SECURANCE CONSULTING

Date: October 11, 2016

Response to Request for Quotes Number 003002:
Application and Network Testing

THE CITY OF COLUMBUS

Contact for RFP Response:

Gillian Tedeschi
Director of Sales & Marketing

gtedeschi@securanceconsulting.com
Office: 877.578.0215 ext. 230
Fax: 813.960.4946

Corporate Office

Securance Consulting
6922 W. Linebaugh Avenue
Suite 101
Tampa, FL 33625
www.securanceconsulting.com

Project Office

Securance Consulting
20 S Third Street
Columbus, OH 43215
www.securanceconsulting.com

SBA-DB | FL-MBE | NMSDC
MBE
Minority Business Enterprise

Table of Contents

SECURANCE CONSULTING

October 11, 2016

Sam Orth III
Director of Technology and CTO
City of Columbus
90 West Broad Street
Columbus, OH 43215

Dear Sam,

Thank you for considering Securance Consulting as your IT risk management partner. Eager to work with the City of Columbus, Department of Technology (City), we appreciate this opportunity to present a plan for your upcoming project.

We are a firm of Senior IT Consultants passionate about helping organizations like yours assess and improve their compliance profiles, risk management programs and IT security postures. Ours is a unique combination: remarkable skill and expertise, reasonable pricing and people who care. We apply our knowledge, years of experience and industry-leading assessment tools to identify and remediate risks before they harm operations and business.

Based on our understanding of the RFP, the City seeks a partner with cyber security expertise to identify and test vulnerabilities in the City's system and network that internal and l or external adversaries could exploit. We will conduct internal and external penetration tests to assess network devices, servers and workstations. We will also perform web-application testing and then provide a prioritized plan to remediate risks.

Securance has expertise working with government agencies of similar size and technology footprint. Recent clients include:

- City of Thornton, Colorado
- Franklin County, Ohio
- Illinois State Board of Education
- Minnesota State Retirement System
- New York City Housing Authority
- Ohio Public Employees' Retirement System

When it comes to achieving your IT objectives, selecting the right vendor is crucial. Our interest is in forging a positive, long-term relationship with you, as we do with all of our clients. We will attend to your organization's particular needs and goals and will support you throughout -- and after -- the remediation phase. Again, thank you for including Securance in your evaluation process. If you have any questions regarding our proposal, please do not hesitate to contact us.

5.1.1 Offer Period

Our response is valid for one hundred eighty (180) days.

5.1.2 Signature

Paul Ashe, President of Securance, is authorized to contractually bind the firm to perform all services described in this proposal.
pashe@securanceconsulting.com
877.578.0215

5.1.3 Identify Materials

For a list of materials enclosed, please see the Table of Contents.

5.1.4 Contact Information

Gillian Tedeschi, Director of Sales and Marketing
gtedeschi@securanceconsulting.com
6922 W. Linebaugh Ave., Suite 101
Tampa, FL 33625
877.578.0215

Professional regards,

Paul Ashe, CPA, CISA, CISSP
President & Sr. IT Security Consultant
Securance Consulting

5.2 Section Two: Competence

5.2.1 Company History | Facts

Securance Consulting is a professional services firm dedicated to IT security, internal audit risk consulting and compliance. In a decade of rapid and substantial growth, Securance Consulting has found success through the power of a simple idea: deliver uncompromising, high-quality services at a reasonable cost, and customers will follow.

Securance was founded on March 4, 2002, by a former trusted member of a "Big 4" consulting team. The founder felt that his experience at Ernst & Young had provided him with an understanding of the challenges that many different kinds of companies face -- as well as what it would take to master those challenges. Securance set out to deliver outstanding results to each and every client and to ensure that projects were always done right. The mission of Securance was twofold: to convince hundreds of companies about the importance of risk and audit services, and to deliver outstanding services in those areas.

Unlike many consulting firms, Securance does not look to hire new college graduates; rather, Securance only hires professionals with a minimum of 15 years' experience. Generally, that means people with Big 4 experience. Each new hire needs to have special technical strength or leadership skills in order to act as team leader. Our professional consultants are highly competent and continually train to remain current in evolving trends and audit regulatory compliance issues. We are frequently asked to speak as subject matter experts at select industry conferences and meetings.

From its inception, Securance has been willing to "go the extra mile" to ensure client satisfaction. With that kind of commitment, clients become true partners. "Our motto is **'Get it right the first time, every time,'** and that means we want it to be done right, on time and on budget, the first time and every time," says the founder.

A summary of our professional services and areas of expertise can be found below.

Summary of Professional Services

- IT Audit and Risk Assessment
- Cybersecurity Assessments
- Vulnerability Assessments and Penetration Testing
- Internal Audit Outsourcing | Co-sourcing
- Compliance (SOX, PCI, GLBA, HIPAA, etc.)
- Information Security Program Review | Development
- Virtual CISO Services
- Business Process Review | Redesign

Areas of Expertise

- IT Risk Management in the following areas:
  - Network Security (LAN, WAN, Wireless)
  - Application and Database Security
  - Operating System Security
  - Cloud Security
  - IT Process Improvement Analysis
  - IT Policy | Procedure Development
  - Disaster Recovery Planning

Securance Added Value

- Most comprehensive risk database.
- We review our client's security posture and provide suggestions about areas that may be improved.
- As a professional services firm, our advanced knowledge of emerging audit guidance and technologies means that we know about an industry's risk before our clients do. We are able to freely share this information.

Just a Few of..."The Securance Differences"

- No junior staff. All of our staff have at least 15 years of experience.
- Our Executive Team will have hands-on involvement with every project, not just with project management.
- We are not driven by budget requirements. If there is extra work to do, we will do it and will not add billings to the project.
- We are truly our client's partner. We assist our clients even when we are not under contract.

5.2.2 Qualifications

5.2.2.1 Similar Engagements

Securance consultants have experience working on projects of similar scope and complexity as the City's upcoming project. Organizations that have trusted Securance to perform similar projects include:

Project	Summary of Scope	Client Name
Information Security Assessment and Penetration Testing	In 2016, Securance conducted a Network and Information Technology (IT) Security Vulnerability Analysis and Security Assessment on behalf of McHenry County's Internal Audit department. The overall objective of this engagement was to perform specific controlled security penetration and diagnostic activities to assess the overall level of security that has been implemented over county's systems and to ensure that "best practice" controls are being used to mitigate known security risks. The scope of the engagement included: external network vulnerability assessment and penetration test; internal network vulnerability assessment and penetration test; wireless network assessment; and social engineering.	**McHenry County, Illinois**
Security Vulnerability Assessment	In 2016, Securance conducted an external and semi-internal network and web-application security assessment for the Minnesota Bureau of Criminal Apprehension (BCA). The objective of the review was to identify technology-specific vulnerabilities and risks. The scope of the engagement included an assessment of the external network, the internal network and select web-applications.	**Minnesota State Bureau of Criminal Apprehension**
Information Systems Security Assessment	In 2015, Securance conducted an Information Systems Security Assessment for the County of Fresno. The objective of the engagement was to assess the security posture of the following: external network vulnerability assessment and penetration test; router configuration analysis; firewall configuration analysis; VPN security review; wireless network assessment; and web-application testing.	**County of Fresno, California**
IT Security Audits	In 2014, a Colorado state agency contracted with Securance to perform a risk-based vulnerability assessment, penetration test and technical information security assessment. The goal of the review was to determine if key technologies, networks and systems supporting the state government's operations were appropriately secured. We tested the security of networks, systems and infrastructure technologies managed by the agency. Our review included assessments of: external and internal network security; firewall configuration; enterprise application security and technical application controls; web-application security; and user security awareness.	**Client Name Confidential** *Colorado State Agency*
IT Security Assessment	In 2014, Securance conducted an external network and web-application security assessment for a regional international organization. Our goal was to identify technology-specific vulnerabilities and documented pathways to breaching network and web-application security. We used manual security audit techniques and scanning tools to perform blind vulnerability assessments of the external IP network and several web-applications.	**Client Name Confidential** *Regional International Organization*
Network Security Assessment	In 2013 and 2014, Securance conducted vulnerability assessments of a Toronto agency's external and internal networks and website. We applied our vulnerability assessment methodology, combining manual security audit techniques with commercial and proprietary tools, to scan the external and internal IP networks and website for technical vulnerabilities.	**Client Name Confidential** *Toronto Municipality*

5.2.2.2 Security, Privacy and Compliance

Our firm has offered application and network penetration testing services since its inception in 2002. Vulnerability assessments and penetration tests are among our specialties. As such, Securance understands the confidential nature of information technology security assessments. Our Senior IT Consultants have vast experience working in environments containing private and sensitive information, and we guarantee our consultants will keep such information confidential.

Securance Consulting only hires experienced IT audit and security professionals. We take great care in matching our consultants to engagements that suit their strengths and backgrounds, so that our customers receive the best possible service, while meeting their compliance and management objectives. Each member of every team has at least 15 years' experience, not merely in the services outlined in the project scope on pages 6-7, but, rather, in performing diverse assessments for government and industry leaders.

The team will consist of a combination of personnel with technical and business credentials, including CISA, CISSP, MCP, CPA, CEH, CFE, CIA, CISM and CITP. We understand the difference between "textbook" and real-world, practical security. Our consultants' experience will allow us to effectively strike the balance that is crucial to your organization and your IT security goals. Securance's proposed project team for this engagement is as follows:

Paul Ashe, President and Engagement Manager - CPA, CISA, CISSP
Paul, Founder and President of Securance Consulting, has provided hands-on project management to lead numerous engagements throughout the past 15 years. A former IT consultant for Ernst & Young, Paul has leveraged his knowledge and experience into an effective, time- and budget-conscious project management style. An experienced security consultant, he conducts vulnerability assessments and penetration tests of various systems and classes of IPs. Paul is proficient in network infrastructure and architecture reviews, physical security assessments, social engineering, policy reviews and more.

His recent application and network penetration projects include:

- City of Fort Collins, Colorado - Cyber Security Assessment
- Colorado Public Employees' Retirement Association - Network Security Assessment
- Dormitory Authority of the State of New York - External and Internal Vulnerability Assessment
- Franklin County, Ohio - IT Security and Vulnerability Assessment
- Illinois State Board of Education - IT Risk and Security Assessment
- Louisville-Jefferson County Metro Government - Vulnerability Assessment and Penetration Test
- Minnesota State Bureau of Criminal Apprehension - Security Vulnerability Assessment
- Minnesota State Retirement System - Vulnerability Assessment and Penetration Test
- New York City Housing Authority - External Network and Web-Application Security Assessment
- Ohio Public Employees' Retirement System - IT and Network Security Assessment

Please see his complete resume in Appendix A on pages i-ii.

Chris Bunn, Practice Director and Senior IT Security Consultant - CISA, CHP

Chris, Practice Director at Securance Consulting, is an expert in IT security, risk management and regulatory compliance, from best practice control frameworks to international, federal, state and industry-specific security regulations. With over 30 years of IT experience, Chris has audited information security, managed project teams and established successful risk assessment programs for global corporations, small- to medium-sized businesses and government entities. His expertise includes diverse systems, platforms, network architecture schemes and compliance requirements.

His recent application and network penetration projects include:

- Atlanta Housing Authority - IT Security Audit Services
- City of Fort Collins, Colorado - Cyber Security Assessment
- Colorado Office of the State Auditor - IT Security Audits
- Dormitory Authority of the State of New York - External and Internal Vulnerability Assessment
- Franklin County, Ohio- IT Security and Vulnerability Assessment
- Louisville-Jefferson County Metro Government - Application Security and Compliance Review
- Massachusetts Technology Collaborative - IT Security Audit
- Ohio Public Employees' Retirement System - IT and Network Security Assessment
- Waterfront Toronto - Vulnerability Assessment and Penetration Test

Please see his complete resume in Appendix A on pages iii-iv.

Chris Cook, Senior IT Security Consultant - CISSP, CISA

A Senior IT Consultant with over 20 years' experience, Chris helps public and private sector leaders identify threats, enhance controls, and make lasting improvements to their risk and security profiles. A subject matter expert in ISO 17799 l 27001 and NIST compliance, Chris has extensive experience with a variety of security frameworks, control standards and regulations, including CoBIT, GLBA, HIPAA, SOX and the PCI Data Security Standards. He has significant experience penetrating Internet-facing systems and web-applications; securing network infrastructure; and helping clients develop effective security policies, practices and monitoring procedures.

His recent application and network penetration projects include:

- City of Richmond, Virginia - Network Security Assessment
- City of Tacoma, Washington - Cyber Security Vulnerability Assessment
- County of Marin, California - Information Risk Assessment
- Educational Service Unit #3 - Network Security Audit
- Entergy Services Corporation - Penetration Security Assessment
- Hallmark Cards - Corporate VPN and Digital Website Vulnerability Assessments
- Kissimmee Utility Authority - Information Systems Risk Assessment and Network Security Review
- Orange County Sanitiation District - IT Security Assessment
- Santee Cooper - IT Security Assessment

Please see his complete resume in Appendix A on pages v-vi.

5.3 Section Three: Quality and Feasibility

5.3.1 Solution Provisioning Plan

Based on our understanding of the scope of requested services, Securance will execute the following activities:

A) External Network Vulnerability Assessment and Penetration Test

- Perform an External Network Vulnerability Assessment and Penetration Test:
  - Assess Internet presence:
    - Identify public IP space;
    - Identify all running services on each system, via comprehensive port scanning in stealth mode;
    - Identify all vulnerabilities on each device, system or server, running all tools in stealth mode;
    - Review results of initial scans with the City's personnel;
    - Perform penetration activities based on feedback from the City's Project Manager; and
    - Review results with the City's Project Management.

