Response to Request for Information:
Cyber-Security Assessment, Remediation, and Identity Protection, Monitoring and Restoration Services

Contact for RFP Response:

Paul Ashe
pashe@securanceconsulting.com
Office: 877.578.0215
Direct: 813.758.2532
Fax: 813.960.4946

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

Project Office:
Securance Consulting
6922 W. Linebaugh Avenue
Suite 101
Tampa, FL 33625
www.securanceconsulting.com
This proposal contains confidential material proprietary to Securance Consulting. The material, ideas and concepts contained herein are to be used solely and exclusively to evaluate the capabilities of Securance Consulting to provide assistance to the State of Florida (“the State”). This proposal does not constitute an agreement between Securance Consulting and the State. Any services Securance Consulting may provide to the State will be governed by the terms of a separate written agreement signed by both parties. All offers to provide professional services are valid for sixty (60) days.
September 3, 2015

Joel Atkinson
Associate Category Manager
Department of Management Services
Division of State Purchasing
4050 Esplanade Way, Suite 360
Tallahassee, Florida 2399-0950

Dear Joel,

I’d like to thank you for considering Securance Consulting as your IT security partner. We appreciate this opportunity to present our qualifications and approach to providing cyber security assessment services to Florida’s state agencies (collectively referred to as “the State”).

We are a firm of senior IT consultants passionate about helping organizations mitigate risks, establish effective controls and comply with regulatory requirements. Ours is a unique combination: “Big 4” expertise with the personal attention and hands-on executive involvement that only a small business can offer. We apply our knowledge, years of experience and industry-leading assessment tools to identify risks before they harm operations and business.

When it comes to achieving your IT objectives, selecting the right vendor is crucial. Our interest is in forging a long-term relationship with the State. We will attend to the State’s needs and goals throughout the assessment process, and will provide support throughout -- and after -- the remediation phase.

Again, thank you for including Securance in your evaluation process. Please review our qualifications, and do not hesitate to contact me with questions or comments.

I look forward to hearing from you.

Professional regards,

Paul Ashe, CPA, CISA, CISSP
President and Senior IT Consultant
Securance Consulting
Executive Summary

Securance Consulting is an IT audit firm dedicated to risk analysis, cyber security assessment and compliance testing. Founded in 2002 by a former “Big 4” consultant, we have been a leader in the information security industry for over thirteen years. We are privately owned, independent of affiliate firms, technology vendors and service providers. We pride ourselves on delivering objective assurance and reliable, untainted results.

Unlike larger firms that aim to do it all, we know our sweet spot. Our consultants have expertise on both sides of the aisle -- that is, in internal audit and IT -- but we focus on what we love and do best: information security. We will complement the skills of your in-house resources by providing specialized IT audits and security assessments, uncovering the risks that you need to address but are likely unaware of. Based on our experience helping government entities assess and improve their cyber security postures, we’re confident that we can develop solutions that align with the State’s objectives, priorities and needs.

Qualifications
Each member of our consulting practice has at least 15 years’ experience in information security and risk management. Our consultants participate in a rigorous continuing education program to stay ahead of emerging threats and regulatory compliance requirements. In addition, they maintain prestigious professional certifications and licenses, such as:

- Certified Information Systems Auditor - CISA
- Certified Information Systems Security Professional - CISSP
- Certified Internal Auditor - CIA
- Certified Information Security Manager - CISM
- Certified Public Accountant - CPA
- Certified Ethical Hacker - CEH
- GIAC Certified Incident Handler - GCIH
- Certified Business Continuity Professional - CBCP

Client Experience
Securance specializes in assessing technology risk and developing targeted, feasible remediation plans. We partner with internal auditors and IT staff to develop and execute audit plans and security assessment strategies. Our recent projects for government clients include:

- Atlanta Housing Authority - IT Security Audits
- Colorado Office of the State Auditor - IT Security Audits
- County of Fresno, California - IT Security Audit
- Dormitory Authority of the State of New York - IT Risk Assessment, Audit Plan and Cyber Security Audit
- Illinois State Board of Education - IT Risk and Security Assessment
- Louisville-Jefferson County Metro Government - Application Security and Compliance Review
- Maryland-National Park and Planning Commission - Network Vulnerability Assessments and IT General Controls Audit
- New York City Housing Authority - IT Security Assessments
- Orange County, Florida - IT Audit
- Pinellas County, Florida - IT Security Assessment and PCI-DSS Compliance Review
Executive Summary

Assessment Approach
Based on our understanding of the scope of services requested in the State’s Request for Information (RFI), we plan to deliver pre-incident assessment and consulting services in the following categories:
- Incident Response Agreement Development
- Information Security Assessments
- Security Incident Response Assessments
- Best Practice Recommendations for Information Security and Incident Response
- Guidance Relative to Regulatory Requirements
- Incident Response Plan Development
- Staff Training

The typical deliverables for each engagement will include:
- Audit work papers in electronic and hard copy
- Written analysis of findings and recommendations
- Technician’s report, if applicable, containing raw data extracts from utilized security tools
- Executive-level presentation of findings and recommendations, if applicable

We submit draft deliverables within one week of completing fieldwork.

Ongoing Support
Our knowledge and experience in government environments means we can provide the State with the expertise it requires. Once a Securance client, the State will be a client for life. Indeed, we look forward to a long-term partnership and will not turn our backs once our deliverables have been accepted. Rather, we will offer ongoing technical support and advice, free of charge, during and after the remediation phase.
Securance Consulting: Success Built on Results

Official Registered Name: Securance LLC

Dun & Bradstreet Number: 041637542

Primary SIC Numbers: 8721 - Accounting, Auditing, Bookkeeping

Secondary SIC Number: 7379 - Computer Related Services
8742 - Management Consulting Services
8748 - Business Consulting Services, NEC

Address: 6922 West Linebaugh Avenue, Suite 101, Tampa, FL 33625

Main Number (Toll-Free): 877.578.0215

Facsimile Number: 813.960.4946

Key Contact: Paul Ashe - President
877.578.0215
pashe@securanceconsulting.com

Firm History: Securance is a risk management firm that specializes in IT auditing, cyber security assessment and regulatory compliance consulting. Founded in 2002, we have been a leading provider of information security risk management services for over 13 years.
Related Experience

Organizations that have trusted Securance to provide similar services include:

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary of Scope</th>
<th>Client Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT Security Assessment and PCI Readiness Assessment</td>
<td>In 2013 and 2014, Securance performed an IT security assessment for a Florida county government. The purpose of the engagement was to evaluate IT security across key components of the technology environment. Our procedures included external and internal network vulnerability assessments and penetration tests; firewall and network device configuration analyses; application security assessments; social engineering; reviews of the Information Security Program, IT governance policies and technology asset management procedures; data center (physical) security reviews; and a PCI readiness assessment. We reassessed remediated items six months after completing our initial testing. Our deliverables included a comprehensive management report and an executive-level presentation of our findings and recommendations.</td>
<td>Client Name Confidential Florida Municipality</td>
</tr>
<tr>
<td>IT Security Assessments</td>
<td>In 2013, Securance performed an IT security assessment for the Housing Authority of the City of San Buenaventura. The engagement included assessments of external and internal network security; internal security applications and services; server, firewall and DMZ configuration reviews; denial-of-service and incident response procedures; document management procedures; change management policies; organizational structure and select IT processes.</td>
<td>Housing Authority of the City of San Buenaventura</td>
</tr>
<tr>
<td>IT Risk and Security Assessment</td>
<td>In 2014, an Illinois state agency engaged Securance to conduct an IT risk assessment and security review. Our objective was to identify IT process risks and technology-specific vulnerabilities, then formulate detailed remediation recommendations to improve cyber defenses and internal controls. Our review included assessments of IT governance, general controls, security architecture, and network and application security. We reviewed internal IT policies, standards and procedures; tested the operating effectiveness of in-scope IT processes; and performed vulnerability assessments.</td>
<td>Client Name Confidential Illinois State Agency</td>
</tr>
<tr>
<td>IT Audit</td>
<td>In 2014, one of Florida’s most populous counties engaged Securance to audit the County Comptroller’s IT environment. Our objective was to ensure that IT infrastructure was secure, that network hardware was configured appropriately, and that IT general controls were operating effectively. Our review included analyses of key IT processes, internal wireless network security, the configuration of the Internet-facing firewall, and compliance with HIPAA and the PCI Data Security Standards.</td>
<td>Client Name Confidential Florida Municipality</td>
</tr>
</tbody>
</table>
## Related Experience

