boundaries ("Rules of Engagement") agreed upon by the City and Securicon's Project Managers. The Rules of Engagement will include:

- Assumptions and limitations made by the Client and Securicon;
- Risks (identified unstable or highly critical systems) and planned mitigation actions
- Identification of all Contractor personnel assigned to the active tasks;
- Coordinated schedules for interviews, testing and other project activities;
- Locations and source IP address ranges from which testing will be authorized;
- Equipment or software anticipated to be used during testing;
- Frequency and methods of communication; and
- Incident handling and response procedures and contact information.

B. PROJECT STATUS MEETINGS

After task initiation, the Project Manager will coordinate and conduct a monthly project status meeting, at a minimum. However, if any serious vulnerabilities are identified that could provide immediate access to internal or highly critical systems by easily executed exploit techniques, Securicon will not wait for a regularly scheduled status update. If such weaknesses are identified, Securicon will provide recommendations for near-term mitigation actions that should be taken immediately, pending potentially more in-depth or longer term recommendations that will be provided in the report. A summary briefing will be presented at the conclusion of each milestone, prior to the analysis and reporting phase. The goal of the communication efforts is to ensure there will be no surprises at the end of the task, and that City IT professionals will be included in discussions that help ensure a more effective implementation of mitigation efforts after the report is submitted.

C. MONTLY STATUS EMAIL REPORT

Securicon will develop and maintain an email report to provide the City with status updates on project issues, coordination efforts, action items, schedule, budget, and any other items required to keep the City informed of each project milestone.

D. DETAILED BILLING

Securicon will invoice at the beginning of each month for all work and travel completed during the previous month. Each monthly invoice will include a detailed breakdown of all individuals and will clearly show the number of hours, the billing rate, and the travel expenses for each consultant on the task.

E. DETAILED BUDGET SUMMARY

Securicon's invoices also include a detailed Invoicing History report that presents an overview of the contracted amount, all monthly invoices to-date along with the remaining labor and travel funds available on the contract.

TASK 2 - VULNERABILITY ASSESSMENT

A. DEVELOP PHYSICAL SECURITY GUIDELINES

Following the kickoff meeting and development of rules of engagement, Securicon's task team will meet with the City executive management team to develop they outline and discuss the details of the of the physical security policy that best supports the City's business processes. Securicon will leverage its experience in developing similar Information Security policies for organizations such as the government agencies, Internet Service Providers and Financial Institutions. Our recommended approach is to build policies as a modular set of documents, to allow for easier modification as the City changes and grows in the years to come.

Milestone 1 – Detailed Outline: Securicon will work the City Management to develop a detailed outline of the Information Security Policy. The outline will include a detailed list of documents to be created as part of the effort and a timeline for delivery of the modules. Securicon will deliver the outline to the City's technical management team for review. The review process is crucial to a successful engagement, as the outline will provide a foundation for the actual policy development.

Milestone 2 – Delivery of draft policy modules: To facilitate in accelerating the policy development process, Securicon will deliver draft versions of each module as it is completed for the City's review. The City will provide comments and edits to the draft policy documents within 2 business days of receipt, where Securicon will have at least 5 business days to provide the final document.

Milestone 3 – Delivery of final policy modules: Once comments and edits have been received on the draft policy modules, Securicon will develop final modules for delivery to the City. Securicon has found that in its experience policy development is a highly iterative process, in which draft modules are often heavily modified and changed during the process. Because of this, Securicon expects that it will take 5-7 business days to finalize the policy modules.

B. DEVELOP PHYSICAL SECURITY CHECKLIST & CONDUCT ASSESSMENT

Utilizing the approved Physical Security Policy, Securicon will develop a checklist, tailored to the City's environment, for the assessors to use while visiting the facilities during the assessment. The draft checklist used by the assessment team will be reviewed and approved by the City management and other stakeholders. Of special interest would be areas of concern to City management, discussion of known or attempted compromises of the City infrastructure and issues unique to each of the sites.

Using the City approved checklist, a team of assessors will perform the Physical Security Assessment for approximately 55 water wells, 10 water treatment plants, 16 water storage reservoirs, 40 pump stations, 3 power generation plants, 13 electric sub-stations, major electric supply transmission points, major communication hubs, and six office buildings. Depending on staff availability and group participation preferences at the site, we anticipate 5 days on site for the in-brief and data gathering engagement. Participants may be requested to substantiate evidence of processes and capabilities discussed and evident may take the form of:

- Printouts and listings
- Screen shots from selected systems
- Photographs of systems, implementations or
- Other artifacts deemed appropriate or germane to the assessment.

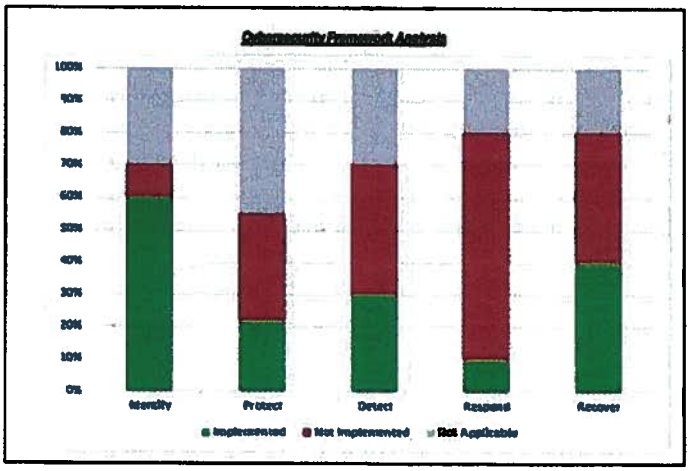
At the conclusion of each of the onsite activities, an out-brief meeting will be scheduled with the City where the preliminary findings will be reviewed to verify and clarify the findings. This will serve to re-enforce the findings identified by the various participants.