    (See detailed methodology in Appendix B on pages vii-xi.)

B) Internal Network Vulnerability Assessment and Penetration Test

- Perform an Internal Network Vulnerability Assessment and Penetration Test:
  - Identify internal network segment in scope for testing;
  - Identify all running services on each system via comprehensive port scanning in stealth mode;
  - Identify all vulnerabilities on each device, system or server, running all tools in stealth mode;
  - Review results of initial scans with the City's personnel;
  - Perform penetration activities based on feedback from the City's Project Manager; and
  - Review results with the City's Project Management.

  (See detailed methodology in Appendix B on pages xii-xvi.)

C) Web-Application Testing

- Perform Unprivileged and Privileged Web-Application Testing:
  - Perform unprivileged web-application testing (i.e., testing the web-application without login information):
    - Identify web-applications;
    - Assess hosting server and associated web server's configurations;
    - Perform unprivileged web-application vulnerability testing; and
    - Pending testing and authorization, attempt to modify application content.
  - Perform privileged web-application testing (i.e., testing the web-application with client-provided authentication information):
    - Identify web-applications;
    - Assess hosting server and associated web server's configurations;
    - Perform privileged web-application vulnerability and configuration testing; and
    - Pending testing and authorization, attempt to modify application content.

    (See detailed methodology in Appendix B on pages xvii-xviii.)

D) Prepare Deliverables

- Management Report, Including:
  - Executive summary;
  - Introduction and scope;
  - Approach and methodology; and
  - Findings (with associated risk rankings) and actionable recommendations.
- Technician's Report:
  - Raw data extracts from utilized security tools.

  (See sample reports in Appendix C.)

Project Management Approach

Each project we undertake will follow this standard accountability model.

Engagement Manager

- Ensure the appropriate team is assembled for each project.
- Initial point of contact for the City's Management Team.
- Ensure engagement is performed in a timely way and without any issues.
- Resolve any issues that may arise.
- Deliver and review project reports.

Senior IT Security Consultants

- Draft detailed security procedures.
- Lead the execution of the procedures.
- Prepare workpapers that meet the reperformance standard.
- Identify vulnerabilities and exposures.
- Prepare periodic status reports and review with the City's Project Manager.
- Notify the Engagement Manager of any potential project issues or concerns.
- Draft security reports.

Independent Reviewer

- Perform an independent review of the project and report to ensure they meet our firm's Quality Standards.

The City's Project Manager

- Coordinate meetings between Securance and the City's staff.
- Join project interview meetings as considered necessary or desired.
- Review periodic status reports and discuss any concerns with Engagement Manager.
- Provide Securance with guidance relative to the City's mode of operations.
- Review vulnerabilities to obtain a clear understanding of the risks and recommendations.

Status Reports

- Depending on the size of a project, we issue weekly or biweekly status reports. These reports are designed to capture and communicate the following information about an ongoing project:
  - Budget to actual hours and projected hours to complete project;
  - Project issues or risks that may hinder project completion;
  - Change control items (typically only applicable if the scope changes);
  - Project milestone status;
  - Upcoming activities; and
  - Summary of any potential findings.

Safeguards to Protect the City's IT Assets, Including eCommunications

- All Securance consultants will execute a confidentiality agreement.
- All Securance consultants will perform their activities on a company-issued workstation. The workstation will be configured using whole disk encryption; local firewalls will be enabled; and the anti-virus solution will be current.
- This full-disk encryption software will protect data from unauthorized access, providing strong security for intellectual property, customer and partner data.
- It will often be essential that sensitive information be shared between Securance and the City. In these situations, our team will adhere to the following standards:
  - Any sensitive information shared via email must be encrypted.
  - Any reports containing sensitive information must be encrypted and password-protected.
  - All passwords used will meet or exceed standard complex password standards.
  - Any passwords that need to be communicated will be communicated via telephone or under separate email cover.
- Any hardcopy documents containing sensitive information will be shredded upon completion of the engagement.
- Engagement information will be shared only with the Engagement Team.
- At the conclusion of the engagement, all electronic data will be permanently deleted from all consultants' workstations. All engagement workpapers will be digitized, encrypted and stored on a secure file server. The City's Project Manager may direct Securance to destroy all workpapers after an electronic copy has been delivered to the designated personnel.

Workpaper Security Standards

- All working papers are maintained electronically on our secured drive for a period of three years.
- All data on the Securance network is regularly backed up, archived and securely stored according to best practice standards.
- All working papers obtained from clients are considered confidential and treated as such. Securance does not provide any working papers to any third parties without explicit written permission from the client.
- Any data obtained for the performance of the review that is classified as "sensitive" is either reviewed on site or disposed of via best practice standards at the completion of the review; Securance does not retain sensitive client information.
- Upon engagement, Securance will also discuss any further data retention standards required by our clients.

Procedures to Ensure No Disruption to IT Systems

- All vulnerability assessments and penetration testing will be performed after normal business hours or at a time requested by the City's IT personnel.
- All vulnerability assessments and penetration testing will be **performed using a policy that ensures no disruption to the network**. If more aggressive scanning procedures need to be performed, they will only be performed after we obtain explicit approval from the City's Project Manager.
- All procedures with the potential to be disruptive will be performed using manual techniques and at a guarded pace. During the performance of these procedures, IT Management will be asked to monitor network and system performance and to notify Securance consultants if performance becomes unacceptable. In the unlikely event of network or system disruption, the active procedures will be terminated.
- Securance will not attempt exploitation of mission-critical systems or resources without explicit written permission from the City's Project Manager.
- Securance will log all actions, including changes to system settings and configurations, taken against compromised systems. After completing our penetration testing procedures, we will restore all settings and configurations to their initial values.

Quality Assurance Process

All projects are led by Senior IT Audit and Security Consultants with a minimum of 15 years' experience. Their work is reviewed by the Engagement Manager, and the final product is reviewed by an executive independent of the project. Additionally, our service level commitment to our clients is as follows:

- Our work product will meet or exceed the requirements of our client's internal standards.
- We ask you to measure our quality based on the comprehensiveness and quality of our reports.
- We ask our clients to complete a satisfaction survey.

Independence Assurance Process

Securance Consulting adheres to the principle guidelines outlined in the Institute of Internal Audit Practice Standards. Our Management Team ensures that the firm maintains independence and objectivity on each project. Our staff is required to maintain select certifications; this requirement ensures independence, proficiency and due care.

Assumptions We Have made

- Securance consultants will have full access to all client participants and personnel, as required, throughout the duration of the engagement.
- The City's personnel will provide Securance consultants with all information requested to complete this engagement in a timely manner.
- The City's Project Manager will hold meetings with the Securance Engagement Manager, as necessary, to assess the project's progress.
- The City's Management will be responsible for all remediation of identified vulnerabilities and risks.

Logistic Requirements

- Securance consultants will need adequate workspace and Internet connections while on site to access email and other firm resources.
- Securance consultants will need access to a dedicated phone extension and printing capabilities.

Estimated Hours

Securance estimates the project requires 220 hours of work.

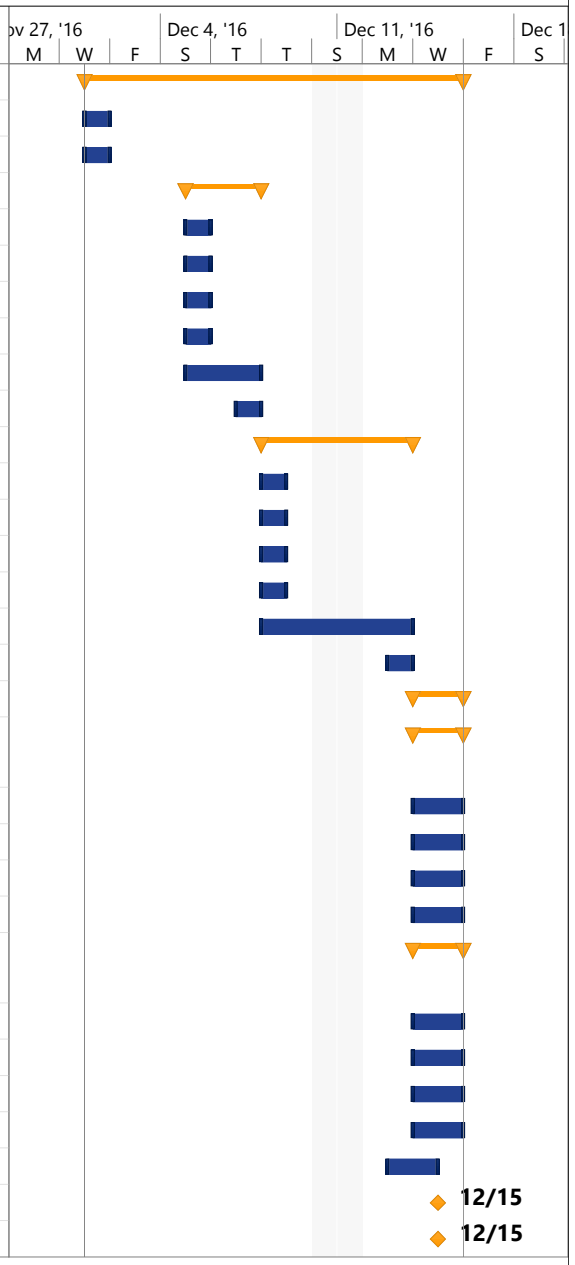
Proposed Project Plan

On the following page, we provide a detailed project plan based on our understanding of the scope of requested services. The Gantt chart outlines each step in our assessment process, designating major tasks, subtasks and key milestones.

The Gantt chart shows how our assessment will progress from start to finish. The target start and end dates are not fixed. We are flexible with respect to when we start this project. We look forward to working with the City's stakeholders to determine the best possible start date and finalize the assessment timeline.

City of Columbus
Proposed Project Plan

Task Name	Start	Finish
The City Project Plan	**Thu 12/1/16**	**Thu 12/15/16**
Introduce Team to Client	Thu 12/1/16	Thu 12/1/16
Review Client Assistance Request	Thu 12/1/16	Thu 12/1/16
Perform an External Network Vulnerability Assessment and Penetration Test	Mon 12/5/16	Wed 12/7/16
Identify Public IP Space	Mon 12/5/16	Mon 12/5/16
Identify All Running Services on Each System via Comprehensive Port Scanning in Stealth Mode	Mon 12/5/16	Mon 12/5/16
Identify All Vulnerabilities on each Device, System or Server Running All Tools in Stealth Mode	Mon 12/5/16	Mon 12/5/16
Review Results of Initial Scans with the City's Personnel	Mon 12/5/16	Mon 12/5/16
Perform Penetration Activities Based on Feedback from the City's Project Manager	Mon 12/5/16	Wed 12/7/16
Review Results with the City's Project Management	Wed 12/7/16	Wed 12/7/16
Perform an Internal Network Vulnerability Assessment and Penetration Test	Thu 12/8/16	Tue 12/13/16
Identify Internal Network Segment in Scope for Testing	Thu 12/8/16	Thu 12/8/16
Identify All Running Services on Each System via Comprehensive Port Scanning in Stealth Mode	Thu 12/8/16	Thu 12/8/16
Identify All Vulnerabilities on each Device, System or Server Running All Tools in Stealth Mode	Thu 12/8/16	Thu 12/8/16
Review Results of Initial Scans with the City's Personnel	Thu 12/8/16	Thu 12/8/16
Perform Penetration Activities Based on Feedback from the City's Project Manager	Thu 12/8/16	Tue 12/13/16
Review Results with the City's Project Management	Tue 12/13/16	Tue 12/13/16
Perform Unprivileged and Privileged Web-Application Testing	Wed 12/14/16	Thu 12/15/16
Perform unprivileged web-application testing (i.e. testing the web-application without login information)	Wed 12/14/16	Thu 12/15/16
Identify web-applications	Wed 12/14/16	Thu 12/15/16
Assess hosting server and associated web server's configurations	Wed 12/14/16	Thu 12/15/16
Perform unprivileged web-application vulnerability testing	Wed 12/14/16	Thu 12/15/16
Pending testing and authorization, attempt to modify application content	Wed 12/14/16	Thu 12/15/16
Perform privileged web-application testing (i.e. testing the web-application with client-provided authentication information)	Wed 12/14/16	Thu 12/15/16
Identify web-applications	Wed 12/14/16	Thu 12/15/16
Assess hosting server and associated web server's configurations	Wed 12/14/16	Thu 12/15/16
Perform privileged web-application vulnerability and configuration testing	Wed 12/14/16	Thu 12/15/16
Pending testing and authorization, attempt to modify application content	Wed 12/14/16	Thu 12/15/16
Reporting	Tue 12/13/16	Wed 12/14/16
Review Reports	Thu 12/15/16	Thu 12/15/16
Exit Conference	Thu 12/15/16	Thu 12/15/16



Milestone | Project Summary | Manual Task | Manual Summary

5.3.2 Satisfaction of Requirements

As described in the Proposed Scope on pages 6-7, our proposed solution will meet the City's objectives outlined in section 2 of the RFP. Please see below in regards to the requirements listed in section 3.

3.1.1 Term
As stated in the RFP, if selected to provide the requested services, the contract between Securance and the City will be active for one (1) year from the date of the purchase order.