<table>
<thead>
<tr>
<th>Project</th>
<th>Summary of Scope</th>
<th>Client Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Security Audit</td>
<td>In 2015, Securance conducted an IT risk assessment and developed a multi-year audit plan for the Dormitory Authority of the State of New York (DASNY). After reviewing our findings and recommendations, DASNY engaged Securance to perform a technical audit of its cyber security infrastructure. We conducted detailed external and internal vulnerability assessments; reviewed firewall configurations and the implementation of intrusion detection and prevention systems; and assessed the design and effectiveness of network security controls, including user access controls, virus and malware protection software, content filtering tools and email SPAM filters.</td>
<td>Dormitory Authority of the State of New York</td>
</tr>
<tr>
<td>IT Security and General Controls Assessment</td>
<td>In 2013, Securance conducted a network security and general controls assessment for an Oregon municipality. Our objectives were to identify technical vulnerabilities and to verify the operating effectiveness of select IT general controls. The engagement included vulnerability assessments of the external and internal IP networks; an assessment of the wireless network's configuration and security posture; an analysis of critical application security, with a focus on password configuration; a review of Active Directory configuration and audit policy settings; reviews of select IT general controls (mobile device management, business continuity and disaster recovery, and change and patch management); and a review of IT security policies and procedures.</td>
<td>Client Name Confidential Oregon Municipality</td>
</tr>
<tr>
<td>IT Security Audits</td>
<td>In 2014, Securance performed a risk-based vulnerability assessment, penetration test and technical information security assessment for a Colorado state agency. The scope of our review included evaluated external and internal network security, firewall configurations, enterprise and web-based application security, and user security awareness. We combined manual audit procedures with vulnerability assessment techniques to identify and analyze security risks within the agency's IT environment.</td>
<td>Client Name Confidential Colorado State Agency</td>
</tr>
<tr>
<td>Information Systems Risk Assessment and Network Security Review</td>
<td>Securance conducted an information systems risk assessment and network security review for the Kissimmee Utility Authority (KUA). Our objective was to determine if the policies and standards governing the management of KUA's technology environment were adequate to protect the security and integrity of its information assets. We reviewed the design and functionality of KUA's risk management framework, governance policies and key IT processes, including disaster recovery, change and patch management, user provisioning, physical access controls and database controls over enterprise systems. We also tested the external network, internal network and internal databases for vulnerabilities; reviewed internal LAN architecture; and analyzed the configuration of the Internet-facing firewall.</td>
<td>Kissimmee Utility Authority</td>
</tr>
</tbody>
</table>
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.

Pinellas County
315 Court Street - Clearwater, FL 33756

Mr. Jeff Rohrs, Business Technology Services Chief Technologist
Direct: (727) 453-3455 l email: jrohrs@pinellascounty.org l www.pinellascounty.org

- IT Security Assessment
- Payment Card Industry (PCI) Readiness Assessment

Orange County
201 South Rosalind Avenue - Orlando, FL 32801

Mr. David Hardison, Budget Administrator
Direct: (407) 836-7393 l email: Dave.Hardison@ocfl.net l www.ocfl.net

- IT Audit

Kissimmee Utility Authority
1701 W. Carroll Street - Kissimmee, FL 34741

Mr. Joe Hostetler, Vice President of Finance and Risk Management
Direct: (407) 933-7777 ext. 6200 l email: jhostetl@kua.com l www.kua.com

- Information Systems Risk Assessment
Service Capabilities

Execute, Analyze, REPORT and Improve

Securance provides a range of cyber security assessment services, including the following services listed in Section IV of the RFI:

**Category 1 - Pre-Incident Services:**
- Incident Response Agreements:
  - Provide consultative services relative to the development of incident response agreements.
- Assessments:
  - Evaluate current information security and incident response capabilities.
- Preparation:
  - Deliver guidance and recommendations regarding best practices and compliance requirements for cyber security and incident response programs.
- Developing Cyber Security Incident Response Plans:
  - Develop or help the State develop incident response plans aligned with industry standards, best practices and regulatory requirements.
- Training:
  - Develop or help the State develop staff training programs, from user security awareness to technical education programs.
Technical Methodologies

**IT Audit**

Our audit approach is unlike that of any other professional services or accounting firm. We focus on technology risk as it translates into business risk.

Our approach will focus on continuous assessment of the State’s IT controls. As we begin the audit process, we will work closely with Internal Audit Management to better understand key technology issues and changes in the organization’s IT environment.

We will leverage available resources in your IT and Internal Audit Departments -- teaming to eliminate unnecessary duplication of effort, to enhance quality and to maximize cost effectiveness. Securance Consulting’s continuous assessment of these factors will result in discussions with Management to determine what procedures should be performed during the audit, who should perform them and when they should be performed.

As a result, we will strategically focus our efforts on areas of high technology risk. Ultimately, our process will deliver assurance. Our audit results are objective. Through continuous communication throughout the process, we deliver a real-time view of technology risk, providing early warnings and no surprises.
Technical Methodologies

Co-Development Session
- Initial planning meeting:
- Team introductions
- Methodology discussion and clarification
- Project scope analysis
- Project timeline definition
- Risk matrix completion
- Audit guidelines to be followed
- Q-and-A discussion

Memo defines the project audit strategy and addresses the following areas:
- Planning meeting summary
- Client background
- Audit scope
- Technology under review
- Technology structure (i.e., 3-tier, 2-tier, etc.)
- IT control environment and internal control structure
- Deliverables

Audit Strategies Memo

Technical Memo & Internal Controls Documentation
Technical memo captures a summary of the IT environment, including:
- Applications
- Business processes being supported
- Host names and addresses
- Host platforms
- Application development method
- Access control solutions
- Management control solutions
- Telecommunication topology
Internal control documentation captures a summary of the current state of control throughout the IT environment, including:
- IT strategic planning in support of company objectives
- System development and program change management
- Business continuity
- Disaster recovery
- Remote access management
- Policies and procedures
- Logical and physical access
- Network controls
- System monitoring solutions

Review Program
Detailed listing of the procedures to be performed to ensure accurate value-added results:
- Team introductions
- Reviewed and approved by client
- Planning procedures
- Data and system access procedures
- Platform interrogation
- Technology-specific review steps
- Change procedures
- Test of identified controls
- Other technology issues identified
- Wrap-up procedures

Audit Program Execution
Our consultants use their experience, technology skill and a variety of commercial and proprietary tools to perform the procedures outlined in the review program.

Our process includes a structured set of eWorkpapers and an independent review to support our findings.

Our consultants use the review program as a guide and perform additional procedures, if necessary.

Executive Summary & Value Scorecard
The final project deliverable is an easy-read executive summary.

This report includes:
- Applications
- Brief background of the project
- Executive summary of findings and recommendations
- Technical summary of findings and recommendations
- Value scorecard - listing of business value provided by the engagement
CoBIT I COSO Objectives
IT controls should consider the overall governance framework to support the quality and integrity of information.