C. IDENTIFY IMPROVEMENTS

The data and artifacts collected during the assessment will be reviewed and analyzed for content and consistency and compared with industry baselines and best practices. A list of preliminary findings will be created. This will be in the form of a Preliminary Findings document with commentary on why the assessment team identified the issues listed. These issues can range from the obvious to more nuanced items uncovered in discussions. Also, typically, issues may be identified in one group's discussions that pertain to other situations, and this report provides a point of communication of those issues and a vehicle for further discussion. The Preliminary Findings document also contains a, "quick win" with remedial steps.

The draft Preliminary Findings report will be available roughly 5 business days after the on-site assessment. Occasionally, some level of disagreement arises and will be annotated as the process does allow for a "minority report" response. Verification is seeking validation on the findings—a disagreement on a specific issues it, itself, a finding and needs to be identified as such.

After the out-brief session, comments and modifications, if any, will be incorporated into a final version of the Assessment Report. The final version of the Assessment report will categorize observations and findings against the Executive Order 13636, NIST Cybersecurity Framework, and rank the completeness of security controls for each of the five classification areas. This will be represented graphically in a cart similar to the one below:



D. DEVELOP CYBER SECURITY GUIDELINES & ASSESS THE PROGRAM

Securicon will meet with the City executive management team to develop the outline and discuss the details of the Cyber Security Policy that best supports the City's business processes. Securicon will utilize the same approach that was used to develop the Physical Security Guideline, beginning with a policy outline, development of the policy modules, a review and approval by the City Management Team, followed by the finalization of the Cyber Security Policies.

Once the Cyber Security Policies have been approved and finalized, Securicon will conduct a comprehensive review of selected network and security architectures within the City's IT environment. The purpose of the architecture review is to gather a complete understanding of all current networking/security components and to identify any potential issues within the current design. The architecture review will include interviews, comparisons to policies and standards, and a review of the network management infrastructure, evaluating all for their ability to securely support the business, operational and technical requirements. The information collected in the network review will help in providing recommendations for optimization of network security, stability and performance. Securicon's network assessment methodology ensures that all necessary information is captured to accomplish successful risk analysis, with all potential performance, stability and security issues identified.

E. DEVELOP IMPLEMENTATION PLAN WITH COST ESTIMATES

Having completed the assessments against the approved security policies, Securicon will identify areas for improvement in the City's physical and cyber infrastructure. These improvements will be categorized for priority and an effort made to collect individual improvements into security posture Improvement Packages, aggregating tasks where possible to minimize costs to the City. Once the prioritized Improvement Packages are developed, an implementation plan can be developed to coordinate both the expense and scheduling of the proposed improvements.

F. VULNERABILITY ASSESSMENT REPORTING

Following the execution of each assessment phase of the task, Securicon will analyze the data collected and document all assessment methods and results in the *City of Riverside Assessment Report*. The report will include descriptions of each phase of the assessment and analysis of issues identified during the assessment efforts, along with a specific listing of each identified weakness. Each weakness will be accompanied by a description of its ability to impact the applicable network or systems, a rating of risk it creates and detailed recommendations to correct the weakness. In addition to specific technical recommendations where a pattern indicates the need for additional procedural controls, Securicon will also recommend changes in practices and procedures to prevent a reoccurrence of the weakness in the future. The report will be submitted in draft form, enabling the applicable managers and technical staff to review the report and provide feedback in the form of comments and questions. Securicon will revise the report as necessary to address the comments and deliver the final version.

Security Assessment Report(s)

The report, both in draft and final form, will include the following sections and information:

- **Executive Summary:** The Executive Summary will include a high-level description of the activities performed during the assessment and a summary of the pertinent findings. The executive summary will be written in non-technical language to ensure a broad understanding of information security shortcomings, impacts, and recommended actions. The Executive Summary Report can be delivered as a separate document or in its own major section of the main report.
- **Introduction:** Contains the task objectives and a high level description of the steps performed.
- **Description of Methods and Tools Used:** A detailed description of the processes and procedures used by Securicon to perform the task. This section contains a description of tools and techniques used by the assessment team to analyze the systems, applications and associated infrastructure.
- **Vulnerabilities and Recommendations:** The report is anticipated to include major sections dedicated to each phase of the task or each system assessed, so that portions of the report can be distributed to the appropriate groups to perform remediation activities. This section is intended to be highly technical for IT Security, System Administrators, Network Engineering staffs and any other technical stakeholders. Each major section will each contain the following subsections:
  - Description of the environment that was tested, including enticement information that was available to a potential hacker, the controls that were in place to prevent an intrusion and active security monitoring that was encountered.
  - Assessment Findings: A comprehensive list of findings associated with the objective and scope, including a detailed discussion that explains each issue discovered and it's implication. Each finding will be accompanied by an evaluation of risk it creates, based on the likelihood that the vulnerability will be exploited and the potential impact if it were to be exploited. In addition, where applicable, the descriptions will also include an evaluation of the level of expertise or knowledge required to exploit the weakness
  - Recommendations: Specific, detailed recommendation to remediate risk created by the vulnerability.
- **Appendices:** Any additional information identified as necessary or desirable by either Securicon or the City will be included in an appendix.