3.1.2 Pricing
Securance proposes an hourly rate of $135 for this project. The hourly rate applies to all work efforts, regardless of type or complexity, and to all staff, regardless of title, skills or experience level; it is inclusive of all costs and expenses. Please refer to 5.6 Section 6: Cost and Payment Terms (on page 16) for itemized pricing.

3.1.3 Geographic Location
Our Senior IT Consultants will perform all external assessments and reporting remotely at our headquarters in Tampa, Florida. All internal assessments will be performed on-site in Columbus, Ohio.

3.1.4 Work Hours
All assessments will be performed at a time requested by the City's IT personnel. Securance's project manager and consultants can be reached during normal business hours via phone or email Monday to Friday from 8:30 a.m. to 5:30 p.m.(EST).

3.1.5 Supplier Personnel
Securance conducts the following background checks on all professional and administrative staff:

- Credit worthiness;
- Criminal felony and misdemeanor (unlimited);
- Employment history; and
- Citizenship verification.

Upon request, we will conduct any additional check(s) not listed above. If necessary, we will provide proof that a background check has been performed for each Securance employee.

Use of Subcontractors
Securance will not subcontract any of the work associated with RFQ003002 Application and Network Penetration Testing Services.

3.2.1 Relevant Experience
Please refer to section 5.2.2.1 Similar Engagements on page 3 for Securance's relevant experience within the past three years.

3.3.2 Experienced Staff
Each member of Securance's proposed project team has over 15 years experience and has performed multiple application and network penetration tests. Please refer to their resumes in Appendix A on pages i-vi.

3.2.3 References
Please refer to 5.5 Section Five: Past Performance on page 15 for previous client references.

3.2.4 City of Columbus Contract Compliance
Securance will obtain a valid City of Columbus contract compliance number upon award.

5.4 Section Four: Ability

5.4.1 Workload

We are currently engaged on a number of client projects. We attempt to keep our workload commensurate with our staff. However, we believe the best way to measure our ability to complete task orders on time is through discussion with our current clients (see client references on page 15).

We guarantee that we will:

- Properly staff each project with employees that are qualified and technical experts;
- Begin all task orders on time;
- Complete them within budget, within the required time frame; and
- Deliver a draft report within one (1) week of fieldwork completion.

Certification of Key Personnel

Securance certifies that all key personnel will be employed by Securance as full-time employees and will not be removed from the City's account without prior written notice and the approval of the City's Project Manager. If any key personnel resign from Securance or leave the employment of the firm, the City will be notified within five (5) business days of such separation.

In addition, Securance will provide a replacement of equal or better experience and credentials. The City will review and approve all replacement resources.

5.4.2 Financial Responsibility

As a privately held firm, Securance does not engage a third party to perform an independent review of its financial statements. Securance enjoys a strong financial position. Over the past three years, our revenues have remained high. Please refer below for financial statement summaries covering the three most recent fiscal years.

SECURANCE LLC - FINANCIAL STATEMENTS

INCOME STATEMENT

	Jan - Dec 15	Jan - Dec 14	Jan - Dec 13
Revenue	$ 1,418,900.05	1,468,012.47	1,408,596.50
Cost of Goods Sold	$ 613,628.82	708,629.45	803,047.74
Gross Profit	$ 805,271.23	759,383.02	605,548.76
G&A Expenses			
Office Personnel Expenses	$ 396,667.24	323,776.40	257,149.66
Other G&A Expenses	$ 279,941.41	214,538.70	233,223.99
Total Expense	$ 676,608.65	538,315.10	490,373.65
Net Ordinary Income	128,662.58	221,067.92	115,175.11

BALANCE SHEET

	Jan - Dec 15	Dec 31, 14	Dec 31, 13
ASSETS			
Total Current Assets	$ 83,299.45	124,071.56	103,711.71
Total Fixed Assets	$ 2,607.53	4,866.85	8,667.34
Total Other Assets	$ 600.00	600.00	600.00
TOTAL ASSETS	$ 86,506.98	129,538.41	112,979.05
LIABILITIES & EQUITY			
Liabilities			
Total Current Liabilities	$ 29,844.62	15,804.45	28,325.35
Total Long Term Liabilities	$ 79,033.24	87,586.54	101,956.62
Total Liabilities	$ 108,877.86	103,390.99	130,281.97
Total Equity	$ (22,370.88)	26,147.42	(17,302.92)
TOTAL LIABILITIES & EQUITY	$ 86,506.98	129,538.41	112,979.05

5.5 Section Five: Past Performance

Selected Client References

The following client references were selected because the services provided by Securance Consulting resemble those that you have requested. We invite you to talk with our clients to confirm the quality and added value of the services we provided.

Franklin County, Ohio

373 S. High Street, 9th Floor, Columbus, OH 43215

Julie Lust, Director - Financial Services
Direct: (614) 525-5826 l email: jalust@franklincountyohio.gov l www.franklincountyohio.gov

Project: IT Security and Vulnerability Assessment **Project Cost:** $78,368

Project Scope: In 2016, Securance conducted an information technology security assessment for Franklin County Data Center (FCDC). The objective of the review was to assess the current state of information system security. The scope of the review included: IT process risk assessment; external network vulnerability assessment; internal network vulnerability assessment; intrusion prevention system review; firewall configuration analysis; router l switch configuration analysis; enterprise application security assessment; active directory assessment; database security assessment; web-application testing; wireless network testing; HIPAA Security and Privacy Rule compliance; and Payment Card Industry (PCI) readiness assessment.

Ohio Public Employees' Retirement System

277 East Town Street - Columbus, OH 43215-4642

Mr. Dave McKnight, IT Auditor
Direct: (614) 222-0088 l email: dmcknight@opers.org l www.opers.org

Project: Network and IT Security Assessment **Project Cost:** $30,910

Project Scope: In 2014, Securance performed an IT and network security assessment for Ohio Public Employees' Retirement System (OPERS). Our goal was to evaluate the security of the fund's external network, internal network, web-applications and mainframe computing environment by conducting targeted vulnerability testing procedures. We used commercial and proprietary scanning tools, together with manual audit techniques, to identify technology-specific vulnerabilities affecting networks and systems. Then, we developed remediation recommendations to address weaknesses in the IT security infrastructure.

New York City Housing Authority

90 Church Street - New York, NY 10007

Mr. Jeff Benson, Chief IT Auditor
Direct: (212) 306-8070 l email: jeff.benson@nycha.nyc.gov l www.nyc.gov/nycha

Project: External Network and Web-Application Assessment **Project Cost:** $5,120

Project Scope: In 2014, New York City Housing Authority (NYCHA) contracted with Securance to perform a technical security assessment of its external network and 12 web-applications. We used automated tools and manual audit techniques to identify technology-specific vulnerabilities and avenues of attack that a hacker could exploit to access personally identifiable information and sensitive data.

5.6 Section Six:
Cost and Payment Terms

5.6.1 Cost

As a market leader in providing technology risk consulting services, we offer a full range of service options to meet our clients' needs. We continually invest in the development of our risk consulting services -- people, process, technology and knowledge -- in order to deliver outstanding service to our clients.

Securance Consulting is a firm of Senior IT Audit and Security Consultants, which simplifies our fee structure. Our all inclusive hourly rate for all our services and seasoned consultants is $135. **Securance will absorb 100 percent of travel expenses associated with this engagement.**

Project Scope Item	Line Item Fee
External Network Vulnerability Assessment and Penetration Test	$8,950
Internal Network Vulnerability Assessment and Penetration Test	$13,450
Web-Application Assessment ***(price for 1 application)***	$5,175
Reporting	$2,048
Administrative Fee*	$878
Total	**$30,501**

Ask about Our Price Match Guarantee!

*Administrative Fee is 5% of billable hours at a rate of $80.00 per hour. This is a fee added to all engagements to cover back office costs related to the project such as printing materials, deliverables, shipping, copies, and archives of workpapers.

This fee estimate is based on our understanding of the activities required to successfully complete this engagement. We believe that our fee estimate is competitive for these services. Often in a proposal situation, we find that most of the differences in fee quotations relate to variations in scope of work. If you find this to be the situation here, we would be glad to discuss our understanding of the scope and preliminary work plan with you so that you can make an "apples-to-apples" comparison of the proposals.

Should any material changes in scope occur or unforeseen situations arise, Securance will first determine their potential impact on the project, project approach, schedule and professional fees, then present any changes to the City for discussion and consideration. The Engagement Manager will review the status and any changes to these estimates as necessary from time to time during the course of this engagement. Securance will submit an invoice after the initial Management Report draft has been delivered. The final Management Report will be delivered upon processing of invoice.

5.6.2 Payment Terms

Securance's policy is payment is due when a draft management report is delivered.

Appendix A

Paul Ashe, CPA, CISA, CISSP

President and Senior IT Security Consultant

Senior Executive Professional. 15 years' diverse IT experience.
Extraordinary cross-functional management background.
Focused on protecting information for major corporations
and other organizations requiring high security.

Overview

Paul Ashe, President of Securance Consulting, has a proven track record of success delivering profit-driven technology solutions and minimizing technology-related risk to top organizations. Over the course of his career, he has taken charge of risk management engagements throughout the public and private sectors - and, in so doing, has established Securance as a leader in the IT field. Paul is an expert in:

- Security Operations
- Systems Engineering
- Risk Assessments
- Research
- Business Governance
- Security Management

Experience: IT Security

Paul has been the lead security professional on numerous attack and penetration engagements. He has significant experience breaching MS Windows and UNIX platforms and perimeter security devices and is proficient in the use of over 75 security tools. His functional experience includes:

- Security Infrastructure Management
- Security Auditing
- Business Impact Assessment
- Risk and Threat Analysis
- Vulnerability Assessments
- Penetration Testing
- VPN Solutions
- IDS Deployment
- SLA and Vendor Management
- Incident Response
- "Best Practice" Deployment
- Software Functionality Reviews
- Physical Security Management
- Web-Application Testing
- Mobile Device Reviews
- Social Engineering
- Secure Network and DMZ Architecture Development

Paul has formulated security policies and procedures to address areas that include:

- Incident Management
- Technical Vulnerability Control
- Patch and Vulnerability Management
- Equipment Security
- Roles and Responsibilities
- Data Destruction
- Firewall Security
- Mobile Device Management

Experience: Project-Specific

Paul works closely with leaders in the government sector to help them improve their security postures and to ensure that best practice controls are used to mitigate known security threats. Recent projects include:

- City of Bowling Green, Kentucky - IT Security and General Controls Audit
- City of Chattanooga, Tennessee - Vulnerability Assessment
- City of Florence, South Carolina - IT Security Audits
- City of Fort Collins, Colorado - Cyber Security Assessment
- City of Grants Pass, Oregon - Network Security Assessment
- City of Madison, Wisconsin - Network Security Assessment
- City of Milwaukee, Wisconsin - External and Internal Vulnerability Assessment
- City of Richmond, Virginia - Network Security Assessment
- City of Tacoma, Washington - Cyber Security Assessment
- City of Thornton, Colorado - Security Assessment
- Colorado Public Employees' Retirement Association - Network Security Assessment
- County of Fresno, California - Information Systems Security Assessment
- Dormitory Authority of the State of New York - External and Internal Vulnerability Assessment
- Franklin County, Ohio - IT Security and Vulnerability Assessment
- Henrico County, Virginia - Network Vulnerability Assessment and PCI Readiness Assessment
- Housing Authority of the City of San Buenaventura - IT Security Assessments
- Illinois State Board of Education - IT Risk and Security Assessment
- Louisville-Jefferson County Metro Government - Vulnerability Assessment and Penetration Test
- Maryland National Capital Park and Planning Commission - Network Vulnerability Assessment
- Minnesota State Bureau of Criminal Apprehension - Security Vulnerability Assessment
- Minnesota State Retirement System - Vulnerability Assessment and Penetration Test
- New York City Housing Authority - External Network and Web-Application Security Assessment
- Ohio Public Employees' Retirement System - IT and Network Security Assessment
- Organization of American States - External Network and Web-Application Security Assessment
- Pinellas County, Florida - IT Security Assessment with PCI Readiness Assessment
- Waterfront Toronto - Network Security Assessment

Technological Skills

- Platforms - MS Windows; UNIX (SCO, HP-UX, Solaris, Linux, AIX); OS/400; RS/600; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions - MS SQL; MySQL; DB2; SAP; Lawson; MYOB; Oracle; PeopleSoft; JDE; Dynamics; and industry-specific solutions.
- Security Tools - Commercially available and Open-Source tools.

Education, Training and Certifications

- Certified Information Systems Auditor
- Certified Public Accountant (Florida)
- Certified Information Systems Security Professional
- SANS Firewall, Perimeter Protection and Security Training
- Bachelor of Science - Accounting and Management Information Systems (Dual Degree)
- Master of Science - Accounting Information Systems

Chris Bunn, CISA, CHP

Practice Director and Senior IT Security Consultant

Practice Director and Senior IT Consultant.
30-plus years' experience in IT security, risk management
best practice implementation and regulatory compliance.

Overview

Chris Bunn, Practice Director at Securance Consulting, is a Senior Management Professional and Certified Information Systems Auditor with over 30 years' experience in the IT field. An expert in IT security, risk management and regulatory compliance, he has delivered successful, efficient IT solutions to clients in a broad range of industries.