**Plan & Organize**
- **PO1** Define a Strategic Plan
- **PO2** Define the Information Architecture
- **PO3** Determine Technological Direction
- **PO4** Define the IT Processes, Organization & Relationships
- **PO5** Manage the IT Investment
- **PO6** Communicate Management Aims & Direction
- **PO7** Manage IT Human Resources
- **PO8** Manage Quality
- **PO9** Assess & Manage IT Risks

**Deliver & Support**
- **DS1** Define & Manage Service Levels
- **DS2** Manage Third-party Services
- **DS3** Manage Performance & Capacity
- **DS4** Ensure Continuous Service
- **DS5** Ensure Systems Security
- **DS6** Identify & Allocate Costs
- **DS7** Educate & Train Users
- **DS8** Manage Service Desk & Incidents
- **DS9** Manage the Configuration
- **DS10** Manage Problems
- **DS11** Manage Data
- **DS12** Manage the Physical Environment
- **DS13** Manage Operations

**Acquire & Implement**
- **AI1** Identify Automated Solutions
- **AI2** Acquire & Maintain Application Software
- **AI3** Acquire & Maintain Technology Infrastructure
- **AI4** Enable Operation & Use
- **AI5** Procure IT Resources
- **AI6** Manage Changes
- **AI7** Install & Accredit Solutions & Changes

**Monitor & Evaluate**
- **ME1** Monitor & Evaluate IT Performance
- **ME2** Monitor & Evaluate Internal Control
- **ME3** Ensure Compliance with External Requirements
- **ME4** Provide IT Governance
External and Internal 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.


Our methodology includes:

A) Information Gathering I Footprinting

- External Network Methodology:
  - 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.

- Internal Network Methodology:
  - 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) Planning the Attack

- External Network Methodology:
  - Business Resources
  - Domain Name Resources
  - Whois Database:
    - NSLookup, ARIN and DIG
  - Social Engineering Techniques and Guessing
  - Brute Force Attempts

- Internal Network Methodology:
  - 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.
- 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.

The Security 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
C) Vulnerability Testing (continued)

- 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 proceed 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.
Technical Methodologies

**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/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 | 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
- Httpprint
- 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
- Wininfo
- Winhex
- Wireshark
- Xscan
Project Management

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 State’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 State’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 State’s Project Manager
- Coordinate meetings between Securance and the State’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 State’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.
Information Sharing Security

Safeguards to Protect the Agency’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 Agency. 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 Agency’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 Agency’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 Agency’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.

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.
Staff Qualifications

Staff Biographies and Resumes

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 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 controls. 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, leads our audit and security teams. A former IT consultant for Ernst & Young, he translates his knowledge and experience into an effective, time- and budget-conscious project management style. He helps clients in every industry evaluate the security of their information systems, establish best practice controls and improve compliance with regulatory standards.

Paul's areas of expertise include securing networks, infrastructure components and application systems; evaluating and improving user security awareness; and optimizing internal policy structure to support organizational initiatives. He conducts vulnerability assessments, penetration tests and configuration reviews of various systems, platforms, network components and IP addressing schemes, as well as internal policy reviews and security controls assessments. Please see his complete resume on pages 24 and 25.

**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 frameworks and control standards to international, federal, state and industry-specific regulations. With over 30 years of IT experience, Chris has audited information security, managed project teams and established successful risk management programs for global corporations, small- to medium-sized businesses, and government entities. His expertise includes diverse application systems, network architecture schemes, platforms and compliance requirements. Please see his complete resume on pages 26 and 27.
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 | 27001 and NIST compliance, Chris has extensive experience with a variety of security frameworks, control standards and regulations. 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. Please see his complete resume on pages 28 and 29.

Martin Goss, Senior IT Security Consultant
CISA

With over 30 years of IT audit and security experience, Martin helps organizations implement, assess and maximize the benefits of secure IT systems and policies. His client list includes public and private sector entities in the United States and abroad. Please see his complete resume on pages 30 and 31.

James McDonald, Senior IT Security Consultant
CISSP, CISA, GCIH, CEH

James is a Senior IT Consultant with over 15 years’ experience identifying, analyzing and successfully combating IT threats. His expertise includes network, application and operating system security; incident response planning; policy and procedure development; and regulatory compliance. Please see his complete resume on pages 32 and 33.
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
- Mobile Device Management

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 helps leaders in every industry identify threats, optimize their internal security controls, and meet best practice standards. His recent projects include:

- Atlanta Housing Authority - IT Security Audit Services
- City of Madison - IT Security Assessment
- City of Tacoma - Cyber Security Vulnerability Assessment
- Colorado Office of the State Auditor - IT Security Audits
- Community Development Commission of the County of Los Angeles - IT Security Assessment
- County of Fresno - Information Systems Security Assessment
- Denny's Corporation - Vulnerability Assessments and Penetration Tests
- Dormitory Authority of the State of New York - Cyber Security Audit
- FirstMerit Corporation - IT Audit Services
- Hallmark Cards - Corporate VPN and Digital Website Vulnerability Assessments
- Henrico County - IT Security Assessments 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 Assessment
- Kao USA - Vulnerability Assessment and Penetration Test
- Louisville-Jefferson County Metro Government - Application Security and Compliance Review
- Lowe's - Vulnerability Assessment and Penetration Test
- Maryland-National Capital Park and Planning Commission - Network Vulnerability Assessments and IT General Controls Review
- Massachusetts Technology Collaborative - IT Security Audits
- New York City Housing Authority - External Network and Web-Application Security Assessments
- Ohio Public Employees Retirement System - IT and Network Security Assessment, Information Systems Risk Assessment and IT General Controls Review
- Pinellas County - IT Security Assessment and PCI-DSS Compliance Review
- Transocean - Penetration Test and Social Media Security Consulting Services
- University of Kentucky - Application Security and HIPAA Compliance Assessment

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 Auditor
- Certified Public Accountant (Florida)
- Certified Information Systems Security Professional (Pending)
- 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 Security 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 (GC²R) 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
Chris helps clients identify, analyze and remediate technology risks to meet internal objectives and regulatory standards. His recent projects include:

- Atlanta Housing Authority - IT Security Audits
- Cedar Falls Utilities - Network Security Risk Assessment
- Colorado Office of the State Auditor - IT Security Audits
- Community Coffee Company - Vulnerability Assessment and Penetration Test
- Dell MEDITECH Solutions Group - IT General Controls Audit of the MEDITECH Hosting Environment
- Dormitory Authority of the State of New York - Cyber Security Audit
- FirstMerit Bank - IT Audits
- Hallmark Cards - Corporate VPN and Digital Website Vulnerability Assessments
- Houston Community College - IT Audit
- Illinois State Board of Education - IT Risk Assessment
- Kissimmee Utility Authority - Information Systems Risk Assessment and Network Security Review
- Maryland-National Capital Park and Planning Commission - IT General Controls Audit
- Massachusetts Technology Collaborative - IT Security Assessment
- Ohio Public Employees Retirement System - IT and Network Security Assessment, Information Systems Risk Assessment and IT General Controls Review
- Oil States International - Application Security Audits
- Orange County Board of County Commissioners - IT Audit
- Pinellas County - IT Security Assessment
- Pioneer Electric Cooperative - IT Security Assessment and PCI Compliance Review
- Simpson Manufacturing Company - Enterprise IT Risk Assessment
- Teachers’ Retirement System of the State of Illinois - IT General Controls Review
- University of Kentucky - Application Security and HIPAA Compliance Assessment
- Waterfront Toronto - Network Security Assessments
- 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
- Master of Science - Management Information Systems
- Bachelor of Science - Computer Science for Business
Chris Cook, CISSP, CISA
Sr. IT Security Consultant

Subject matter expert with superior knowledge of NIST, ISO, CoBIT and other best practice standards. Significant experience enhancing infrastructure and controls to secure critical assets.