Risk Evaluation and Ranking

During the different phases of the assessment, Securicon will report on vulnerabilities and flaws it finds and each will be identified in the assessment report accompanied by a discussion of its potential impact and recommendations for corrective action. Each vulnerability is assigned a qualitative estimate of the risk it represents to the client's assets: critical, high, medium or low. These ratings are general estimates based on Securicon's extensive experience in conducting security assessments and vulnerability analyses. The level of risk for each vulnerability was determined through an assessment of the information obtained via the various phases of the assessment and the results of any exploitation that occurred. Both the likelihood of the threat

occurring and the potential impact to the client's information assets (if the threat should occur) were considered in the risk analysis process.

Risk is a measure of the vulnerabilities impact should it be exploited by a potential threat. For risk to exist there must be some likelihood that a threat exists, some potential impact if it should materialize, and a weakness in controls (vulnerability) that permits the threat to impact the assets. Table 1 depicts the logic of risk determination through a combination of the likelihood of occurrence of a particular threat and the potential impact if it were to occur. Though these separate factors are not listed individually for the risk ratings, it is important to understand that they form a basis for risk determination.

		Potential Impact				
		Critical	High	Medium	Low	
Likelihood of Occurrence	Critical	Critical	Critical to High	Medium to High	Medium	Resultant Risk
	High	High to Critical	High	Medium to High	Medium	
	Medium	High	Medium to High	Medium	Low to Medium	
	Low	High	Medium	Low to Medium	Low	
Example: If the likelihood is high that the vulnerability will be exploited, but the potential impact of that exploitation is low, the resulting severity would typically be rated as Medium.						

Table 1 - Explanation of Severity Ratings

The likelihood that a threat will occur is shown on the left side of the table. The likelihood of occurrence is largely based on a combination of the threat assessment and the architecture of the system and network, as modified by any existing protective measures. Explanations of critical, high, moderate and low likelihood of occurrence conditions are listed in the following bullets:

- **Critical Likelihood of Occurrence** – These are vulnerabilities that are very likely to be exploited because they are exposed to a very large potential attack audience and can be exploited by readily available, public tools and/or the need for very little expertise.
- **High Likelihood of Occurrence** – These vulnerabilities are somewhat less likely to be exploited because they require some, though little, effort to discover, are exposed to a large potential attack audience, and can be exploited with slightly more obscure tools and exploits and require some level of sophistication on the part of the attacker.
- **Medium Likelihood of Occurrence** – These vulnerabilities are not as likely to be exploited due to their exposure to a smaller malicious audience or because they are more difficult to exploit or require significant expertise on the part of the attacker.
- **Low Likelihood of Occurrence** – These vulnerabilities are unlikely to be exploited because they are exposed to a very limited audience or require extensive knowledge or where the vulnerability either requires other factors to be present (such as a race condition, non-standard configuration, etc.) or have vulnerabilities that have proven to be largely theoretical in nature.

The other factor in determining risk is the potential impact that exploitation of the vulnerability would have to the client. Here again, potential impact ratings of critical, high, moderate, and low are used. Explanations of these impact conditions are described below:

- **Critical Potential Impact** – These are vulnerabilities that, if exploited, could severely and negatively impact business, operations, information, and reputation in a manner from which it would be difficult and potentially expensive to recover.
- **High Potential Impact** – These vulnerabilities, if exploited, would seriously and negatively impact business and operations and would require significant effort and expense to repair or recover.
- **Medium Potential Impact** – These are vulnerabilities that, if exploited, could moderately impact business and operations and may require some expense from which to recover.
- **Low Potential Impact** – These are vulnerabilities that, if exploited, could represent a minimal impact to business and operations and may not require any significant investment from which to recover.

The goal of the Assessment Report will be to provide an action plan that can be used to improve both the existing security posture, as well as the security management program in general.

Presentations and Meetings

Securicon will conduct a presentation for Executive/Management teams. The presentation can be conducted remotely with WebEx/PowerPoint or in-person (Securicon is located in the Washington DC area). The presentation will be organized for approximately 90 minutes, with 45-60 minutes as actual presentation and the remainder for questions and answers. The presentation will provide:

- Overview of findings
- Comparison of findings to peer institutions
- Ranking/Benchmarking relative to peer financial institutions
- Overview of threat landscape
- Recommendations

The presentation can be performed on site or remotely through WebEx, at the City's option. Note that Task 2.12 in the pricing section is for an optional on site presentation of the final VA Report.

TASK 3 - ADDITIONAL ENGINEERING SERVICES

A. ADDITIONAL SERVICES

As requested in the RFP, Securicon will include a controlled allowance for additional services to be performed if desired by the City. This portion of the assessment will not exceed 10% of the total project.

Our most commonly-requested professional services categories are listed below. However, we are happy to discuss and explore issues your organization is facing that might fall outside those listed here. We can customize a solution for every need.

Security Assessments	Our unique approach combines traditional assessment methodologies with controlled penetration techniques and cooperative analyses to identify and assess risks and weaknesses. All assessments are combined with clear and concise recommendations for remediation.
Network Security Architecture Consulting	Our services include thorough reviews of existing architectures, cost-effective recommendations to improve security, and redundant, cascading security controls to create a defense-in-depth architecture.
Application Security Services	Securicon's application security services span the application life cycle and include design evaluations, vulnerability and penetration assessments, remediation services, and education to prevent vulnerabilities before they are able to impact business operations.
Governance, Risk Management, Compliance	In addition to framing our recommendations in terms of applicable GRC guidance, we also help clients meet such rigorous information security regulatory requirements as NERC CIP, HIPAA, FISMA, and more.
Cloud Security Services	We strengthen the security capabilities of cloud service providers' applications, products, and appliances through FedRAMP and FISMA gap analyses, security architecture reviews, penetration and vulnerability assessments, application assessments, FedRAMP-compliant policies and procedures, and FedRAMP-compliant authorization package development.