Experience: IT Risk Management

Experis Finance – Risk Advisory Services Senior Consultant

- Responsible for the execution of Sarbanes-Oxley (SOX 404) compliance audits for clients in the banking, manufacturing, healthcare and energy industries. Clients included Bank of America, Dycom Industries and Sempra Energy.
- Completed ISO 27002 compliance, VMware security, Six Sigma and HIPAA compliance audits for Cedars-Sinai Medical Center.
- Performed General Computing Control Audits (GC^2R) utilizing COSO and CoBIT audit frameworks.
- Performed segregation of duties reviews, ITIL Service Management (ITSM) V3 evaluations, architecture reviews, business intelligence, IT governance and other information system audits.

University of Florida – IT Audit Manager

- Planned, supervised, and conducted audits of PeopleSoft 8 ERP and Data Warehouse and reporting systems residing on Unix AIX platform; financial systems; and information security operations.
- Supervised and performed audits of computer systems residing on a variety of hardware platforms.
- Managed HIPAA compliance audits for Shands Hospital.
- Implemented Paisley (Thomson Reuters) Enterprise GRC tool and AutoAudit for Windows to streamline risk management processes within the Internal Audit Division.

BDO Seidman LLP – IT Audit Manager

- Delivered SAP BI and GRC advisory services for mySAP ERP with NetWeaver, Oracle's PeopleSoft enterprise applications, and other SOA ERP systems.
- Responsible for business development and project management in technology risk and security, business process improvement, business intelligence and advanced analytics, SOX 404 and JSOX compliance, FISMA compliance, IFRS transition and IT compliance, service organization (SAS70 Type II) and internal audit service lines.

Experience: Project-Specific

Together with Engagement Manager Paul Ashe, Chris helps top organizations improve their risk profiles and establish best practice controls. His recent projects include:

- Atlanta Housing Authority - IT Security Audit Services
- Capital City Bank Group - Security Framework Testing
- Cedar Falls Utilities - Network Security Risk Assessment
- Central New Mexico Electric Cooperative - IT Security Assessment
- City of Aurora, Colorado - SCADA System Vulnerability Assessment
- City of Fort Collins, Colorado - Cyber Security Assessment and NIST 800-53 Gap Analysis of Water Resources and Treatment Industrial Control Systems
- Colorado Office of the State Auditor - IT Security Audits
- Community Coffee Company - Penetration Test
- County of Marin, California - Information Risk Assessment and Compliance Audit
- Dormitory Authority of the State of New York - External and Internal Vulnerability Assessment
- First Financial Bank - IT Security Assessment
- Franklin County, Ohio- IT Security Assessment, HIPAA Compliance Assessment, and PCI Readiness Assessment
- Hallmark Cards - IT Security Assessment
- Kitsap County, Washington - HIPAA Security Assessment
- Liberty Savings Bank - IT Security Assessment
- Louisville-Jefferson County Metro Government - Application Security and Compliance Review
- Massachusetts Technology Collaborative - IT Security Audit
- Northern Kentucky University - Security Audit
- Pioneer Electric Cooperative - IT Security Assessment and PCI SAQ Review
- Ohio Public Employees' Retirement System - IT and Network Security Assessment
- Oil States International - Application Security Audits
- Orange County, Florida - HIPAA | HITECH Security Assessment
- Pinellas County, Florida - IT Security Assessment
- United Community Bank - Network Security Assessments
- Waterfront Toronto - Vulnerability Assessment and Penetration Test
- Western and Southern Financial Group - Vulnerability Assessment and Penetration Test

Technical Skills

- Platforms - MS Windows; UNIX; OS/400; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions – MS SQL; Oracle, DB2; MySQL; SAP; Oracle; PeopleSoft; Lawson; JDE; Dynamics; and industry-specific.
- Security Tools - Commercially available and open-source tools.

Education, Training and Certifications

- Certified Information Systems Auditor
- Certified HIPAA Professional
- Master of Science - Management Information Systems
- Bachelor of Science - Computer Science for Business

Chris Cook, CISSP, CISA

Sr. IT Security Consultant

Senior IT Security Consultant with 20-plus years' diverse IT experience.
Significant expertise with NIST, ISO and other
regulatory compliance frameworks.

Overview

Chris Cook, a Senior IT Consultant with Securance for the last 9 years, has remarkable experience in IT security, risk analysis and regulatory compliance. His expertise includes:

- Security Evaluations
- Risk Assessments
- Vulnerability Assessments
- Penetration Tests
- UNIX l Linux and Windows Server Reviews
- Internet Security Assessments
- Application Vulnerability Assessments
- Regulatory Compliance Reviews and Testing
- NIST, ISO, PCI, HIPAA and SOX Compliance

Experience: IT Security

Ericsson - Senior Security Analyst

- Assessed application security. Formulated actionable recommendations for remediation of identified risks and vulnerabilities.

NASA Ames Research Center - Senior Control Analyst

- Prepared FISMA certification and accreditation packages according to NIST guidelines.
- Packages included risk assessments, security plans and contingency plans.

BlueCross BlueShield of Kansas City - Project Manager, CoBIT Controls Assessment

- Developed project to assess CoBIT controls for Model Audit Rule (MAR) compliance.
- Assessed corporate policy infrastructure.

IBM - Managing Consultant, Security and Privacy Practices

- Conducted security evaluations according to ISO and NIST standards.
- Performed application vulnerability assessments using WebInspect software.
- Reviewed internal clients' practices for compliance; recommended appropriate solutions

Honeywell FM&T - Senior Security Engineer

- Created a series of automated vulnerability scanning programs that scanned network devices and collected results in a database.
- Developed and delivered in-house IT security training programs.

Experience: Project-Specific

Chris works closely with Engagement Manager Paul Ashe to help top organizations improve their security postures and to ensure that best practice controls are used to mitigate known threats. Recent projects include:

- City of Richmond, Virginia - Network Security Assessment
- City of Tacoma, Washington - Cyber Security Vulnerability Assessment
- County of Marin, California - Information Risk Assessment and Compliance Audit
- Educational Service Unit #3 - Network Security Audit
- Entergy Services Corporation - Penetration Security Assessment
- First Financial Bank - IT Security Assessment
- Hallmark Cards - Corporate VPN and Digital Website Vulnerability Assessments
- Inter-American Development Bank - Extended Enterprise Mobility Security Assessment
- Kissimmee Utility Authority - Information Systems Risk Assessment and Network Security Review
- Liberty Savings Bank - IT Security Assessment
- Newtown Savings Bank - Network Vulnerability Assessment
- Orange County Sanitiation District - IT Security Assessment
- Santee Cooper - IT Security Assessment
- Transocean - Penetration Test

Technical Skills

- Platforms - MS Windows; UNIX (SCO, HP-UX, Solaris, Linux, AIX); OS/400; RS/600; RACF; and ACF2.
- Tools - ACL; PhoneSweep; ToneLoc; Monarch; eWorkpaper; and application audit tools.
- Database and ERP Solutions - MS SQL; MySQL; DB2; SAP; Lawson; MYOB; Oracle; PeopleSoft; JDE; Dynamics; and industry-specific solutions.
- Security Tools - Commercially available and open-source tools.

Education, Training and Certifications

- Certified Information Systems Security Professional
- Certified Information Systems Auditor
- SOA Fundamentals and Security
- SANS Track 4 - Hacker Techniques, Exploits and Incident Handling
- SANS Track 6 - Securing UNIX l Linux
- SANS Track 12 - SANS Security Leadership Essential
- SANS Securing Solaris Using the Center for Internet Security Benchmarks
- SANS Track 7 Auditing Networks, Perimeters and Systems
- Department of Energy Cyber Security Training and Basic Security Survey
- Network Associates Sniffer University
- Bachelor of Science – History

Appendix B

Approach and Methodology

External Network Vulnerability Assessment and Penetration Test

Securance Consulting executes a rigorous rules-of-engagement methodology when performing penetration testing services. Testing, even black box-style testing, is never commenced without prior written authorization. We work closely with our clients' internal resources to ensure that the appropriate personnel designate the proper time windows for testing, which can be during business or non-business hours. Our goal is to work with clients to provide them with the most realistic real-world attack possible without any disruption to their daily operations.

Securance Consulting will utilize a combination of industry-leading techniques during this engagement, including the National Institute of Standards and Technology (NIST) Special Publications 800-115 (Technical Guide to Information Security Testing and Assessment), ISO 27000 series, Open Web Application Security Project (OWASP), Information Systems Security Assessment Framework (ISSAF) and Open-Source Security Testing Methodology Manual (OSSTMM).

Our methodology includes:

A) Information Gathering l Footprinting

- Search for public information about the target.
- Search for information about and develop a map of the internal network structure systems or business-critical applications.
- Identify security holes and weaknesses in the implementation process.

B) Planning the Attack

- Business resources
- Domain name resources
- Whois database:
  - NSLookup, ARIN and DIG
- Social engineering techniques and guessing
- Brute force attempts

C) Vulnerability Testing

- Analyze information gathered.
- Evaluate company profile.
- Plan the penetration.
- Identify modes of access.
- Locate trust hosts.
- Identify sensitive data flows.
- Document network topology, including:
  - DMZ, extranets, portals, VPN terminations and remote access points.
- Perform scans using various tools and cross-reference available services against a comprehensive listing of vulnerability databases, such as: Security Focus, Microsoft Security Bulletins, Common Vulnerability Database (OSVDB), United States Computer Emergency Response Team (USCERT), SANS, Securiteam, PacketStorm Security, Security Tracker, Secunia, Bugtraq, etc.

C) Vulnerability Testing *(continued)*

- The Securance Consulting vulnerability assessment and penetration test performs a series of checks to discover methods to breach your systems. Here is a summary list of checks we include in our methodology:
  - Buffer Overflows
  - Bypass Authentication
  - Info from Case Studies, Presentations
  - Command Injection
  - Cross Site Request Forgery
  - Cross Site Scripting
  - Cross Site Tracing
  - Database Scan
  - Default Passwords
  - Directory Traversal
  - Info from DNS Records
  - Fire Walking
  - Firewall Vulnerability Detection
  - Hard Coded Secrets
  - HTML Source Code Analysis
  - Integer Overflows
  - Info from Job Postings
  - LDAP Injection
  - Info from Mailing Lists
  - Open Relay Scan
  - OS Fingerprinting
  - Password Cracking
  - Password Guessing
  - Ping Sweep
  - Port Scanning
  - Info from Press Releases, Newsletters
  - Info from Publicly Available Resumes
  - Router Vulnerability Detection
  - Look for Sensitive Error Messages
  - Server I Service Fingerprinting
  - Session ID Prediction
  - SNMP Scan
  - SQL Injection
  - SSL Configuration
  - Info from Trade Publications
  - Validate Cryptographic Strength
  - Vulnerable Sample Applications
  - Web Server Vulnerability Scan
  - Info from WHOIS Records
  - XPATH Injection

- Our testing techniques scale from soft to aggressive. Below are examples of soft and aggressive techniques we will utilize:
  - Soft techniques include:
    - Simple port scanning to identify listening ports;
    - Default password identification;
    - Observation-based social engineering; and
    - "Safe check" vulnerability scanning.
  - Aggressive techniques include:
    - Brute force password attacks;
    - Multi-location network sniffing;
    - Hard-sell social engineering;
    - Applying a denial of service attack; and
    - Aggressive vulnerability scanning.

These examples complement each other in that soft techniques typically precede aggressive techniques. In world-class security organizations, soft techniques are often used to alert system administrators when aggressive techniques are being run against the network or system.

D) False Positives

- Our staff has extensive experience performing vulnerability scans and penetration tests. The following methods will be used to identify false positives.
- The tools used will be configured specifically to the network device or system being tested.
- Our staff is highly experienced. The team will rely on the experience of the SME to identify vulnerabilities that are false.
- Pending client approval, we will execute select exploits to confirm certain vulnerabilities.
- Exploit vulnerabilities and leave a trophy; and
- Prior to reporting, we will validate our technical findings with IT Management.

E) Reporting and Summarizing

- Executive Summary
- Technician's Report

Vulnerability Management and Reporting

Our deliverable includes a Technician's Report. This report identifies true vulnerabilities and provides a proven step-by-step method for mitigating the vulnerability. In addition, we provide real-world examples of the risk being assumed by an organization if it elects not to mitigate a proven vulnerability. The risk associated with each vulnerability varies. As such, unless true vulnerabilities are identified, we do not provide specific real-world examples of the business risk to an organization.

Standard Software Tools

The following is a list of the tools we will most likely utilize during the performance of parts of this engagement. Please note that the specific tool(s) used will be dictated by the specific technology being assessed.

In order to assess network components, servers and databases, we utilize "best in-class" automated tools in conjunction with our manual procedures. A short list of the tools we may use is as follows:

- ❋ **NMAP Scanner -** a comprehensive port scanner used to identify a host status and listening ports and to fingerprint an operating system.
- ❋ **NESSUS Scanner -** a comprehensive network vulnerability assessment tool for measuring system risks. Nessus is used to probe systems and report vulnerabilities that might create an exposure.
- ❖ **GFI LANguard** - a network security scanner designed specifically for Windows.
- ❋ **Netcat -** a simple UNIX utility which reads and writes data across network connections, using TCP or UDP protocol.
- ❖ **AppDetective** - a commercially licensed database-specific vulnerability and penetration testing tool.
- ❖ **SolarWinds** - a powerful combination of network discovery, monitoring and attack tools.
- ❋ **Metasploit Framework** - an advanced open-source platform for developing, testing and using exploit code.
- ❋ **Wireshark** - a network sniffer and TCP I IP analysis tool.
- ❖ **WebInspect -** an automated scanning tool that provides a comprehensive assessment of web service vulnerabilities.
- ❋ **Dsniff** - a network auditing and penetration tool.
- ❋ **Nikto** - a web server scanner that tests web servers for over 3,500 vulnerabilities.
- ❖ **MegaPing** - a commercially available application that provides network information.
- ❋ **Password Crackers** - commercially available tools for cracking passwords and password-protected files.