Overview
Chris Cook, a Senior IT Consultant with Securance for the last 9 years, has over 20 years’ experience in IT security, risk analysis and regulatory compliance. His expertise includes:

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

Experience: IT Risk Management

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 helps clients improve their security postures and establish best practice controls to mitigate known risks. His recent projects include:

- City of Richmond - Network Security Assessment
- Entergy Services Corporation - Vulnerability Assessment and Penetration Test
- First Financial Bank - IT Security Assessment
- Hallmark Cards - Corporate VPN and Digital Website Vulnerability Assessments
- Inter-American Development Bank - Extended Enterprise Mobile Security Assessment
- Kissimmee Utility Authority - Information Systems Risk Assessment and Network Security Review
- Orange County Sanitation District - IT Security Assessment
- Santee Cooper - IT Security Assessment
- Tacoma Water - Cybersecurity Assessment
- Transocean - Vulnerability Assessment and 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 | 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
Martin Goss, CISA  
Senior IT Security Consultant

30 years’ experience delivering solutions for IT management, project management, teambuilding and training. Exceptional problem resolution skills.

Overview
Senior IT Audit Consultant Martin Goss helps organizations identify objectives, establish deadlines, reduce costs and maximize the benefits of their IT systems and management guidelines. His expertise includes:

- Sarbanes-Oxley (SOX) Internal IT Auditing
- IT Risk Analysis and General Controls Auditing
- Policy and Procedure Development
- Infrastructure Design, Implementation and Installation
- IT and Business Process Documentation
- IT Management and Project Management
- ISO 9001 Quality Management Systems
- Regulatory Compliance Auditing for Domestic and Foreign Companies

Experience: IT Risk Management
Martin has helped countless organizations meet and exceed internal and compliance standards and improve their business and IT processes. Recent client projects include:

- Illinois State Board of Education - IT Risk Assessment and Security Review
- Inteliquent - IT General Controls Audit
- PoolCorp - Annual SOX IT Controls Review
- Milwaukee County - IT Risk Assessment for HIPAA Compliance
- Kingsway Insurance Company - SOX Reviews and IT Restructuring
- Kiewit Construction Omaha - IT Business Process Analysis and Documentation
- Hooker Furniture, Bradington & Young and Sam Moore Furniture - Annual Internal Reviews
- Tyco Industries, Allied Tube and Conduit Division - Internal Compliance Reviews
- Johnson Controls, Inc. - SOX Control Testing
- Allscripts Health Services - IT General Controls Audit; Compliance Software (“S-O-Comply”) Implementation
Technical Skills
- Network Architecture and Design
- Hardware Integration
- System Upgrading
- Telecommunications Integration
- Platforms - MS Windows; NT Server; UNIX; AS400; and Novell.
- Database and ERP Solutions - ERP; Oracle, SAP; JDE; Mapics; and PeopleSoft.
- Programs - MS Office; MS Visio; MS Project; MS Sharepoint; McAfee Virus Scan; Norton Anti-Virus; Powerway Quality Management Systems Software; Symantec Ghost; LAN I WAN; and CMS.

Education, Training and Certifications
- Certified Information Systems Auditor
- A + Certification
- PC Hardware Training
- Novell 3.1 and 4.11 Training
- Kendall College, Loyola University and Oakton Community College
James McDonald, CISSP, CISA, CEH, GCIH
Senior IT Security Consultant

Over 15 years’ experience analyzing and combating IT threats. Expertise in all facets of IT security, risk analysis and systems administration.

Overview
Senior IT Consultant James McDonald has been with Securance since 2010. With a deep background in IT security assessment and risk management, he is experienced in a wide range of consulting services. His expertise includes:

- Security Auditing
- IT Risk Analysis
- Vulnerability Assessments
- Penetration Tests
- Web-Application Testing
- Server Reviews
- Internet Security Assessments
- Application Security Assessments
- IT Security Policies & Procedures
- Incident Response, Disaster Recovery and Business Continuity Planning
- PCI, SOX, HIPAA and HITECH Compliance

Experience: IT Risk Management

Securance Consulting - Senior IT Consultant
- Helps clients in every industry identify, analyze and remediate security vulnerabilities and IT process risks.
- Recent clients include:
  - Louisville-Jefferson County Metro Government - Vulnerability Assessment and Penetration Test
  - Liberty Savings Bank - IT Security Assessment
  - Performance Software - IT Security Consulting Services

Major Retail Organization - Senior Information Security Analyst
- Responsible for penetration testing, vulnerability validation, web-application testing, e-discovery, computer and network forensics, and incident response.
- Deploys and maintains SIEM solutions, network file encryption programs and web-application firewalls in multiple environments.
- Key role in PCI compliance initiatives.

BayCare Health System - Network Security Analyst
- Responsible for daily security operations. Developed security policies and procedures. Team lead on multiple projects.
- Deployed and maintained security services, network devices, and intrusion detection and prevention systems.
- Tested web-application security. Worked with system developers and administrators to remediate areas of risk.
- Key roles in HIPAA, HITECH and PCI compliance audits and subsequent remediation programs.
Experience: Project-Specific (continued)

**APPTIS, Inc.** - Information Assurance Engineer, MacDill Air Force Base
- Analyzed threats based on information in open-source and intelligence reports. Deployed effective measures to combat threats. Created threat advisories.
- Analyzed network and system changes for potential effects on security.
- Established security regulations and directives.

**KForce, Inc.** - Security Analyst III
- Responsible for systems security, vulnerability and risk assessment, disaster recovery and business continuity planning, and SOX 404 internal controls.
- Designed effective SOX controls. Worked closely with business units and internal and external auditors to improve relevant controls and business processes. Conducted quarterly access control audits.
- Conducted quarterly security configuration audits (automated and manual testing) in a mixed HP-UNIX 11i, Redhat Linux and Windows environment.
- Developed, tested and improved security and incident response policies and procedures.

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
- Certified Ethical Hacker
- GIAC Certified Incident Handler
- Bachelor of Science - Management Information Systems
The Next Step

What to Expect

Qualifications – the team we proposed includes senior leadership from the firm. Our team leaders and staff are Certified IT Security Professionals with intimate knowledge of the technologies in your environment.

IT Security Expertise – as a firm of Senior IT Consultants, we intimately understand IT security and internal controls. Our methodology is designed around global best practices. We are experts already.

Sustained Improved Security – only the Securance approach includes a sustainable improved security posture solution. Our team will identify and share processes and improvements to current processes that will help improve the State’s security on an ongoing basis.

Experience – key members of our team of consultants are former “Big 4” IT consultants. In addition, our team has real-world experience that enables us to differentiate between “textbook” and real-world, practical security. Your reports will not contain recommendations that cannot be implemented in your environment.

High-Quality Deliverable – our Management Report is tailored to the various audiences that will receive it. The report contains an easy-to-read executive summary with no technical jargon. Yet, it also contains sufficient detail that your team of system administrators and engineers can implement our proven recommendations.

True Partnership – we are long-term partners with staying power. We will not simply leave when the assignment is over. We will be there to support the remediation and ensure the implementation of our recommendations is successful. When needed, we will roll up our sleeves and participate in the implementation. The State will become a Securance client for life. This means you can contact us for support or technical advice, free of charge, even when not under contract. That is the Securance definition of a partner!

It is easy to see why Securance should be the firm of choice!
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 State’s personnel will provide Securance consultants with all information requested to complete this engagement in a timely manner.