B. SCADA PENETRATION TEST

As requested in Addendum 01 of the RFP, Securicon has provided the methodology below for a SCADA penetration test as an optional service.

The goal of the External Network Security Assessment is to identify security risks and vulnerabilities that may exist in the City's external network and systems, evaluate the risk associated with any identified vulnerabilities, and to develop strategies and recommendations to resolve these issues and reduce the risk to an acceptable level.

Securicon has thirteen years of experience in performing vulnerability assessments and penetration tests in SCADA and industrial control networks. The techniques we use are adaptive to the types of equipment we discover in the operational environment under test. We are aware that:

- Some SCADA devices do not respond well to traditional scanning techniques
- The first priority of any industrial control environment is maintaining availability, so any disruption is unacceptable

Because of these conditions, Securicon has developed a methodology that separates manual and automated components to achieve the desired objectives of the assessment while not introducing operational risk into the environment under test.

Using this specialized methodology, Securicon will conduct a controlled assessment to identify weaknesses in the external security perimeter of the City's network. Where potential vulnerabilities are identified, Securicon will validate them and eliminate false positive results from the reported findings. Initial efforts of the assessment team will be to identify vulnerabilities in systems that can be reached directly from the Internet and to logically map the gateway topology. The ultimate goal is to determine if unauthorized access is possible to the City's internal systems.

Testing will be nondestructive in nature (i.e. there will be no denial of service tests mounted). However, where applicable, systems and configurations susceptible to denial of service attacks will be noted. No tools or techniques are used on client systems without first being thoroughly tested.

Specific goals of external testing are to:

- Identify external points of access between the SCADA environment and the City's networks
- Identify vulnerabilities in externally accessible systems
- Identify potential vulnerabilities in network access controls, firewalls, routers, and the designed network topology, even if they do not immediately provide access to the SCADA network
- Determine through analysis, if it might be possible to combine the identified vulnerabilities and the network design and topology to gain access to the SCADA network directly or indirectly from the Internet

Vulnerabilities of multiple components will be compared with the gateway architecture to determine if multiple minor weaknesses could be combined to provide stepping-stones to create a much greater risk of intrusion.

Though the specific tests vary, based on the SCADA network topology, interfaces with City and vendor networks and the types of equipment encountered, the overall methodology is described in the following sections.

Information Gathering and Research

- Passive Information Gathering - Prior to the beginning of active penetration efforts, the Securicon Test Team will conduct an extensive research effort to gather information on the City networks and components. The collection of publicly available information concerning a target network is a vital first step in a penetration effort. A wealth of information about any public network is available via a series of internetworking system services, as well as through use of information gathering tools. The types and importance of the information varies with each service and tool, but together this information can be used to identify potential vulnerabilities that may enable a successful penetration of the network perimeter.
- Network and System Services Discovery - Physical network design and routing information can often be determined through use of IP scanning tools, trace routes, and probes against various routing protocols. Depending on the network topology and devices observed or suspected in the SCADA environment, Securicon will identify targets for scanning and targets for manual inspection. First, focusing on the scanning targets, the team uses IP scanning tools to perform discovery of systems within the customer's gateway IP addresses. Each system that is discovered is scanned for active network services, using a combination of public, commercial off the shelf and proprietary scanning tools. For the targets to be manually inspected, Securicon will rely on information gleaned from running configurations, contents of CAM tables on routers and other sources to determine the addresses, ports and services for those devices.. These activities will result in a collection of common results for the set of hosts and services which are active on the target systems and the set of services which are permitted to pass through any firewalls or routing filters. In many cases, it will also show which services are being blocked by firewall or routing filters.

Vulnerability Assessment of Exposed Systems

Each targeted device or system will be evaluated for vulnerabilities that reduce its security profile. Though there are far too numerous specific vulnerabilities to discuss in detail here, the following paragraphs discuss the process for identifying some of the major types of vulnerabilities.

- Vulnerable Versions of Software - Many systems that have not been fastidiously updated are running vulnerable versions of software that provides network services. These outdated network services contain software bugs that enable the service to be manipulated into providing information or even providing unauthorized access to the system. Therefore, once all active hosts and services have been identified, Securicon will probe these services to identify their make and versions, and will cross-reference the active services against a database of potentially vulnerable services.

- Anonymous Access - In addition to versions of software, simple misconfigurations and insecure use of certain protocols can permit the compromise of a system. Systems that might permit anonymous access are checked for anonymous read, and even more importantly, anonymous write access. If access is discovered, an Engineer checks the service to determine if access exists to directories that might be used to create unauthorized access, denial of service, or to plant malicious software. Services that commonly provide anonymous access include HTTP (web), FTP and TFTP (file transfer), and NFS and NetBIOS (network file sharing).
- Weak Protocols - A number of services, such as point-to-point tunneling protocol (PPTP), remote procedure call (RPC) and X-Windows (X.11) may rely on processes that are weakly authenticated, not authenticated at all, or weakly protected from eavesdropping. These protocols may be vulnerable to attacks that exploit the services or take advantage of the lack of authentication. Systems that have active such services are checked for access controls and susceptibility to spoofing and exploitation of trust relationships. In this way, recommendations are not only offered about the dangers of the general use of some of the more vulnerable of these services, but specific services that are vulnerable to known attacks in the active configurations and versions are listed in the vulnerabilities.
- VPN Testing – The high prevalence of Virtual Private Network installations now means that internal networks can be exposed with a single vulnerability in the VPN server or a misconfiguration that results in weak internal passwords for guest or service accounts being used to authenticate to a VPN server. All externally exposed VPN services are checked for common vulnerabilities, patch levels, and weak authentication.