Most importantly, we modify our methodology and approach to meet the needs of our clients and the specific technical environments we work in.

Software Tools Legend:
❖ Commercially Licensed
❋ Open-Source I Shareware

Select Software Tools

An indicative list of the other tools used during penetration testing is as follows:

- Brutus
- Cattscanner
- Cisco Auditing Tool
- Dirb
- Fpdns
- Ftpcheck
- Getif
- Hping2
- Httprint
- Hydra
- Ike-Scan
- MD-Webscan
- Metacoretex
- Metasploit Framework
- MSSQL Tools
- Nessus
- Nikto
- Nmap
- Oracle Auditing Tool
- Oracle Tools
- Paros
- Queso
- Sam Spade
- Sara
- SinFP
- Sitedigger
- Smtp-Scan
- Braa SNMP tool
- SQL Auditing Tool
- THC_Amap
- Webfuzzer
- Webroot
- Webscarab
- Wikto
- Winfingerprint
- Winfo
- Winhex
- Wireshark
- Xscan

Internal Network Vulnerability Assessment and Penetration Test

Our internal network assessment methodology follows the same rules of engagement as our external network methodology. Our methodology includes:

A) Information Gathering

- Connect to a "hot" port on the internal network.
- Obtain internal IP information about approved targets.
- In stealth mode, perform a port sweep to develop a map of the internal network structure and design.
- Attempt to identify critical business systems.
- Attempt to identify database systems, web applications and other technologies based on footprint.
- Review information with client's Project Manager.

B) Plan the Attack

- Configure scanning software based on approved scanning techniques.
- Plan social engineering schemes, if approved, to gain unauthorized access.
- Configure brute force testing against logins, if approved, to gain unauthorized access.

C) Vulnerability Testing

- Analyze information gathered.
- Plan the penetration.
- Identify modes of access.
- Locate trust hosts.
- Identify sensitive data flows.
- Document internal network topology.
- Perform scans using various tools and cross-reference available services against a comprehensive listing of vulnerability databases, such as: Security Focus, Microsoft Security Bulletins, Common VulnerabilityDatabase (OSVDB), United States Computer Emergency Response Team (US-CERT), Computer Emergency Response Team, SANS, Securiteam, PacketStorm Security, Security Tracker, Secunia, Bugtraq, etc.
- Exploit vulnerabilities and leave a trophy.
- Our testing techniques scale from soft to aggressive. Below are examples of soft and aggressive techniques we will utilize:
  - Soft techniques include:
    - Simple port scanning to identify listening ports;
    - Default password identification;
    - Observation-based social engineering; and
    - "Safe check" vulnerability scanning.
  - Aggressive techniques include:
    - Brute force password attacks;
    - Multi-location network sniffing;
    - Hard-sell social engineering;
    - Applying a denial of service attacks; and
    - Aggressive vulnerability scanning.

These examples complement each other in that soft techniques typically precede aggressive techniques. In world-class security organizations, soft techniques are often used to alert system administrators when aggressive techniques are being run against the network or system.

D) False Positives

Our staff has extensive experience performing vulnerability scans and penetration tests. The following methods will be used to identify false positives:

- The tools used will be configured specifically to the network device or system being tested;
- Our staff is highly experienced. The team will rely on the experience of the SME to identify vulnerabilities that are false;
- We will execute select exploits to confirm certain vulnerabilities; and
- Prior to reporting, we will validate our technical findings with IT Management.

E) Reporting and Summarizing

- Executive Summary
- Technician's Report

The Securance Consulting vulnerability assessment and penetration test performs a series of checks to discover methods to exploit your systems. Here is a summary list of checks we normally include in our methodology:

- Buffer Overflows
- Bypass Authentication
- Info from Case Studies, Presentations
- Command Injection
- Cross Site Request Forgery
- Cross Site Scripting
- Cross Site Tracing
- Database Scan
- Default Passwords
- Directory Traversal
- Info from DNS Records
- Fire Walking
- Firewall Vulnerability Detection
- Hard Coded Secrets
- HTML Source Code Analysis
- Integer Overflows
- Info from Job Postings
- LDAP Injection
- Info from Mailing Lists
- Open Relay Scan
- OS Fingerprinting
- Password Cracking
- Password Guessing
- Ping Sweep
- Port Scanning
- Info from Press Releases, Newsletters
- Info from Publicly Available Resumes
- Router Vulnerability Detection
- Look for Sensitive Error Messages
- Server I Service Fingerprinting
- Session ID Prediction
- SNMP Scan
- SQL Injection
- SSL Configuration
- Info from Trade Publications
- Validate Cryptographic Strength
- Vulnerable Sample Applications
- Web Server Vulnerability Scan
- Info from WHOIS Records
- XPATH Injection

Vulnerability Management and Reporting

Our deliverable includes a Technician's Report. This report identifies true vulnerabilities and provides a proven step-by-step method for mitigating the vulnerability. In addition, we provide real-world examples of the risk being assumed by an organization if it elects not to mitigate a proven vulnerability. The risk associated with each vulnerability varies. As such, unless true vulnerabilities are identified, we do not provide specific real-world examples of the business risk to an organization.

Standard Software Tools

The following is a list of the tools we will most likely utilize during the performance of parts of this engagement. Please note that the specific tool(s) used will be dictated by the specific technology being assessed.

In order to assess network components, servers and databases, we utilize "best in-class" automated tools in conjunction with our manual procedures. A short list of the tools we may use is as follows:

- ❋ **NMAP Scanner -** a comprehensive port scanner used to identify a host status and listening ports and to fingerprint an operating system.
- ❋ **NESSUS Scanner -** a comprehensive network vulnerability assessment tool for measuring system risks. Nessus is used to probe systems and report vulnerabilities that might create an exposure.
- ❖ **GFI LANguard** - a network security scanner designed specifically for Windows.
- ❋ **Netcat -** a simple UNIX utility which reads and writes data across network connections, using TCP or UDP protocol.
- ❖ **AppDetective** - a commercially licensed database-specific vulnerability and penetration testing tool.
- ❖ **SolarWinds** - a powerful combination of network discovery, monitoring and attack tools.
- ❋ **Metasploit Framework** - an advanced open-source platform for developing, testing and using exploit code.
- ❋ **Wireshark** - a network sniffer and TCP I IP analysis tool.
- ❖ **WebInspect -** an automated scanning tool that provides a comprehensive assessment of web service vulnerabilities.
- ❋ **Dsniff** - a network auditing and penetration tool.
- ❋ **Nikto** - a web server scanner that tests web servers for over 3,500 vulnerabilities.
- ❖ **MegaPing** - a commercially available application that provides network information.
- ❋ **Password Crackers** - commercially available tools for cracking passwords and password-protected files.

Most importantly, we modify our methodology and approach to meet the needs of our clients and the specific technical environments we work in.

Software Tools Legend:
- ❖ Commercially Licensed
- ❋ Open-Source I Shareware

Select Software Tools

An indicative list of the other tools used during penetration testing is as follows:

- Brutus
- Cattscanner
- Cisco Auditing Tool
- Dirb
- Fpdns
- Ftpcheck
- Getif
- Hping2
- Httprint
- Hydra
- Ike-Scan
- MD-Webscan
- Metacoretex
- Metasploit Framework
- MSSQL Tools
- Nessus
- Nikto
- Nmap
- Oracle Auditing Tool
- Oracle Tools
- Paros
- Queso
- Sam Spade
- Sara
- SinFP
- Sitedigger
- Smtp-Scan
- Braa SNMP tool
- SQL Auditing Tool
- THC_Amap
- Webfuzzer
- Webroot
- Webscarab
- Wikto
- Winfingerprint
- Winfo
- Winhex
- Wireshark
- Xscan

Web-Application Testing

The Securance web-application testing methodology includes looking for vulnerabilities at various layers and testing the overall security of web applications. Securance Consulting will perform an in-depth analysis of publicly available web servers, concentrating on security-related issues including, but not limited to:

- Cross Site Scripting (XSS)
- Malicious File Execution
- Insecure Direct Object Reference
- Information Leakage and Improper Error Handling
- SQL Injection
- CRLF Injection
- Remote Execution
- Directory l File Traversal
- PHP File Include
- Parameter Deletion
- Special Parameter Addition
- Boolean Parameter Tampering
- Broken Authentication and Session Management
- Buffer Overflow
- Format String
- Integer Overflow
- Information Exposure
- Generic HTTP Attacks
- Microsoft CGI Attacks
- CGI Attacks
- Microsoft IIS Attacks
- Common HTTP Device Attacks
- Cross Site Request Forgery (CSRF)
- Failure to Restrict URL Access
- Insecure Communications
- Insecure Cryptographic Storage
- Blind SQL Injection
- Injection Flaws

In addition to the procedures described above, the Securance web-application security testing methodology includes:

OS Level Assessment

- If access is to the operating system is obtained or provided, we perform a detailed security review of the operating system configuration. These procedures are performed against all servers that comprise the web-application infrastructure.

Database Assessment

- In addition to the operating system-level procedures, we perform a comprehensive security analysis against the portal's backend database. Initial attempts are made to access the database without credentials. Pending success, we perform a database-specific vulnerability scan using commercial tools (e.g., Application Detective or SecureSphere).

Web Login Assessment

- Our methodology includes assessing the web application by logging into the application and testing for various vulnerabilities. Our process will uncover hidden input fields; test input parameters; crawl the portal and identify exploratory features; attempt to discover sensitive and private information; uncover common software writing errors; identify common injection vulnerabilities that may allow malicious code execution; and assess error handling that may expose the application.

Source Code Review

The Securance source code review methodology begins with gaining a detailed understanding of the application's architecture. This is achieved through interviews with the application owner, senior developer and business owner. The following additional steps aid in understanding the application prior to performing an automated source code review:

- Gaining an understanding of the system development life cycle (SDLC) methodology that was used to guide development;
- Gaining an understanding of the development and coding standards in place;
- Reviewing all available requirements, design, UI and technical documentation;
- Performing a structured walkthrough of the source code; and
- Reviewing all available project plans, tracking systems and testing documentation.

Upon completing the above tasks, we then assess the source code using an automated source code analyzer. This process is useful to complete the following:

- Identify calls to insecure library functions;
- Detect type confusion;
- Detect memory errors;
- Identify vulnerabilities in sequence of operations;
- Perform data flow and loop analyses; and
- Identify potential buffer overflows.

Appendix C

Sample Report
Provided for:

THE CITY OF COLUMBUS

Network Security Report

TABLE OF CONTENTS

EXECUTIVE SUMMARY

INTRODUCTION AND SCOPE

In May 2016, Securance Consulting conducted a Network Security Assessment for ABC Corporation (herein ABC). The overall objective of the engagement was to identify technology-specific vulnerabilities, information technology (IT) process risks, and documented pathways for breaching network security. The scope of the engagement included assessments of:

- Select IT controls – including IT security policies, general IT administration and physical security;
- External Internet Protocol (IP) network – including a configuration review of one (1) perimeter firewall; and
- Internal IP Network – including five (5) selected internal IP ranges, three (3) selected databases, the internal wireless network and a review of Active Directory (AD) username and password management.

The review was limited to those areas specifically defined by ABC's Information Security Office and management personnel, and was not intended to be a comprehensive examination of ABC's entire information systems function.

FINDING LEGEND:

Urgent-Risk (Level 5) – Immediate remediation required.
Note: If finding is a technical vulnerability, it provides remote intruders with remote root or remote administrator capabilities.

Critical-Risk (Level 4) – Immediate action recommended with remediation ASAP.
Note: If finding is a technical vulnerability, it provides intruders with remote user, but not remote administrator or root user, capabilities.

High-Risk (Level 3) – Immediate action recommended with remediation in 90 days.
Note: If finding is a technical vulnerability, it provides hackers with access to specific information stored on the host, including security settings. This level of vulnerabilities could result in potential misuse of the host by intruders.

Medium-Risk (Level 2) – Action recommended with remediation in 180 days.
Note: If finding is a technical vulnerability, it may expose some sensitive information from the host, such as precise versions of services. With this information, hackers could research potential attacks to try against a host.

Low-Risk l Informational (Level 1) – Effective control. No immediate changes recommended. Opportunity for slight improvement.

Advisory comment…action suggested at the discretion of management.

SUMMARY OF FINDINGS

The following section provides a summary of our findings, a graphical analysis of the vulnerabilities identified that are considered urgent, critical, high, or medium risks, and our conclusion regarding ABC's security posture.

Review of select information technology (IT) controls:

No. 1: Formal IT Governance Program – ABC's IT organization does not have a comprehensive IT governance program. As a result, critical IT policies and procedures are nonexistent. Specifically, we were unable to obtain a management-approved IT security or user administration policy. These policies are necessary to establish a secure computing environment.