- The State’s Project Manager will hold meetings with the Securance Engagement Manager, as necessary, to assess the project’s progress.

- The State’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.

What’s Next for the State?

- Engage Securance Consulting today!

- Conduct a planning session.

- We’ll hit the ground running, with interviews scheduled in advance of our site visit and pre-defined client assistance requirements. We’ll adjust our schedules to ensure minimal disruption to your staff.

- Fast return on investment as you realize the benefits of engaging Securance Consulting.
<table>
<thead>
<tr>
<th>Contractor</th>
<th>Securance LLC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule</td>
<td>General Purpose Commercial Information Technology Equipment, Software and Services Schedule 70</td>
</tr>
<tr>
<td>Contract Number</td>
<td>GS – 35F – 0583X</td>
</tr>
<tr>
<td>Special Item Number</td>
<td>132-51 – Information Technology (IT) Professional Services</td>
</tr>
<tr>
<td></td>
<td>FPDS Code D310: IT Backup and Security Services</td>
</tr>
<tr>
<td></td>
<td>FPDS Code D324: IT and Telecom - Business Continuity</td>
</tr>
<tr>
<td></td>
<td>FPDS Code D399: Other Information Technology Services, Not Elsewhere Classified</td>
</tr>
<tr>
<td>Business Size / Status</td>
<td>Small Business</td>
</tr>
</tbody>
</table>

**Price List current as of May 2, 2014**

Products and ordering information in this Authorized Information Technology Schedule Pricelist are also available on the GSA Advantage! System at [www.gsaadvantage.gov](http://www.gsaadvantage.gov)

---

**Contract Administrator**

Paul Ashe  
apshe@securanceconsulting.com  
Office: 877.578.0215  
Direct: 813.758.2532  
Fax: 813.960.4946

**Corporate Office:**

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

INFORMATION FOR ORDERING ACTIVITIES APPLICABLE TO ALL SPECIAL ITEM NUMBERS.......................................................................................................................... 2

SPECIAL NOTICE TO AGENCIES: Small Business Participation............................................. 2

TERMS AND CONDITIONS APPLICABLE TO INFORMATION TECHNOLOGY (IT) PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-51) AND IDENTITY ACCESS MANAGEMENT PROFESSIONAL SERVICES (SPECIAL ITEM NUMBER 132-60F) ........ 12

USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS.............................................................................................................. 17

PREAMBLE ...................................................................................................................................... 17

COMMITMENT ............................................................................................................................ 17

BEST VALUE BLANKET PURCHASE AGREEMENT FEDERAL SUPPLY SCHEDULE........... 18

Securance LLC BLANKET PURCHASE AGREEMENT......................................................... 19

BASIC GUIDELINES FOR USING “CONTRACTOR TEAM ARRANGEMENTS”............... 21
INFORMATION FOR ORDERING ACTIVITIES
APPLICABLE TO ALL SPECIAL ITEM NUMBERS

SPECIAL NOTICE TO AGENCIES: SMALL BUSINESS PARTICIPATION

SBA strongly supports the participation of small business concerns in the Federal Acquisition Service. To enhance Small Business Participation SBA policy allows agencies to include in their procurement base and goals, the dollar value of orders expected to be placed against the Federal Supply Schedules, and to report accomplishments against these goals.

For orders exceeding the micropurchase threshold, FAR 8.404 requires agencies to consider the catalogs/pricelists of at least three schedule contractors or consider reasonably available information by using the GSA Advantage! on-line shopping service (www.gsaadvantage.gov). The catalogs/pricelists, GSA Advantage!™ and the Federal Acquisition Service Home Page (www.gsa.gov/fas) contain information on a broad array of products and services offered by small business concerns.

This information should be used as a tool to assist ordering activities in meeting or exceeding established small business goals. It should also be used as a tool to assist in including small, small disadvantaged, and women-owned small businesses among those considered when selecting pricelists for a best value determination.

For orders exceeding the micropurchase threshold, customers are to give preference to small business concerns when two or more items at the same delivered price will satisfy their requirement.

1. GEOGRAPHIC SCOPE OF CONTRACT

Domestic delivery is delivery within the 48 contiguous states, Alaska, Hawaii, Puerto Rico, Washington, DC, and U.S. Territories. Domestic delivery also includes a port or consolidation point, within the aforementioned areas, for orders received from overseas activities.

Overseas delivery is delivery to points outside of the 48 contiguous states, Washington, DC, Alaska, Hawaii, Puerto Rico, and U.S. Territories.

Offerors are requested to check one of the following boxes:

[ ] The Geographic Scope of Contract will be domestic and overseas delivery.

[ ] The Geographic Scope of Contract will be overseas delivery only.

[ x ] The Geographic Scope of Contract will be domestic delivery only.

For Special Item Number 132-53 Wireless Services ONLY, if awarded, list the limited geographic coverage area:

__________________________________________________________________________________

__________________________________________________________________________________
2. CONTRACTOR’S ORDERING ADDRESS AND PAYMENT INFORMATION

Securance LLC
6922 Linebaugh Avenue
Suite – 101
Tampa, Florida 33625

Contractor must accept the credit card for payments equal to or less than the micro-purchase for oral or written orders under this contract. The Contractor and the ordering agency may agree to use the credit card for dollar amounts over the micro-purchase threshold (See GSAR 552.232-79 Payment by Credit Card). In addition, bank account information for wire transfer payments will be shown on the invoice.

The following telephone number(s) can be used by ordering activities to obtain technical and/or ordering assistance:

877-578-0215

When Authorized Dealers are allowed by the Contractor to bill ordering activities and accept payment, the order and/or payment must be in the name of the Contractor, in care of the Authorized Dealer.

3. LIABILITY FOR INJURY OR DAMAGE

The Contractor shall not be liable for any injury to ordering activity personnel or damage to ordering activity property arising from the use of equipment maintained by the Contractor, unless such injury or damage is due to the fault or negligence of the Contractor.

4. STATISTICAL DATA FOR GOVERNMENT ORDERING OFFICE COMPLETION OF STANDARD FORM 279

Block 9: G. Order/Modification Under Federal Schedule Contract
Block 16: Data Universal Numbering System (DUNS) Number: 041637542
Block 30: Type of Contractor: _B_____________________
   A. Small Disadvantaged Business
   B. Other Small Business
   C. Large Business
   G. Other Nonprofit Organization
   L. Foreign Contractor

Block 31: Woman-Owned Small Business - ____no__________ **Yes or No**
Block 37: Contractor’s Taxpayer Identification Number (TIN): ___030392503_____
Block 40: Veteran Owned Small Business (VOSB): ___No____________________
       A. Service Disabled Veteran Owned Small Business
       B. Other Veteran Owned Small Business

4a. CAGE Code: _1XTH7____________
4b. Contractor has registered with the Central Contractor Registration Database.
5. FOB DESTINATION

6. DELIVERY SCHEDULE

a. TIME OF DELIVERY: The Contractor shall deliver to destination within the number of calendar days after receipt of order (ARO), as set forth below:

<table>
<thead>
<tr>
<th>SPECIAL ITEM NUMBER</th>
<th>DELIVERY TIME (Days ARO)</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>132-51</em>____________</td>
<td>_As negotiated with Customer on PO _____ Days</td>
</tr>
<tr>
<td>____________________</td>
<td>_______________ Days</td>
</tr>
</tbody>
</table>

b. URGENT REQUIREMENTS: When the Federal Supply Schedule contract delivery period does not meet the bona fide urgent delivery requirements of an ordering activity, ordering activities are encouraged, if time permits, to contact the Contractor for the purpose of obtaining accelerated delivery. The Contractor shall reply to the inquiry within 3 workdays after receipt. (Telephonic replies shall be confirmed by the Contractor in writing.) If the Contractor offers an accelerated delivery time acceptable to the ordering activity, any order(s) placed pursuant to the agreed upon accelerated delivery time frame shall be delivered within this shorter delivery time and in accordance with all other terms and conditions of the contract.