Manual Vulnerability Validation / False Positive Elimination

Securicon will collect data from automated vulnerability scanners, proprietary tools and manual assessment efforts in order to build a normalized list of identified exposures. Vulnerabilities will then be manually validated, in order to make a determination of whether the respective, reported vulnerability represents an actual exposure, how that exposure may impact the system, and other systems on the network, and any mitigating factors which may prohibit the vulnerability from being exploited in certain conditions, or without certain prerequisites (such as authentication credentials).

While validation methodologies will vary based upon the nature of the vulnerability being analyzed, the methodologies we employ are chosen for being both viable in the time available, and benign in nature, so as to minimize any potential operational impacts on the system. Finally - no validation techniques used during this phase of testing involve the exploitation of software, or operating system type vulnerabilities (such as buffer overflows, denial of service conditions and format string attacks).

Penetration Testing vs Vulnerability Assessments

In Securicon's network vulnerability assessment the engineer will test the exploitability of vulnerabilities and application/infrastructure flaws identified both individually and in combination. The object of the vulnerability assessment is to come up with a registry of findings for which there is a high probability that they can be turned into an exploit to compromise the

integrity of the system or data, or to allow the theft and unauthorized manipulation of data and resources.

For a Penetration Test, the Securicon Engineer will take the analysis the next step and actually attempt the exploitation. Securicon assumes the role of a malicious attacker and attempts to capture sensitive data, change access privilege, change user context and other activities to probe the extent that a malicious party can compromise the network or application.

Securicon's rules of engagement include:

- Both Securicon and the client will establish a point of contact individual who will be available during the testing time period to answer questions or to modify of halt testing activities if necessary
- Securicon will not attempt brute force password compromise unless specifically requested by the client
- Securicon will not use high volume network traffic to force denial of service situations, and
- If Securicon encounters any issue it considers to be a critical security concern, the engineer will halt the test and escalate the issue to the specified client point of contact.

C. PERSONNEL

The Securicon Project Team will consist of not only a Project Manager and team of experts but also an Executive oversight, which is standard for every major project we conduct. Our engagement process is designed to insure 100% satisfaction from start to completion. Our team members that will conduct the engagement will be 100% dedicated to this task.

All persons assigned to this project are engineering professionals with experience in all facets of cyber security for real time controls systems as well as the corporate enterprise. Securicon is one of the very few providers that blends IT professional expertise with real time control system expertise from one organization

Securicon assigns our consultants from a resource pool on a per-engagement basis, based upon their experience in the applicable area of information security. The following sections present bios of the staff that will comprise the talent pool for this assessment. Full resumes are included in Appendix A.

Project Management

Securicon's approach to task management combines an on-site task lead with a Project Manager for oversight. However, all task personnel are directly responsible to Securicon's VP of Security Services, Mr. Harry Regan.

- **Mr. Harry Regan, CISSP, CISM, PSP – VP, Security Services:** Mr. Harry Regan is a security, information technology (IT) and operations professional with over 30 years of commercial, federal, and defense experience. He has functioned in executive, senior technical staff, and consulting engagements with assignments encompassing corporate and program management, computer and network operations, and executive-level consulting. Mr. Regan has extensive experience with physical security, as well as

EXHIBIT "B"

COMPENSATION

D. ESTIMATE OF CONSULTING FEE

LEVEL OF EFFORT

The price quote below is based on Securicon's understanding of some basic information about the City. Utilizing the information provided in the RFP, we have estimated how much consulting and engineering time will be required for the task. The following table reflects estimated level of effort to accomplish the assessment, as described in this proposal.

Description	Duration in Business Days	Engineers	Estimated Assessment Hours
Task 1 - Project Management Services			
Task 1.1 Pre-engagement Planning	3	1	24
Task 1.2 Project Kickoff Meeting	2	1	2
Task 1.3 Project Status Meetings and Project Support	Recurring	1	59
Task 2 - Vulnerability Assessment			
Task 2.1 Develop Draft Physical Security Guidelines	7	2	112
Task 2.2 Develop Draft Cyber Security Guidelines	10	2	160
Task 2.3 Coordinate Final Physical Security Guidelines	3	1	24
Task 2.4 Coordinate Final Cyber Security Guidelines	3	1	24
Task 2.5 Conduct City Physical Protection Assessment	5	2	120
Task 2.6 Develop City Physical Protection Recommendations	5	2	80
Task 2.7 Conduct City Cyber Protection Assessment	8	2	192
Task 2.8 Develop City Cyber Protection Recommendations	8	2	128
Task 2.9 Develop Plan and Estimate for Recommendation Implementation	7	2	112
Task 2.10 Develop Draft VA Report	10	1	80
Task 2.11 Develop Final VA Report	5	1	40
Task 2.12 On-site Presentation of the Final VA Report	2	2	32
Task 3 - Additional Engineering Services			
Task 3.1 Additional Engineering Services (Optional)	TBD	TBD	TBD
Task 3.2 SCADA Penetration Test (Optional)	5	1	63
Total Hours			1252

Note: The draft report is typically delivered two weeks after completion of all testing. This allows for analysis of the collected data, development of recommendations, documentation of the draft report, and both peer and management review.

PRICE QUOTE

Securicon has priced the Assessment on a Time and Material (T&M) basis, based on an hourly consulting rate and the defined scope. Securicon expects the engagement to incur approximately 1252 hours of senior security consultant time. However, additional time can be added at the client's discretion, if a change in scope is desired.