External Internet Protocol (IP) network, including a configuration review of one (1) perimeter firewall:

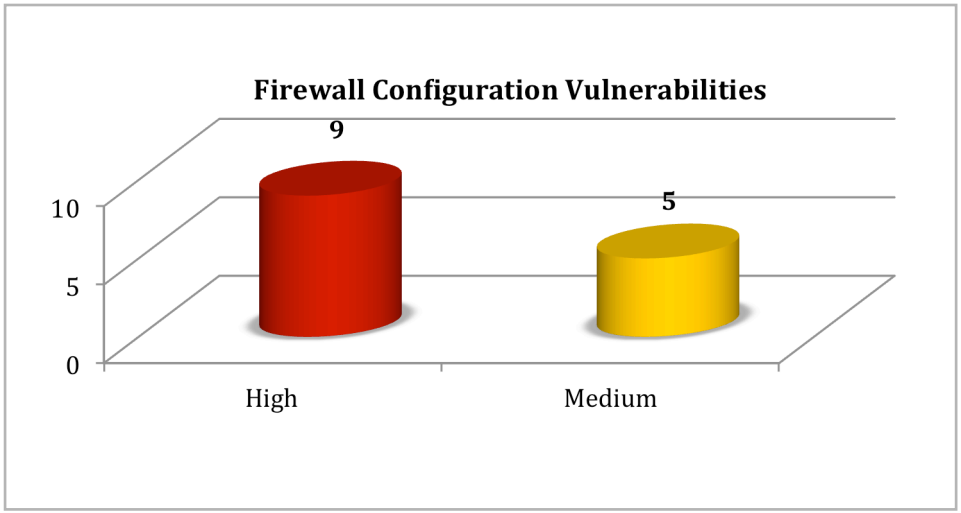
No. 2: External IP Network Vulnerability Assessment – We performed a detailed scan against ABC's external IP address block and identified one (1) critical and seven (7) high-priority vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated network breach. The chart on page fifteen (15) provides a snapshot of the vulnerabilities identified, prioritized by level of severity. The detailed body of this report summarizes the unique vulnerabilities, the affected systems, and the recommended solutions.

No. 3: Firewall Configuration Risks – We performed a detailed scan against one (1) perimeter firewall and identified the nine (9) areas of high risk and five (5) areas of medium risk. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated firewall breach. The chart on page nine (9) provides a snapshot of the vulnerabilities identified, prioritized by level of severity. The detailed body of this report summarizes the unique vulnerabilities, the affected systems, and the recommended solutions. In many cases the recommended solution requires a modification of the firewall rule.

The remainder of this section is omitted from the sample report.

Firewall Configuration Review Analysis

- *Identified nine (9) high vulnerabilities, including:*
  - Three (3) services: Risky Microsoft services, MSSQL, and TFTP can enter your network.
  - Two (2) vulnerabilities related to the "Any" service.
  - Four (4) findings related to DNS/UDP HTTP and Telnet which makes addresses reachable from the outside.
  - Internal addresses can use SMTP to connect to the outside.
- *Identified seven (7) medium vulnerabilities, including:*
  - Three (3) vulnerabilities related to the "Any" service.
  - IP addresses on your network are reachable via SMTP.
  - SNMP and RPC can enter your network.
  - Machines on the network can access peer-to-peer file sharing services.



CONCLUSION

Based on the procedures we performed, our knowledge of ABC's computing environment and our IT security experience, it is our opinion, as of the date of this review, that ABC's external network (including the firewall) and internal network (including the wireless network, databases and Active Directory) are ineffective from a security perspective. We recommend the review and implementation of the solutions provided to improve the organization's security posture. As with all recommendations that may affect a computer system or network device, changes should be tested in a non-production environment prior to implementation in production.

The remainder of this report provides a detailed analysis of our approach and methodology and specific vulnerabilities identified.

Remainder of this page left blank intentionally.

NETWORK SECURITY ASSESSMENT REPORT

BACKGROUND

During February 2014, Securance Consulting conducted a Network Security Assessment for ABC. The overall objective of the engagement was to identify technology-specific vulnerabilities, IT process related risks, and documented pathways to breaching network security. The scope included assessments of:

- Select Information Technology (IT) controls – including IT security policies, general IT administration and physical security;
- External Internet Protocol (IP) network – including a configuration review of one (1) perimeter firewall; and
- Internal IP network – including five (5) selected internal IP ranges, three (3) selected databases, the internal wireless network and a review of Active Directory (AD) username and password management.

The review was limited to those areas specifically defined by ABC's Department of Information Security Office and management personnel, and was not intended to be a comprehensive examination of ABC's entire information systems function.

SPECIFIC OBJECTIVES AND SCOPE

The objective of the review was to assess the adequacy of administrative controls over select IT processes and to identify technical vulnerabilities within ABC's internal and external networks. The scope of the review included assessments of the following processes, networks, systems, and technologies:

- Select IT Controls:
  - IT security policies and procedures;
  - General IT administration; and
  - Physical security.

- External Network Internet Protocol (IP) Addresses:
  - 165.xxx.xxx.xxx
  - 165.xxx.xxx.xxx
  - 165.xxx.xxx.xxx
  - 140.xxx.xxx.xxx
  - 140.xxx.xxx.xxx

- Firewall Configuration Review:
  - Checkpoint ASA Firewall

- Internal Network Internet Protocol (IP) Ranges:
  - 10.xx.xx.x – 10.xx.xx.xxx
  - 10.xx.x.x – 10.xx.x.xxx
  - 10.xx.x.x – 10.xx.x.xxx
  - 10.xx.x.x – 10.xx.xx.xxx
  - 10.xx.x.x – 10.xx.xx.xxx

- Database Security Assessment:
  - DATABASE 01
  - DATABASE 02
  - DATABASE 03

- Internal Wireless Network

- Active Directory System

APPROACH AND METHODOLOGY

To achieve the objectives of this engagement, within the defined scope, we performed diagnostic and vulnerability assessment activities utilizing our proven methodology. The following describes the high-level tasks performed for each component of the project:

SELECT IT CONTROLS:

During this phase, our assessment was supported by the following activities:

- On/off-site interviews with key IT personnel;
- Review of available policies and procedures;
- On-site physical walkthrough of the data center; and
- Access point configuration review:
  - We employed automated and manual techniques to assess signal strength bleed, rogue access point identification, encryption strength and protocol assessment, network segmentation and control, and administrative access controls.

ACTIVE DIRECTORY USER ACCOUNT ANALYSIS:

During this phase, we performed an automated scan against the Active Director system to gather data for manual analysis. During our analysis, we reviewed all account settings and security configurations to identify the appropriateness of user accounts.

FINDINGS AND RECOMMENDATIONS – SELECT IT CONTROLS

The following recommendations, which resulted from the review of the selected ABC's IT policies and procedures, general IT administration and physical security, are submitted to assist in improving ABC's IT security posture.

No. 1: Formal IT Governance Program

IT governance is a program designed, in part, to establish management's tone of internal controls over the technology environment. Most often, IT governance is established in the form of management approved IT policies and procedures. ABC's IT organization does not have a comprehensive IT governance program. As a result, several critical IT policies and procedures are nonexistent. Specifically, we were unable to obtain a management-approved IT security or user administration policy. These policies are necessary to establish a secure computing environment.

Risk:
The lack of an IT governance program that is inclusive of an IT security and user administration policy creates an IT environment where the application of IT security controls is inconsistent and may not meet management's standards, as the standards are unknown. This type of environment inappropriately places reliance on IT engineers, administrators, and professionals to establish a set of controls based on prior knowledge. This exposes the environment to network, system and data breaches, as the implemented controls may not provide adequate protection.

Recommendation:
We recommend the implementation of a comprehensive IT governance program that establishes management's intention for IT security and internal controls. At a minimum, a comprehensive IT security policy that addresses all applicable facets of IT security should be drafted and approved by management. The following is a list of select components of a best practice IT security policy:

- Data Classification and Ownership
- Data Transmission and End User Computing
- End User Training (Security Awareness Training)
- Incident Management and Escalation Management

- Wireless Services
- Remote Access Management
- Network Security (i.e., Virus Protection, IDS/IPS and Firewall Security)
- Event Monitoring and Logging
- Configuration Management (i.e., Network Devices, Platforms, Database Systems and Applications)

This policy should be supported by detailed IT procedures that provide guidance on how such security should be implemented, maintained and monitored.

In addition, a user administration policy and supporting procedures should be implemented. This policy should be designed to govern the process of granting modifying and revoking user access.

Management's Response:

FINDINGS AND RECOMMENDATIONS – EXTERNAL NETWORK VULNERABILITY ASSESSMENT

The following recommendations, which resulted from the external network vulnerability assessment, are submitted to assist in improving the security posture of the target segment of ABC's external network.

No. 2: External Network Vulnerabilities

We performed a detailed scan against ABC's external IP address block and identified one (1) critical and seven (7) high risk vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated network breach.

The charts on page twenty (20) provide a snapshot of the vulnerabilities identified, prioritized by level of severity. The pages that follow summarize unique vulnerabilities, the affected systems and the recommended solutions. In many cases, the recommended solution requires a system security patch.

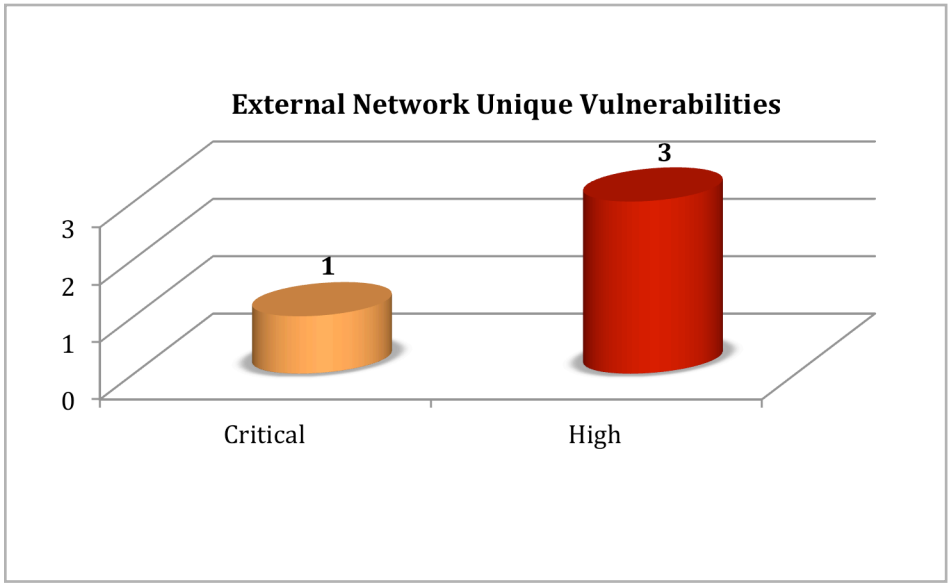
Risk:
ABC's external network is at risk of being compromised by an attacker. Depending upon the type of breach executed, systems could be rendered unresponsive, data could be compromised, or segments of the network could be used to breach internal systems and/or other department systems.

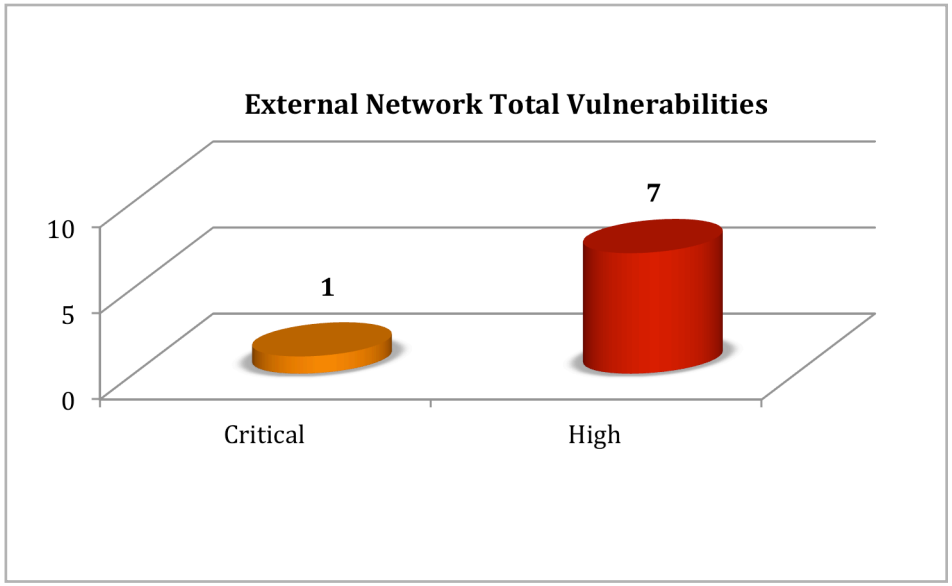
Recommendation:
We strongly recommend that ABC immediately address all critical and high vulnerabilities. As with all recommendations that may affect a computer system or network device, changes should be tested in a non-production environment prior to implementation in production.

Vulnerability details are provided in a separate Technician's Report. All low-risk vulnerabilities and informational disclosures are only provided in the Technician's Report. A finding and technical vulnerability legend is provided on page five (5).

Management's Response:

Remainder of this page left blank intentionally.





Remainder of this page left blank intentionally.