c. i. SIN 132-54 and SIN 132-55, ACCELERATED SERVICE DELIVERY (7 calendar days or less): the time required for COMSATCOM services to be available after order award. Under Accelerated Service Task Orders, service acceptance testing, unless otherwise required by the satellite provider or host nation, shall be deferred until Ordering Activity operations permit.

   ii. SIN 132-54 and SIN 132-55, TIME-CRITICAL DELIVERY (4 hours or less): the time required for COMSATCOM services to be available after order award. Under Time-Critical Task Orders, service acceptance testing unless otherwise required by the satellite provider or host nation shall be deferred until Ordering Activity operations permit. Time-Critical Delivery shall be predicated on the availability of COMSATCOM transponded capacity (contracted bandwidth and power, pre-arranged Host Nation Agreements, frequency clearance) or COMSATCOM subscription services (bandwidth, terminals, network resources, etc.).

   iii. For SIN 132-54 and SIN 132-55, EXTENDED SERVICE DELIVERY TIMES: the time required under extenuating circumstances for COMSATCOM services to be available after order award. Such extenuating circumstances may include extended time required for host nation agreements or landing rights, or other time intensive service delivery requirements as defined in the individual requirement. Any such extended delivery times will be negotiated between the Ordering Activity and Contractor.
7. DISCOUNTS

Prices shown are NET Prices; Basic Discounts have been deducted.

a. Prompt Payment: ___% - ___ days from receipt of invoice or date of acceptance, whichever is later.
b. Quantity: None
c. Dollar Volume: None
d. Government Educational Institutions – Offered same discount as other Government Customers.
e. Other: None

8. TRADE AGREEMENTS ACT OF 1979, as amended:

All items are U.S. made end products, designated country end products, Caribbean Basin country end products, Canadian end products, or Mexican end products as defined in the Trade Agreements Act of 1979, as amended.

9. STATEMENT CONCERNING AVAILABILITY OF EXPORT PACKING

10. Small Requirements: The minimum dollar value of orders to be issued is $100.00.

11. MAXIMUM ORDER (All dollar amounts are exclusive of any discount for prompt payment.)

a. The Maximum Order value for the following Special Item Numbers (SINs) is $500,000:

   Special Item Number 132-51 - Information Technology Professional Services

12. ORDERING PROCEDURES FOR FEDERAL SUPPLY SCHEDULE CONTRACTS

Ordering activities shall use the ordering procedures of Federal Acquisition Regulation (FAR) 8.405 when placing an order or establishing a BPA for supplies or services. These procedures apply to all schedules.

a. FAR 8.405-1 Ordering procedures for supplies, and services not requiring a statement of work.
b. FAR 8.405-2 Ordering procedures for services requiring a statement of work.

13. FEDERAL INFORMATION TECHNOLOGY/TELECOMMUNICATION STANDARDS REQUIREMENTS

Ordering activities acquiring products from this Schedule must comply with the provisions of the Federal Standards Program, as appropriate (reference: NIST Federal Standards Index). Inquiries to determine whether or not specific products listed herein comply with Federal Information Processing Standards (FIPS) or Federal Telecommunication Standards (FED-STDS), which are cited by ordering activities, shall be responded to promptly by the Contractor.
13.1. FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATIONS (FIPS PUBS)

Information Technology products under this Schedule that do not conform to Federal Information Processing Standards (FIPS) should not be acquired unless a waiver has been granted in accordance with the applicable "FIPS Publication." Federal Information Processing Standards Publications (FIPS PUBS) are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Information concerning their availability and applicability should be obtained from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, Virginia 22161. FIPS PUBS include voluntary standards when these are adopted for Federal use. Individual orders for FIPS PUBS should be referred to the NTIS Sales Office, and orders for subscription service should be referred to the NTIS Subscription Officer, both at the above address, or telephone number (703) 487-4650.

13.2 FEDERAL TELECOMMUNICATION STANDARDS (FED-STDs)

Telecommunication products under this Schedule that do not conform to Federal Telecommunication Standards (FED-STDs) should not be acquired unless a waiver has been granted in accordance with the applicable "FED-STD." Federal Telecommunication Standards are issued by the U.S. Department of Commerce, National Institute of Standards and Technology (NIST), pursuant to National Security Act. Ordering information and information concerning the availability of FED-STDs should be obtained from the GSA, Federal Acquisition Service, Specification Section, 470 East L’Enfant Plaza, Suite 8100, SW, Washington, DC 20407, telephone number (202)619-8925. Please include a self-addressed mailing label when requesting information by mail. Information concerning their applicability can be obtained by writing or calling the U.S. Department of Commerce, National Institute of Standards and Technology, Gaithersburg, MD 20899, telephone number (301)975-2833.

14. CONTRACTOR TASKS / SPECIAL REQUIREMENTS (C-FSS-370) (NOV 2003)

(a) Security Clearances: The Contractor may be required to obtain/possess varying levels of security clearances in the performance of orders issued under this contract. All costs associated with obtaining/possessing such security clearances should be factored into the price offered under the Multiple Award Schedule.

(b) Travel: The Contractor may be required to travel in performance of orders issued under this contract. Allowable travel and per diem charges are governed by Pub. L. 99-234 and FAR Part 31, and are reimbursable by the ordering agency or can be priced as a fixed price item on orders placed under the Multiple Award Schedule. Travel in performance of a task order will only be reimbursable to the extent authorized by the ordering agency. The Industrial Funding Fee does NOT apply to travel and per diem charges.

(c) Certifications, Licenses and Accreditations: As a commercial practice, the Contractor may be required to obtain/possess any variety of certifications, licenses and accreditations for specific FSC/service code classifications offered. All costs associated with obtaining/possessing such certifications, licenses and accreditations should be factored into the price offered under the Multiple Award Schedule program.

(d) Insurance: As a commercial practice, the Contractor may be required to obtain/possess insurance coverage for specific FSC/service code classifications offered. All costs
associated with obtaining/possessing such insurance should be factored into the price offered under the Multiple Award Schedule program.

(e) Personnel: The Contractor may be required to provide key personnel, resumes or skill category descriptions in the performance of orders issued under this contract. Ordering activities may require agency approval of additions or replacements to key personnel.

(f) Organizational Conflicts of Interest: Where there may be an organizational conflict of interest as determined by the ordering agency, the Contractor’s participation in such order may be restricted in accordance with FAR Part 9.5.

(g) Documentation/Standards: The Contractor may be requested to provide products or services in accordance with rules, regulations, OMB orders, standards and documentation as specified by the agency’s order.

(h) Data/Deliverable Requirements: Any required data/deliverables at the ordering level will be as specified or negotiated in the agency’s order.

(i) Government-Furnished Property: As specified by the agency’s order, the Government may provide property, equipment, materials or resources as necessary.

(j) Availability of Funds: Many Government agencies’ operating funds are appropriated for a specific fiscal year. Funds may not be presently available for any orders placed under the contract or any option year. The Government’s obligation on orders placed under this contract is contingent upon the availability of appropriated funds from which payment for ordering purposes can be made. No legal liability on the part of the Government for any payment may arise until funds are available to the ordering Contracting Officer.

(k) Overtime: For professional services, the labor rates in the Schedule should not vary by virtue of the Contractor having worked overtime. For services applicable to the Service Contract Act (as identified in the Schedule), the labor rates in the Schedule will vary as governed by labor laws (usually assessed a time and a half of the labor rate).