Description	Estimated Labor Hours	Estimated Labor Cost	Estimated Travel	Estimated Total Cost
Task 1 - Project Management Services				
Task 1.1 Pre-engagement Planning	24	$5,400	$0	$5,400
Task 1.2 Project Kickoff Meeting	2	$450	$0	$450
Task 1.3 Project Status Meetings and Project Support	59	$13,275	$0	$13,275
Task 2 - Vulnerability Assessment				
Task 2.1 Develop Draft Physical Security Guidelines	112	$25,200	$6,300	$31,500
Task 2.2 Develop Draft Cyber Security Guidelines	160	$36,000	$8,400	$44,400
Task 2.3 Coordinate Final Physical Security Guidelines	24	$5,400	$0	$5,400
Task 2.4 Coordinate Final Cyber Security Guidelines	24	$5,400	$0	$5,400
Task 2.5 Conduct City Physical Protection Assessment	120	$27,000	$4,200	$31,200
Task 2.6 Develop City Physical Protection Recommendations	80	$18,000	$0	$18,000
Task 2.7 Conduct City Cyber Protection Assessment	192	$43,200	$6,300	$49,500
Task 2.8 Develop City Cyber Protection Recommendations	128	$28,800	$0	$28,800
Task 2.9 Develop Plan and Estimate for Recommendation Implementation	112	$25,200	$0	$25,200
Task 2.10 Develop Draft VA Report	80	$18,000	$0	$18,000
Task 2.11 Develop Final VA Report	40	$9,000	$0	$9,000
Task 2.12 On-site Presentation of the Final VA Report	32	$7,200	$2,100	$9,300
Task 3 - Additional Engineering Services				
Task 3.1 Additional Engineering Services	TBD	$28,170 *(10% of Task)*	$2,730	$30,900
Task 3.2 SCADA Penetration Test	63	$14,175	$2,100	$16,275
Total Cost	**1252**	**$309,870**	**$32,130**	**$342,000**

Securicon shall invoice the City its out-of-pocket, reasonable travel expenses, which are anticipated not to exceed **$32,130.** Reasonable travel expenses means that Securicon engineers travel at coach class airfare and stay in normal business class lodging (such as Marriott Courtyard). Meals are invoiced at Government per-diem rates, which can be verified at government web sites, such as http://www.gsa.gov/portal/category/21287

All prices are valid for 60 days.

E. COMPLETION SCHEDULE

The proposed schedule below assumes the use of two engineers working in order to parallel some of the task elements. Of course, we are willing to work with the City to define a schedule that meets with the client's timing and business requirements.

Example Schedule - Based on a Start Date of January 4, 2016			
Project Phase	**Duration in Bus. Days**	**Start**	**Complete**
Assessment Planning	10	01/04/2016	01/15/2016
Kick-off call to finalize the schedule and rules of engagement.	1	01/06/2016	01/06/2016
Develop Physical Security Guidelines			
Review existing Physical Security Policies	4	01/19/2016	01/22/2016
Develop unified Physical Security Guidelines and Checklists	5	01/25/2016	02/01/2016
City to Review and Approval of Guidelines	10	02/02/2016	02/16/2015
Finalize unified Physical Security Guidelines and Checklists	4	02/17/2016	02/22/2016
Conduct Physical Assessments at defined locations	5	02/29/2016	3/04/2016
Develop Cyber Security Guidelines			
Develop Cyber Security Guidelines	11	02/01/2016	02/15/2016
City to Review and Approval of Guidelines	10	02/16/2016	03/01/2016
Finalize Cyber Security Guidelines	4	03/02/2016	03/07/2016
Conduct Cyber Assessments for defined assets	10	03/14/2016	03/25/2016
Implementation Plan			
Develop the Implementation Plan with Cost Estimates	20	03/28/2016	04/22/2016
City to Review and Approval of Implementation Plan	15	04/25/2016	05/13/2016
Finalize the Implementation Plan with Cost Estimates	10	05/16/2016	05/27/2016
Vulnerability Assessment Report			
Draft Vulnerability Assessment Report	15	04/23/2016	05/02/2016
City to Review Assessment Report	23	05/03/2016	06/03/2016
Final Vulnerability Assessment Report	4	06/06/2015	06/13/2016
Total Project Duration	**113 Days**	**01/04/2016**	**06/13/2016**

ATTACHMENTS - CONTRACTS

Securicon has reviewed both the Professional Services Agreement and the Non-Disclosure Agreement provided in the RFP and takes no exceptions to either agreement.

EXHIBIT "C"

KEY PERSONNEL

integrity of the system or data, or to allow the theft and unauthorized manipulation of data and resources.

For a Penetration Test, the Securicon Engineer will take the analysis the next step and actually attempt the exploitation. Securicon assumes the role of a malicious attacker and attempts to capture sensitive data, change access privilege, change user context and other activities to probe the extent that a malicious party can compromise the network or application.

Securicon's rules of engagement include:

- Both Securicon and the client will establish a point of contact individual who will be available during the testing time period to answer questions or to modify of halt testing activities if necessary
- Securicon will not attempt brute force password compromise unless specifically requested by the client
- Securicon will not use high volume network traffic to force denial of service situations, and
- If Securicon encounters any issue it considers to be a critical security concern, the engineer will halt the test and escalate the issue to the specified client point of contact.

C. PERSONNEL

The Securicon Project Team will consist of not only a Project Manager and team of experts but also an Executive oversight, which is standard for every major project we conduct. Our engagement process is designed to insure 100% satisfaction from start to completion. Our team members that will conduct the engagement will be 100% dedicated to this task.

All persons assigned to this project are engineering professionals with experience in all facets of cyber security for real time controls systems as well as the corporate enterprise. Securicon is one of the very few providers that blends IT professional expertise with real time control system expertise from one organization

Securicon assigns our consultants from a resource pool on a per-engagement basis, based upon their experience in the applicable area of information security. The following sections present bios of the staff that will comprise the talent pool for this assessment. Full resumes are included in Appendix A.