Threat Level	Server	Vulnerability Description	Fix	Recommendation
Critical	• 2xx.xxx.xxx.x	**Microsoft IIS Repost.asp File Upload -** The script '/scripts/repost.asp' is installed on the remote IIS web server and allows an attacker to upload arbitrary files to the '/Users' directory if it has not been configured properly. *REF: CVE-1999-0360; http://www.securityfocus.com/bid/1811/discuss; http://www.osvdb.org/285*	Create the '/Users' directory if necessary and ensure that the Anonymous Internet Account ('IUSER_MACHINE') only has read access to it.
High	• 2xx.xxx.xxx.xx • 2xx.xxx.xxx.xx	**DNS Server Cache Snooping Information Disclosure -** The remote DNS server responds to queries for third-party domains which do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of that financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more. *REF: http://www.rootsecure.net/content/downloads/pdf/dns_cache_snooping.pdf*	Use another DNS software.
High	• 2xx.xxx.xxx.xx • 2xx.xxx.xxx.xx • 2xx.xxx.xxx.xx	**Web Server HTTP Header Internal IP Disclosure -** This may expose internal IP addresses that are usually hidden or masked behind a Network Address Translation (NAT) Firewall or proxy server. There is a known issue with Microsoft IIS 4.0 doing this in its default configuration. This may also affect other web servers, web applications, web proxies, load balancers and through a variety of misconfigurations related to redirection. *REF: CVE-2000-0649*	None at this time. Monitor the vulnerability for a vendor upgrade.

Remainder of findings eliminated for brevity of sample report.

SECURANCE VALUE

Securance Consulting would like to **THANK YOU** for your business. Aside from benefiting from the highest level of service possible, you also received unique advantages that only Securance Consulting delivers. Our hands-on approach is tailored to fit the needs of both the compliance and information technology departments. Our technical expertise, outstanding reputation and personalized attention ensure you a level of service surpassed by no other technology risk management firm in the market.

As a Securance customer, you can be confident in your sound decision to manage your technology risk with a co-sourced relationship with Securance!

Sample Report
Provided for:

THE CITY OF COLUMBUS

Technician's Report

CONFIDENTIAL

This report is intended solely for the management of the City for their internal use and is not intended for, nor may be relied upon by, any other party ("Third Party"). Neither this deliverable nor its contents may be distributed to, discussed with, or otherwise disclosed to any Third Party without the prior written permission of Securance Consulting. Securance Consulting accepts no liability or responsibility to any Third Party who gains access to this report.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
1	208.xx.xxx.xx	CVE-2003-0693	OpenSSH < 3.7.1 Multiple Vulnerabilities	10.0	High	A "buffer management error" in buffer_append_space of buffer.c for OpenSSH before 3.7 may allow remote attackers to execute arbitrary code by causing an incorrect amount of memory to be freed and corrupting the heap, a different vulnerability than CVE-2003-0695.	Upgrade to OpenSSH 3.7.1 or later. **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.
2	208.xx.xxx.xx	CVE-2003-0682	OpenSSH < 3.7.1 Multiple Vulnerabilities	7.5	High	A "buffer management error" in buffer_append_space of buffer.c for OpenSSH before 3.7 may allow remote attackers to execute arbitrary code by causing an incorrect amount of memory to be freed and corrupting the heap, a different vulnerability than CVE-2003-0695.	Upgrade to OpenSSH 3.7.1 or later. **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
3	208.xx.xxx.xx	CVE-2003-0695	OpenSSH < 3.7.1 Multiple Vulnerabilities	7.5	High	Multiple "buffer management errors" in OpenSSH before 3.7.1 may allow attackers to cause a denial of service or execute arbitrary code using (1) buffer_init in buffer.c, (2) buffer_free in buffer.c, or (3) a separate function in channels.c, a different vulnerability than CVE-2003-0693.	Upgrade to OpenSSH 3.7.1 or later. **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.
4	208.xx.xxx.xx	CVE-1999-0502*	Default Password (guest) for 'guest' Account	7.5	High	The account 'guest' has the password 'guest' set. An attacker may use it to gain further privileges on this system.	Set a password for this account or disable it.
5	208.xx.xxx.xx	CVE-2008-1483	OpenSSH X11 Forwarding Session Hijacking	6.9	Medium	The remote SSH service is prone to an X11 session hijacking vulnerability. According to its banner, the version of SSH installed on the remote host is older than 5.0. Such versions may allow a local user to hijack X11 sessions because it improperly binds TCP ports on the local IPv6 interface if the corresponding ports on the IPv4 interface are in use. See also : http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011 http://www.openssh.org/txt/release-5.0	Upgrade to OpenSSH version 5.0 or later. **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
6	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Medium -Auth: None -Conf: Partial -Integ: Partial -Avail: Partial	Open ports and potential malware	6.8	Medium	Identified several open TCP/UDP ports. The following malware may be present on these ports: - TCP80: Back End, Executor, Hooker, RingZero	Confirm presence of malware and remove.
7	208.xx.xxx.xx	CVE-2003-1567 Other References: OSVDB:877 OSVDB:3726 OSVDB:5648 OSVDB:50485	HTTP TRACE / TRACK Methods Allowed	5.8	Medium	The undocumented TRACK method in Microsoft Internet Information Services (IIS) 5.0 returns the content of the original request in the body of the response, which makes it easier for remote attackers to steal cookies and authentication credentials, or bypass the HttpOnly protection mechanism, by using TRACK to read the contents of the HTTP headers that are returned in the response, a technique that is similar to cross-site tracing (XST) using HTTP TRACE.	Disable these methods. Refer to the plugin output for more information.
8	208.xx.xxx.xx	CVE-2004-2320 Other References: OSVDB:877 OSVDB:3726 OSVDB:5648 OSVDB:50485	HTTP TRACE / TRACK Methods Allowed	5.8	Medium	The default configuration of BEA WebLogic Server and Express 8.1 SP2 and earlier, 7.0 SP4 and earlier, 6.1 through SP6, and 5.1 through SP13 responds to the HTTP TRACE request, which can allow remote attackers to steal information using cross-site tracing (XST) attacks in applications that are vulnerable to cross-site scripting.	Disable these methods. Refer to the plugin output for more information.
9	208.xx.xxx.xx	CVE-2010-0386 Other References: OSVDB:877 OSVDB:3726 OSVDB:5648 OSVDB:50485	HTTP TRACE / TRACK Methods Allowed	4.3	Medium	The default configuration of Sun Java System Application Server 7 and 7 2004Q2 enables the HTTP TRACE method, which makes it easier for remote attackers to steal cookies and authentication credentials via a cross-site tracing (XST) attack, a related issue to CVE-2004-2763 and CVE-2005-3398.	Disable these methods. Refer to the plugin output for more information.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
10	208.xx.xxx.xx	CVE-2006-3918	Web Server Expect Header	4.3	Medium	http_protocol.c in (1) IBM HTTP Server 6.0 before 6.0.2.13 and 6.1 before 6.1.0.1, and (2) Apache HTTP Server 1.3 before 1.3.35, 2.0 before 2.0.58, and 2.2 before 2.2.2, does not sanitize the Expect header from an HTTP request when it is reflected back in an error message, which might allow cross-site scripting (XSS) style attacks using web client components that can send arbitrary headers in requests, as demonstrated using a Flash SWF file.	Check with the vendor for an update to the web server. For Apache, the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2 for IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1 for IBM WebSphere Application Server, upgrade to 5.1.1.17.
11	208.xx.xxx.xx	CVE-2007-5944	Cross-site scripting vulnerability	4.3	Medium	Cross-site scripting (XSS) vulnerability in Servlet Engine / Web Container in IBM WebSphere Application Server (WAS) 5.1.1.4 through 5.1.1.16 allows remote attackers to inject arbitrary web script or HTML via the Expect HTTP header. NOTE: this might be the same issue as CVE-2006-3918, but there are insufficient details to be sure.	Check with the vendor for an update to the web server. For Apache, the issue is reportedly fixed by versions 1.3.35 / 2.0.57 / 2.2.2 for IBM HTTP Server, upgrade to 6.0.2.13 / 6.1.0.1 for IBM WebSphere Application Server, upgrade to 5.1.1.17.
12	208.xx.xxx.xx	CVE - None Other References: OSVDB-877 **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Medium -Auth: None -Conf: Partial -Integ: None -Avail: None	Multiple Web Server Dangerous HTTP Method TRACE	4.3	Medium	RFC compliant web servers support the TRACE HTTP method, which contains a flaw that may lead to an unauthorized information disclosure. The TRACE method is used to debug web server connections and allows the client to see what is being received at the other end of the request chain. Enabled by default in all major web servers, a remote attacker may abuse the HTTP TRACE functionality, i.e. cross-site scripting (XSS), which will disclose sensitive configuration information resulting in a loss of confidentiality. GET, HEAD, POST, OPTIONS, TRACE	Disable this method.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
13	208.xx.xxx.xx	CVE-2001-0361 Other References: OSVDB:2116	SSH Protocol Version 1 Session Key Retrieval	4.0	Medium	The remote SSH daemon supports connections made using the version 1.33 and/or 1.5 of the SSH protocol. These protocols are not completely cryptographically safe so they should not be used.	Disable compatibility with version 1 of the protocol. **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.
14	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Inconsistent Hostname and IP Address	0.0	Low	The name of this machine either does not resolve or resolves to a different IP address. This may come from a badly configured reverse DNS	Correct hostname and IP address.
15	208.xx.xxx.xx	CVE-1999-0524	ICMP Timestamp Request Remote Date Disclosure	0.0	Low	The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine. This may help him to defeat all your time based authentication protocols.	Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
16	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Medium -Auth: None -Conf: None -Integ: None -Avail: None	SSH Server Type and Version Information	0.0	Low	An SSH server is listening on this port. It is possible to obtain information about the remote SSH server by sending an empty authentication request. SSH version : SSH-1.99-OpenSSH_3.6.1p1 SSH supported authentication : publickey,password,keyboard-interactive	N/A **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.
17	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Medium -Auth: None -Conf: None -Integ: None -Avail: None	SSH Protocol Versions Supported	0.0	Low	A SSH server is running on the remote host. This plugin determines the versions of the SSH protocol supported by the remote SSH daemon. The remote SSH daemon supports the following versions of the SSH protocol : - 1.33 - 1.5 - 1.99 - 2.0 SSHv1 host key fingerprint : 8a:44:8e:aa:67:c1:77:73:c3:3b:a5:9c:10:a5:65:cc SSHv2 host key fingerprint : 6a:37:45:22:54:8d:89:d5:4f:c5:7b:e7:49:45:fb:ba	N/A **Special Note:** Note to scan customer: Due to increased risk to the cardholder data environment when remote access software is present, please 1) justify the business need for this software to the ASV and 2) confirm it is either implemented securely per Appendix C or disabled/ removed. Please consult your ASV if you have questions about this Special Note.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
18	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	HTTP Server type and version	0.0	Low	A web server is running on the remote host. This plugin attempts to determine the type and the version of the remote web server. The remote web server type is: Apache/2.2.0 (Linux/SUSE)	N/A
19	208.xx.xxx.xx	CVE - None Other References: OWASP-CM-006 **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Web Server Directory Enumeration	0.0	Low	It is possible to enumerate directories on the web server. This plugin attempts to determine the presence of various common directories on the remote web server. By sending a request for a directory, the web server response code indicates if it is a valid directory or not. The following directories were discovered: /cgi-bin, /error, /icons.	N/A
20	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	HMAP Web Server Fingerprinting	0.0	Low	HMAP fingerprints the remote HTTP server. By sending several valid and invalid HTTP requests, it may be possible to identify the remote web server type. In some cases, its version can also be approximated, as well as some options. An attacker may use this tool to identify the kind of the remote web server and gain further knowledge about this host.	N/A

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
21	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	HyperText Transfer Protocol (HTTP) Information	0.0	Low	Some information about the remote HTTP configuration can be extracted. This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc... This test is informational only and does not denote any security problem.	N/A
22	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Backported Security Patch Detection (WWW)	0.0	Low	Security patches are backported. Security patches may have been 'back ported' to the remote HTTP server without changing its version number. Banner-based checks have been disabled to avoid false positives. Note that this test is informational only and does not denote any security problem.	N/A
23	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	HTTP methods per directory	0.0	Low	By calling the OPTIONS method, it is possible to determine which HTTP methods are allowed on each directory. As this list may be incomplete, the plugin also tests various known HTTP methods on each directory and considers them as unsupported if it receives a response code of 400, 403, 405, or 501. Note that the plugin output is only informational and does not necessarily indicate the presence of any security vulnerabilities.	N/A

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
24	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	RPC Services Enumeration	0.0	Low	An ONC RPC service is running on the remote host. By sending a DUMP request to the portmapper, it was possible to enumerate the ONC RPC services running on the remote port. Using this information, it is possible to connect and bind to each service by sending an RPC request to the remote port.	N/A
25	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	RPC portmapper Service Detection	0.0	Low	An ONC RPC portmapper is running on the remote host. The portmapper allows someone to get the port number of each RPC service running on the remote host by sending either multiple lookup requests or a DUMP request.	N/A
26	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	OS Identification	0.0	Low	This script attempts to identify the Operating System type and version by looking at the results of other scripts. The remote host is running Linux Kernel 2.6 on SuSE Linux 10.1	

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
27	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	IP Protocols Scan	0.0	Low	This plugin detects the protocols understood by the remote IP stack. The following IP protocols are accepted on this host: 1 ICMP 2 IGMP 6 TCP 17 UDP 41 IPv6	N/A
28	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Apache Banner Linux Distribution Disclosure	0.0	Low	This script extracts the banner of the Apache web server and attempts to determine which Linux distribution the remote host is running. The linux distribution detected was : - SuSE Linux 10.1	If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.
29	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	TCP/IP Timestamps Supported	0.0	Low	The remote host implements TCP timestamps, as defined by RFC1323. A side effect of this feature is that the uptime of the remote host can sometimes be computed.	N/A