15. CONTRACT ADMINISTRATION FOR ORDERING ACTIVITIES

Any ordering activity, with respect to any one or more delivery orders placed by it under this contract, may exercise the same rights of termination as might the GSA Contracting Officer under provisions of FAR 52.212-4, paragraphs (l) Termination for the ordering activity’s convenience, and (m) Termination for Cause (See 52.212-4)

16. GSA ADVANTAGE!

GSA Advantage! is an on-line, interactive electronic information and ordering system that provides on-line access to vendors’ schedule prices with ordering information. GSA Advantage! will allow the user to perform various searches across all contracts including, but not limited to:

(1) Manufacturer;
(2) Manufacturer’s Part Number;
(3) Product categories.

Agencies can browse GSA Advantage! by accessing the Internet World Wide Web utilizing a browser (ex.: NetScape). The Internet address is http://www.gsaadvantage.gov
17. PURCHASE OF OPEN MARKET ITEMS
NOTE: Open Market Items are also known as incidental items, noncontract items, non-Schedule items, and items not on a Federal Supply Schedule contract. Ordering Activities procuring open market items must follow FAR 8.402(f).

For administrative convenience, an ordering activity contracting officer may add items not on the Federal Supply Multiple Award Schedule (MAS) -- referred to as open market items -- to a Federal Supply Schedule blanket purchase agreement (BPA) or an individual task or delivery order, only if-

1. All applicable acquisition regulations pertaining to the purchase of the items not on the Federal Supply Schedule have been followed (e.g., publicizing (Part 5), competition requirements (Part 6), acquisition of commercial items (Part 12), contracting methods (Parts 13, 14, and 15), and small business programs (Part 19));
2. The ordering activity contracting officer has determined the price for the items not on the Federal Supply Schedule is fair and reasonable;
3. The items are clearly labeled on the order as items not on the Federal Supply Schedule; and
4. All clauses applicable to items not on the Federal Supply Schedule are included in the order.

18. CONTRACTOR COMMITMENTS, WARRANTIES AND REPRESENTATIONS
a. For the purpose of this contract, commitments, warranties and representations include, in addition to those agreed to for the entire schedule contract:
   1. Time of delivery/installation quotations for individual orders;
   2. Technical representations and/or warranties of products concerning performance, total system performance and/or configuration, physical, design and/or functional characteristics and capabilities of a product/equipment/service/software package submitted in response to requirements which result in orders under this schedule contract.
   3. Any representations and/or warranties concerning the products made in any literature, description, drawings and/or specifications furnished by the Contractor.

b. The above is not intended to encompass items not currently covered by the GSA Schedule contract.

c. The maintenance/repair service provided is the standard commercial terms and conditions for the type of products and/or services awarded.

19. OVERSEAS ACTIVITIES
The terms and conditions of this contract shall apply to all orders for installation, maintenance and repair of equipment in areas listed in the pricelist outside the 48 contiguous states and the District of Columbia, except as indicated below:

None
Upon request of the Contractor, the ordering activity may provide the Contractor with logistics support, as available, in accordance with all applicable ordering activity regulations. Such ordering activity support will be provided on a reimbursable basis, and will only be provided to the Contractor's technical personnel whose services are exclusively required for the fulfillment of the terms and conditions of this contract.

20. BLANKET PURCHASE AGREEMENTS (BPAs)

The use of BPAs under any schedule contract to fill repetitive needs for supplies or services is allowable. BPAs may be established with one or more schedule contractors. The number of BPAs to be established is within the discretion of the ordering activity establishing the BPA and should be based on a strategy that is expected to maximize the effectiveness of the BPA(s). Ordering activities shall follow FAR 8.405-3 when creating and implementing BPA(s).

21. CONTRACTOR TEAM ARRANGEMENTS

Contractors participating in contractor team arrangements must abide by all terms and conditions of their respective contracts. This includes compliance with Clauses 552.238-74, Industrial Funding Fee and Sales Reporting, i.e., each contractor (team member) must report sales and remit the IFF for all products and services provided under its individual contract.

22. INSTALLATION, DEINSTALLATION, REINSTALLATION

The Davis-Bacon Act (40 U.S.C. 276a-276a-7) provides that contracts in excess of $2,000 to which the United States or the District of Columbia is a party for construction, alteration, or repair (including painting and decorating) of public buildings or public works with the United States, shall contain a clause that no laborer or mechanic employed directly upon the site of the work shall receive less than the prevailing wage rates as determined by the Secretary of Labor. The requirements of the Davis-Bacon Act do not apply if the construction work is incidental to the furnishing of supplies, equipment, or services. For example, the requirements do not apply to simple installation or alteration of a public building or public work that is incidental to furnishing supplies or equipment under a supply contract. However, if the construction, alteration or repair is segregable and exceeds $2,000, then the requirements of the Davis-Bacon Act applies.

The ordering activity issuing the task order against this contract will be responsible for proper administration and enforcement of the Federal labor standards covered by the Davis-Bacon Act. The proper Davis-Bacon wage determination will be issued by the ordering activity at the time a request for quotations is made for applicable construction classified installation, deinstallation, and reinstallation services under SIN 132-8 or 132-9.

23. SECTION 508 COMPLIANCE

I certify that in accordance with 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d), FAR 39.2, and the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology (EIT) Accessibility Standards (36 CFR 1194) General Services Administration (GSA), that all IT hardware/software/services are 508 compliant:

Yes _______  No ___X____
The offeror is required to submit with its offer a designated area on its website that outlines the Voluntary Product Accessibility Template (VPAT) or equivalent qualification, which ultimately becomes the Government Product Accessibility Template (GPAT). Section 508 compliance information on the supplies and services in this contract are available at the following website address (URL): www.securanceconsulting.com.

24. PRIME CONTRACTOR ORDERING FROM FEDERAL SUPPLY SCHEDULES

Prime Contractors (on cost reimbursement contracts) placing orders under Federal Supply Schedules, on behalf of an ordering activity, shall follow the terms of the applicable schedule and authorization and include with each order—

(a) A copy of the authorization from the ordering activity with whom the contractor has the prime contract (unless a copy was previously furnished to the Federal Supply Schedule contractor); and

(b) The following statement:

This order is placed under written authorization from _______ dated _______. In the event of any inconsistency between the terms and conditions of this order and those of your Federal Supply Schedule contract, the latter will govern.

25. INSURANCE—WORK ON A GOVERNMENT INSTALLATION (JAN 1997)(FAR 52.228-5)

(a) The Contractor shall, at its own expense, provide and maintain during the entire performance of this contract, at least the kinds and minimum amounts of insurance required in the Schedule or elsewhere in the contract.

(b) Before commencing work under this contract, the Contractor shall notify the Contracting Officer in writing that the required insurance has been obtained. The policies evidencing required insurance shall contain an endorsement to the effect that any cancellation or any material change adversely affecting the Government's interest shall not be effective—

(1) For such period as the laws of the State in which this contract is to be performed prescribe; or

(2) Until 30 days after the insurer or the Contractor gives written notice to the Contracting Officer, whichever period is longer.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work on a Government installation and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The Contractor shall maintain a copy of all subcontractors' proofs of required insurance, and shall make copies available to the Contracting Officer upon request.

26. SOFTWARE INTEROPERABILITY

Offerors are encouraged to identify within their software items any component interfaces that support open standard interoperability. An item's interface may be identified as interoperable on the basis of participation in a Government agency-sponsored program or in an independent organization program. Interfaces may be identified by reference to an interface registered in the component registry located at http://www.core.gov.
27. ADVANCE PAYMENTS

A payment under this contract to provide a service or deliver an article for the United States Government may not be more than the value of the service already provided or the article already delivered. Advance or pre-payment is not authorized or allowed under this contract.