Project Management

Securicon's approach to task management combines an on-site task lead with a Project Manager for oversight. However, all task personnel are directly responsible to Securicon's VP of Security Services, Mr. Harry Regan.

- **Mr. Harry Regan, CISSP, CISM, PSP – VP, Security Services:** Mr. Harry Regan is a security, information technology (IT) and operations professional with over 30 years of commercial, federal, and defense experience. He has functioned in executive, senior technical staff, and consulting engagements with assignments encompassing corporate and program management, computer and network operations, and executive-level consulting. Mr. Regan has extensive experience with physical security, as well as

information security and privacy program development; threat and vulnerability assessments; technology countermeasures; System Control and Data Acquisition (SCADA) systems; building and industrial infrastructure protection; NERC Critical Infrastructure Protection (NERC-CIP); and regulatory compliance. Throughout his career, Mr. Regan has also gained subject matter expertise and knowledge of computer and network operations management; technology assessments; high performance architectures; disaster recovery and business continuity planning; and new technology integration. Mr. Regan has received recognition for his expertise and has been featured in interviews on CNN and NBC regarding the operability and effectiveness biometrics and other security technologies. Mr. Regan manages the Securicon commercial security consulting team and is responsible for overseeing the successful execution of commercial engagements and ensuring successful delivery of services to our customers.

Each multi-phase, multi-milestone task is assigned a project manager to ensure the customer has a single Securicon point of contact with which to coordinate assessment activities and documentation review and approvals. Ms. Debra Rosen, one of our highly experienced Managing Consultants, is assigned Project Manager for this task.

- **Debra Rosen, Director, Critical Infrastructure Services:** Ms. Rosen is a Program Manager for all Securicon NERC Critical Infrastructure Protection (CIP) Vulnerability Assessments and Commercial Services security projects, with over 14 years of experience in the IT and security fields. As is the case with many Securicon Security Engineers, Debra Rosen first began her career in IT and moved into information security/assurance after establishing an expert level of knowledge in IT in general. In her case, she began as a Software Test Manager for SAIC for her first four years. After SAIC, she worked in Information Assurance for General Dynamics and was tasked with leading the Integration Test group within the Systems Assurance Program at the Federal Energy Regulatory Commission (FERC) and also supported IV&V (independent verification and validation) testing for an IRS contract. After transitioning from IT to security in 2006, Ms. Rosen joined the Security Services team in Verizon Business Professional Services group. After Verizon, Debra spent a year and a half with the information security company, Symantec, before joining Securicon in 2012. Ms. Rosen holds a master's degree in Information Systems from George Washington University, Washington, DC, awarded in 2006; and has a Project Management Professional (PMP) certification. Ms. Rosen received certification as a Certified Information Security Professional (CISSP) in 2015.

Assessment Team

The technical assessment team will include individuals chosen from Securicon's staff of senior security consultants, based on availability, as well as the goals and scope of each phase of the task. The following bios are anticipated to form the talent pool from which Securicon's consultants will be chosen for this task.

- **Ernie Hayden – Executive Consultant:** Ernie is a highly experienced and seasoned technical consultant, author, speaker, strategist and thought-leader with extensive

experience in the power utility industry, critical infrastructure protection/information security domain, industrial controls security, cybercrime and cyberwarfare areas. His primary emphasis is on project and business development involving cyber and physical security of industrial controls, smart grid, energy supply, and oil/gas/electric systems and facilities with special expertise on industrial controls and NERC Critical Infrastructure Protection (NERC CIP) standards. Hayden has held roles as Global Managing Principal – Critical Infrastructure/Industrial Controls Security at Verizon, held information security officer/manager positions at the Port of Seattle, Group Health Cooperative (Seattle), ALSTOM ESCA and Seattle City Light. In 2012 Ernie was named a "Smart Grid Pioneer" by Smart Grid Today and published an article on Microgrid security in Jesse Berst's Smart Grid News Ernie is a frequent author of blogs, opinion pieces and white papers. He has been cited in the Financial Times, Boston Globe, Energy Biz Magazine, and Puget Sound Business Journal. Many of his articles have been posted to such forums as Energy Central, Public Utility Fortnightly "SPARK," and his own blog on Infrastructure Security. He is an invited columnist for the "Ask the Experts" discussions on www.searchsecurity.com and he published an article regarding electric grid security versus compliance in Public Utility Fortnightly magazine. Other thought-leadership articles have included a chapter on "Cybercrime's Impact on Information Security," in the Oxford University Press Cybercrime and Security Legal Series and several articles in Information Security Magazine including his original research on data lifecycle security and an article on data breaches in the same publication. Ernie is a very active contributor in global security forums. His past includes membership in the Cloud Security Alliance where he was the leader for the Information Lifecycle Domain in the Cloud Security Guidelines document Version 2. He has also been an instructor, curriculum developer and advisor for the University of Washington Information System Security Certificate program in Seattle. Additionally, Ernie has been a contract instructor for the Cyberterrorism Defense and Analysis Center, sponsored by the U.S. Department of Homeland Security. One of his technical papers on cybersecurity governance of the U.S. electric grid received "Best Paper Award" at the 2012 Critical Infrastructure Symposium co-sponsored by the Society of American Military Engineers (SAME). Ernie is a CISSP - Certified Information Systems Security Professional, Certified Ethical Hacker (CEH) and SANS Global Industrial Controls Security Professional (GICSP - GOLD) and holds the ISA99/IEC 62443 Cybersecurity Fundamentals Specialist certificate. He is also a member of ASIS. He received a Masters of Infrastructure Planning and Management and a Bachelors Degree in Business Administration (with International Business emphasis) both from the University of Washington in Seattle. He is also a graduate of the FBI Citizens Academy, Seattle Police Department Citizens Academy, US National SCADA Test Bed (NSTB) SCADA Security Course, and Center for Creative Leadership - Leadership Development Program..