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
30	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Potentially sensitive resource discovered	0.0	Low	The Nikto web application scanner found an interesting file/url. It is recommended to verify that this resource does not contain any sensitive information and is intended to be available to the public. If this is a legitimate resource, then this file/url can be marked to be ignored from future reporting.	
31	208.xx.xxx.xx	CVE - None Other References: OSVDB-3233 **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Default web server page	0.0	Low	A default file, directory or CGI program which installed by default with the web server or installed software was found. While there is no known vulnerability or exploit associated with this, default files often reveal sensitive information or contain unknown or undisclosed vulnerabilities. The presence of such files may also reveal information about the web server version or operating system. GET /icons/README: /icons/README	Remove unnecessary default server pages.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
32	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Medium -Auth: None -Conf: None -Integ: None -Avail: None	ETag header found on server	0.0	Low	A cache management feature is available for Apache that makes use of an entity tag (ETag) header. When this option is enabled and a request is made for a document relating to a file, for caching purposes, an ETag response header is returned containing various file attributes. ETag information allows further requests for files to contain specific information, such as the file's inode number, which allows for faster lookup times. A weakness has been found in the generation of ETag headers under certain configurations implementing the FileETag directive. Among the file attributes included in the header is the file inode number that is returned to a client. This poses a security risk, as this information may aid in launching attacks against other network-based services.	
33	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Apache version outdated	0.0	Low	Apache/2.2.0 appears to be outdated (current is at least Apache/2.2.15). Apache 1.3.42 and 2.0.63 are also current.	Upgrade to the latest Apache server.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
34	208.xx.xxx.xx	CVE - None Other References: OSVDB-3268 **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: None -Integ: None -Avail: None	Directory indexing enabled	0.0	Low	Directory indexing has been found to be enabled on the web server. While there is no known vulnerability or exploit associated with this, it may reveal sensitive or "hidden" files or directories to remote users, or aid in more focused attacks. **Path:** /icons/ **Path:** /icons/small/	N/A
35	208.xx.xxx.xx	CVE-2007-0910	PHP < 5.2.1 Multiple Vulnerabilities	10.0	High	Unspecified vulnerability in PHP before 5.2.1 allows attackers to "clobber" certain super-global variables via unspecified vectors.	Upgrade to PHP version 5.2.1 or later.
36	208.xx.xxx.xx	CVE-2008-0599	PHP < 5.2.6 Multiple Vulnerabilities	10.0	High	The init_request_info function in sapi/cgi/cgi_main.c in PHP before 5.2.6 does not properly consider operator precedence when calculating the length of PATH_TRANSLATED, which might allow remote attackers to execute arbitrary code via a crafted URI.	Upgrade to PHP version 5.2.6 or later.
37	208.xx.xxx.xx	CVE-2008-2050	PHP < 5.2.6 Multiple Vulnerabilities	10.0	High	Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.	Upgrade to PHP version 5.2.6 or later.
38	208.xx.xxx.xx	CVE-2008-2051	PHP < 5.2.6 Multiple Vulnerabilities	10.0	High	The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to "incomplete multibyte chars."	Upgrade to PHP version 5.2.6 or later.
39	208.xx.xxx.xx	CVE-2008-5557	PHP 5 < 5.2.7 Multiple Vulnerabilities - heap-based buffer overflow	10.0	High	Heap-based buffer overflow in ext/mbstring/libmbfl/filters/mbfilter_htmlent.c in the mbstring extension in PHP 4.3.0 through 5.2.6 allows context-dependent attackers to execute arbitrary code via a crafted string containing an HTML entity, which is not properly handled during Unicode conversion, related to the (1) mb_convert_encoding, (2) mb_check_encoding, (3) mb_convert_variables, and (4) mb_parse_str functions.	Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
40	208.xx.xxx.xx	CVE-2009-1955	Apache 2.x < 2.2.12 Multiple Vulnerabilities - DoS memory consumption	7.8	High	The expat XML parser in the apr_xml_* interface in xml/apr_xml.c in Apache APR-util before 1.3.7, as used in the mod_dav and mod_dav_svn modules in the Apache HTTP Server, allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document containing a large number of nested entity references, as demonstrated by a PROPFIND request, a similar issue to CVE-2003-1564.	Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.
41	208.xx.xxx.xx	CVE - None **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Medium -Auth: None -Conf: None -Integ: Partial -Avail: None	MySQL Community Server Multiple Vulnerabilities	7.8	High	The remote database server is susceptible to multiple attacks. The version of MySQL Community Server installed on the remote host is affected by a denial of service and privilege escalation vulnerability. An attacker may crash the server with a special crafted password packet and/or create arbitrary tables using the affected application.	Upgrade to MySQL Community Server version 5.0.45 or later.
42	208.xx.xxx.xx	CVE-2008-0166	OpenSSL version 0.9.8c appears to be outdated	7.8	High	OpenSSL 0.9.8c-1 up to versions before 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.	Upgrade OpenSSL to the latest version.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
43	208.xx.xxx.xx	CVE - None http://www.owasp.org/index.php/SQL_injection **Note:** Manual Scoring Vectors -Access: Network -Access Comp: Low -Auth: None -Conf: Partial -Integ: Partial -Avail: Partial	SQL Injection	7.5	High	SQL injection is a technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and thereby unexpectedly executed. An attacker can use this vulnerability to read any information from the database that the web application has access to, to sometimes write new data to the database, and in some cases the attacker can gain full control over the system. SQL injection occurs when user input is not properly encoded/filtered/properly typed prior to being used in a SQL statement. In order to fix this issue, the application developers must encode/filter/type data prior to being used. For example, if you have a value that is supposed to be an integer, typecast it as an integer. If you have a value that is supposed to be a string encode/filter any SQL command characters. Path: recipe/recipe/recipe_view.php	
44	208.xx.xxx.xx	CVE-2007-0905	PHP < 5.2.1 Multiple Vulnerabilities - bypass safe_mode and open_basedir restrictions	7.5	High	PHP before 5.2.1 allows attackers to bypass safe_mode and open_basedir restrictions via unspecified vectors in the session extension. NOTE: it is possible that this issue is a duplicate of CVE-2006-6383.	Upgrade to PHP version 5.2.1 or later.
45	208.xx.xxx.xx	CVE-2007-0906	PHP < 5.2.1 Multiple Vulnerabilities	7.5	High	Multiple buffer overflows in PHP before 5.2.1 allow attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors in the (1) session, (2) zip, (3) imap, and (4) sqlite extensions; (5) stream filters; and the (6) str_replace, (7) mail, (8) ibase_delete_user, (9) ibase_add_user, and (10) ibase_modify_user functions. NOTE: vector 6 might actually be an integer overflow (CVE-2007-1885). NOTE: as of 20070411, vector (3) might involve the imap_mail_compose function (CVE-2007-	Upgrade to PHP version 5.2.1 or later.
46	208.xx.xxx.xx	CVE-2007-0909	PHP < 5.2.1 Multiple Vulnerabilities - execute arbitrary code	7.5	High	Multiple format string vulnerabilities in PHP before 5.2.1 might allow attackers to execute arbitrary code via format string specifiers to (1) all of the *print functions on 64-bit systems, and (2) the odbc_result_all function.	Upgrade to PHP version 5.2.1 or later.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
47	208.xx.xxx.xx	CVE-2007-1376	PHP < 5.2.1 Multiple Vulnerabilities - read and write to arbitrary memory locations	7.5	High	The shmop functions in PHP before 4.4.5, and before 5.2.1 in the 5.x series, do not verify that their arguments correspond to a shmop resource, which allows context-dependent attackers to read and write arbitrary memory locations via arguments associated with an inappropriate resource, as demonstrated by a GD Image resource.	Upgrade to PHP version 5.2.1 or later.
48	208.xx.xxx.xx	CVE-2007-1453	PHP < 5.2.1 Multiple Vulnerabilities - buffer overflow	7.5	High	Buffer underflow in the PHP_FILTER_TRIM_DEFAULT macro in the filtering extension (ext/filter) in PHP 5.2.0 allows context-dependent attackers to execute arbitrary code by calling filter_var with certain modes such as FILTER_VALIDATE_INT, which causes filter to write a null byte in whitespace that precedes the buffer.	Upgrade to PHP version 5.2.1 or later.
49	208.xx.xxx.xx	CVE-2007-1700	PHP < 5.2.1 Multiple Vulnerabilities - execute arbitrary code	7.5	High	The session extension in PHP 4 before 4.4.5, and PHP 5 before 5.2.1, calculates the reference count for the session variables without considering the internal pointer from the session globals, which allows context-dependent attackers to execute arbitrary code via a crafted string in the session_register after unsetting HTTP_SESSION_VARS and _SESSION, which destroys the session data Hashtable.	Upgrade to PHP version 5.2.1 or later.
50	208.xx.xxx.xx	CVE-2007-1825	PHP < 5.2.1 Multiple Vulnerabilities - buffer overflow	7.5	High	Buffer overflow in the imap_mail_compose function in PHP 5 before 5.2.1, and PHP 4 before 4.4.5, allows remote attackers to execute arbitrary code via a long boundary string in a type.parameters field. NOTE: as of 20070411, it appears that this issue might be subsumed by CVE-2007-0906.3.	Upgrade to PHP version 5.2.1 or later.
51	208.xx.xxx.xx	CVE-2007-1885	PHP < 5.2.1 Multiple Vulnerabilities - execute arbitrary code	7.5	High	Integer overflow in the str_replace function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 allows context-dependent attackers to execute arbitrary code via a single character search string in conjunction with a long replacement string, which overflows a 32 bit length counter. NOTE: this is probably the same issue as CVE-2007-0906.6.	Upgrade to PHP version 5.2.1 or later.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
52	208.xx.xxx.xx	CVE-2007-1887	PHP < 5.2.1 Multiple Vulnerabilities - buffer overflow	7.5	High	Buffer overflow in the sqlite_decode_binary function in the bundled sqlite library in PHP 4 before 4.4.5 and PHP 5 before 5.2.1 allows context-dependent attackers to execute arbitrary code via an empty value of the in parameter, as demonstrated by calling the sqlite_udf_decode_binary function with a 0x01 character.	Upgrade to PHP version 5.2.1 or later.
53	208.xx.xxx.xx	CVE-2007-1890	PHP < 5.2.1 Multiple Vulnerabilities - execute arbitrary code	7.5	High	Integer overflow in the msg_receive function in PHP 4 before 4.4.5 and PHP 5 before 5.2.1, on FreeBSD and possibly other platforms, allows context-dependent attackers to execute arbitrary code via certain maxsize values, as demonstrated by 0xffffffff.	Upgrade to PHP version 5.2.1 or later.
54	208.xx.xxx.xx	CVE-2006-5465	PHP < 5.2 Multiple Vulnerabilities	7.5	High	According to its banner, the version of PHP installed on the remote host is older than 5.2. Such versions may be affected by several buffer overflows. PHP version 5.1.6 appears to be running on the remote host based on the following Server response header : Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c mod_autoindex_color PHP/5.1.6	Upgrade to PHP version 5.2.0 or later.
55	208.xx.xxx.xx	CVE-2008-2371	PHP 5 < 5.2.7 Multiple Vulnerabilities - heap-based buffer overflow	7.5	High	Heap-based buffer overflow in pcre_compile.c in the Perl-Compatible Regular Expression (PCRE) library 7.7 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a regular expression that begins with an option and contains multiple branches. PHP version 5.1.6 appears to be running on the remote host based on the following Server response header : Server: Apache/2.2.3 (Win32) DAV/2 mod_ssl/2.2.3 OpenSSL/0.9.8c mod_autoindex_color PHP/5.1.6	Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
56	208.xx.xxx.xx	CVE-2008-3658	PHP 5 < 5.2.7 Multiple Vulnerabilities - buffer overflow DoS	7.5	High	Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.2 before 5.2.6-r6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.	Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.
57	208.xx.xxx.xx	CVE-2008-5624	PHP 5 < 5.2.7 Multiple Vulnerabilities - bypass safe_mode restrictions	7.5	High	PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.	Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.
58	208.xx.xxx.xx	CVE-2008-5625	PHP 5 < 5.2.7 Multiple Vulnerabilities - write arbitrary files	7.5	High	PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.	Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on.

[Technician's Report Vulnerability Details]

No.	Affected IP Address	CVE Number/ Reference (*CVSS Severity Incomplete Approx)	Vulnerability	CVSS Score (version 2.0)	Severity Level	Vulnerability Details	Suggested Solution | Fix Special Notes
59	208.xx.xxx.xx	CVE-2008-5658	PHP 5 < 5.2.7 Multiple Vulnerabilities - Directory traversal vulnerability in the ZipArchive	7.5	High	Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.	Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was been removed from distribution because of a regression in that version that results in the 'magic_quotes_gpc' setting remaining off even if it was set to on. **Special Note:** Note to scan customer: Browsing of directories on web servers can lead to information disclosure or potential exploit. Due to increased risk to the cardholder data environment, please 1) justify the business need for this configuration to the ASV, or 2) confirm that it is disabled. Please consult your ASV if you have questions about this Special Note.

the advantage of insight

6922 W. Linebaugh Ave., Suite 101
Tampa, FL 33625
877.578.0215
www.securanceconsulting.com