- **Harrison Chang – Senior Security Consultant:** Mr. Chang is an Information Technology (IT) consulting professional with over 7 years of industry experience in network security assessments, compliance audits and consulting, and IT support in a number of industries, including power and energy, financial services, and medical research. He has

extensive experience conducting vulnerability assessments, penetration testing, NERC CIP assessments, as well as conducting IT support, logistics, prototyping new technologies, data, and business analytics. He is also knowledgeable of cloud computing concepts and offerings. Harrison holds a B.A. degree in Information Systems, from the University of Maryland, awarded in 2007. Mr. Chang supports both the Securicon IT Department and the Security Commercial Security Services Division; conducting security audits and assessments for Securicon's clients. He participates with assessment teams to conduct security and network penetration assessments, as well as assisting on tasks involving North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection Standards (CIP) compliance reviews and in security architecture consulting tasks. Mr. Chang's NERC CIP customers have included National Grid, MidAmerican Energy, Constellation and others.

- **Lee Mazza - Senior Security Consultant:** Lee Mazza is an Information Technology consulting professional with over 15 years of experience in the IT field. Lee has extensive experience with information security testing, auditing and data analytics; including penetration tests, vulnerability assessments, web application assessments, and IT audits. Lee has also performed as part of Incident Response (IR) teams responding to data breaches, as well as architectural network design reviews of various Enterprise, Government, Educational, Utility and Health Care network infrastructures and the implementation of various network components (Routers, Switches, IDPs, WAFs, Proxys, Firewalls). Other engagements Lee has performed include implementation projects, forensics, system hardening, VoIP, and various policy reviews (ISO-27001:2005, 17799:2005, PCI).

- **Matthew Bebout, Senior Security Consultant:** Matthew Bebout is an Information Technology consulting professional with over 10 years of experience in the IT field. Mr. Bebout has extensive experience with information security testing and policy development, software testing, and software development. For his clients, Mr. Bebout has conducted penetration tests and vulnerability scans. Mr. Bebout has also assisted a previous employer in creating policies to support data protection. Prior to joining the commercial sector, Mr. Bebout has worked the majority of his career in the government sector in roles relating to information security, software testing, and software development. Mr. Bebout holds multiple certifications including an ISC^2 Certified Information Systems Security Professional (CISSP) and has attended a wide variety of IT security related training.

- **Phil Grimes, Senior Security Consultant:** Phil Grimes is an Information Technology consulting professional with over 10 years of experience in the IT field. Mr. Grimes has extensive experience with architecture evaluations, information security testing, social engineering and data analytics for organizations ranging from small business, financial institutions, the power industry, e-commerce, telecommunications, manufacturing, education, and government agencies. For his clients, Mr. Grimes has conducted penetration tests, vulnerability assessments, architecture evaluations, and IT audits. Mr. Grimes has also assisted clients in creating Information Security Programs including

Disaster Recovery and Business Continuity. Mr. Grimes also has significant experience with ICS and SCADA assessments as well as Incident Response cases, malware reverse engineering, web application security, and mobile/smart phone security. Mr. Grimes is an active public speaker. He presents at various industry conferences and discussion sessions on technology and security topics to his clients.

- **Philip Marasco, RHCE, CISSP – Senior Security Consultant:** Mr. Marasco has over 19 years experience in the technical operations delivery and information security industries with an emphasis on network operations, network security monitoring design, and operational security implementation. Mr. Marasco's recent clients include Chevron, ATCO Power, Minkota Power, TransCanada, and the Defense Advanced Research Projects Agency (DARPA). His expertise ranges from conducting NERC CIP compliance gap analyses to CIP 005 and 007 vulnerability assessments and penetration testing, to consulting on the system and network security aspects of Chevron's refinery modernization program. Mr. Marasco is one of Securicon's presenters in the joint KEMA/Securicon/Iowa State University course, Control Systems Cyber Security - Achieve Compliance and Secure Your Systems. His past experience includes deploying enterprise level solutions using the latest technologies, leading integration teams and performing hands-on infrastructure deployment tasks. However, in the last several years, he has been totally dedicated to security services. He has managed tasks resulting in the successful certification and accreditation of over 30 federal systems and has also conducted numerous security assessments of commercial networks and systems. Mr. Marasco has strong written and verbal communication skills, making him equally comfortable in discussions with the Chief Information Officer (CIO) or with the system design engineer. These skills are applied to responding to customer requirements, developing project management plans, writing security plans, implementation procedures, and other documentation to support client projects.

- **Valerie Thomas, Principal Security Consultant:** Ms. Thomas is a passionate security professional with a diverse technical and management background in vulnerability assessment, penetration testing, social engineering, and security compliance. Her strong educational and leadership background enables her to quickly employ new information and concepts in an operational environment. She has not only worked extensively in vulnerability and penetration assessment roles, she has also worked extensively in social engineering, data loss prevention and intrusion monitoring and prevention. Ms. Thomas is a recognized information security authority. Her recent speaking engagements have included conferences around the United States, as well as conferences in Europe and Asia. Valerie has spoken at DerbyCon, DefCon Shmoocon, Nordic Security Conference, BSides, and many others. In addition to many whitepapers and articles, Valerie recently co-authored the book from Syngress Publishing, titled *Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats*, currently available through Amazon and other sources.