(31 U.S.C. 3324)
1. SCOPE
   a. The prices, terms and conditions stated under Special Item Number 132-51 Information Technology Professional Services apply exclusively to IT/IAM Professional Services within the scope of this Information Technology Schedule.
   b. The Contractor shall provide services at the Contractor’s facility and/or at the ordering activity location, as agreed to by the Contractor and the ordering activity.

2. PERFORMANCE INCENTIVES  I-FSS-60 Performance Incentives (April 2000)
   a. Performance incentives may be agreed upon between the Contractor and the ordering activity on individual fixed price orders or Blanket Purchase Agreements under this contract.
   b. The ordering activity must establish a maximum performance incentive price for these services and/or total solutions on individual orders or Blanket Purchase Agreements.
   c. Incentives should be designed to relate results achieved by the contractor to specified targets. To the maximum extent practicable, ordering activities shall consider establishing incentives where performance is critical to the ordering activity's mission and incentives are likely to motivate the contractor. Incentives shall be based on objectively measurable tasks.

3. ORDER
   a. Agencies may use written orders, EDI orders, blanket purchase agreements, individual purchase orders, or task orders for ordering services under this contract. Blanket Purchase Agreements shall not extend beyond the end of the contract period; all services and delivery shall be made and the contract terms and conditions shall continue in effect until the completion of the order. Orders for tasks which extend beyond the fiscal year for which funds are available shall include FAR 52.232-19 (Deviation – May 2003) Availability of Funds for the Next Fiscal Year. The purchase order shall specify the availability of funds and the period for which funds are available.
   b. All task orders are subject to the terms and conditions of the contract. In the event of conflict between a task order and the contract, the contract will take precedence.

4. PERFORMANCE OF SERVICES
   a. The Contractor shall commence performance of services on the date agreed to by the Contractor and the ordering activity.
   b. The Contractor agrees to render services only during normal working hours, unless otherwise agreed to by the Contractor and the ordering activity.
c. The ordering activity should include the criteria for satisfactory completion for each task in the Statement of Work or Delivery Order. Services shall be completed in a good and workmanlike manner.

d. Any Contractor travel required in the performance of IT/IAM Services must comply with the Federal Travel Regulation or Joint Travel Regulations, as applicable, in effect on the date(s) the travel is performed. Established Federal Government per diem rates will apply to all Contractor travel. Contractors cannot use GSA city pair contracts.

5. STOP-WORK ORDER (FAR 52.242-15) (AUG 1989)

a. The Contracting Officer may, at any time, by written order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this contract for a period of 90 days after the order is delivered to the Contractor, and for any further period to which the parties may agree. The order shall be specifically identified as a stop-work order issued under this clause. Upon receipt of the order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the order during the period of work stoppage. Within a period of 90 days after a stop-work is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, the Contracting Officer shall either-

   (1) Cancel the stop-work order; or
   (2) Terminate the work covered by the order as provided in the Default, or the Termination for Convenience of the Government, clause of this contract.

b. If a stop-work order issued under this clause is canceled or the period of the order or any extension thereof expires, the Contractor shall resume work. The Contracting Officer shall make an equitable adjustment in the delivery schedule or contract price, or both, and the contract shall be modified, in writing, accordingly, if-

   (1) The stop-work order results in an increase in the time required for, or in the Contractor's cost properly allocable to, the performance of any part of this contract; and
   (2) The Contractor asserts its right to the adjustment within 30 days after the end of the period of work stoppage; provided, that, if the Contracting Officer decides the facts justify the action, the Contracting Officer may receive and act upon the claim submitted at any time before final payment under this contract.

c. If a stop-work order is not canceled and the work covered by the order is terminated for the convenience of the Government, the Contracting Officer shall allow reasonable costs resulting from the stop-work order in arriving at the termination settlement.

d. If a stop-work order is not canceled and the work covered by the order is terminated for default, the Contracting Officer shall allow, by equitable adjustment or otherwise, reasonable costs resulting from the stop-work order.

6. INSPECTION OF SERVICES

7. RESPONSIBILITIES OF THE CONTRACTOR
The Contractor shall comply with all laws, ordinances, and regulations (Federal, State, City, or otherwise) covering work of this character. If the end product of a task order is software, then FAR 52.227-14 (Dec 2007) Rights in Data – General, may apply.

8. RESPONSIBILITIES OF THE ORDERING ACTIVITY
Subject to security regulations, the ordering activity shall permit Contractor access to all facilities necessary to perform the requisite IT/IAM Professional Services.

9. INDEPENDENT CONTRACTOR
All IT/IAM Professional Services performed by the Contractor under the terms of this contract shall be as an independent Contractor, and not as an agent or employee of the ordering activity.

10. ORGANIZATIONAL CONFLICTS OF INTEREST
a. Definitions.

“Contractor” means the person, firm, unincorporated association, joint venture, partnership, or corporation that is a party to this contract.

“Contractor and its affiliates” and “Contractor or its affiliates” refers to the Contractor, its chief executives, directors, officers, subsidiaries, affiliates, subcontractors at any tier, and consultants and any joint venture involving the Contractor, any entity into or with which the Contractor subsequently merges or affiliates, or any other successor or assignee of the Contractor.

An “Organizational conflict of interest” exists when the nature of the work to be performed under a proposed ordering activity contract, without some restriction on ordering activities by the Contractor and its affiliates, may either (i) result in an unfair competitive advantage to the Contractor or its affiliates or (ii) impair the Contractor’s or its affiliates’ objectivity in performing contract work.

b. To avoid an organizational or financial conflict of interest and to avoid prejudicing the best interests of the ordering activity, ordering activities may place restrictions on the Contractors, its affiliates, chief executives, directors, subsidiaries and subcontractors at any tier when placing orders against schedule contracts. Such restrictions shall be consistent with FAR 9.505 and shall be designed to avoid, neutralize, or mitigate organizational conflicts of interest that might otherwise exist in situations related to individual orders placed against the schedule contract. Examples of situations, which may require restrictions, are provided at FAR 9.508.
11. INVOICES
The Contractor, upon completion of the work ordered, shall submit invoices for IT/IAM Professional services. Progress payments may be authorized by the ordering activity on individual orders if appropriate. Progress payments shall be based upon completion of defined milestones or interim products. Invoices shall be submitted monthly for recurring services performed during the preceding month.

12. PAYMENTS
For firm-fixed price orders the ordering activity shall pay the Contractor, upon submission of proper invoices or vouchers, the prices stipulated in this contract for service rendered and accepted. Progress payments shall be made only when authorized by the order. For time-and-materials orders, the Payments under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to time-and-materials orders placed under this contract. For labor-hour orders, the Payment under Time-and-Materials and Labor-Hour Contracts at FAR 52.212-4 (MAR 2009) (ALTERNATE I – OCT 2008) (DEVIATION I – FEB 2007) applies to labor-hour orders placed under this contract. 52.216-31 (Feb 2007) Time-and-Materials/Labor-Hour Proposal Requirements—Commercial Item Acquisition As prescribed in 16.601(e)(3), insert the following provision:

a. The Government contemplates award of a Time-and-Materials or Labor-Hour type of contract resulting from this solicitation.
b. The offeror must specify fixed hourly rates in its offer that include wages, overhead, general and administrative expenses, and profit. The offeror must specify whether the fixed hourly rate for each labor category applies to labor performed by—
   (1) The offeror;
   (2) Subcontractors; and/or
   (3) Divisions, subsidiaries, or affiliates of the offeror under a common control.

13. RESUMES
Resumes shall be provided to the GSA Contracting Officer or the user ordering activity upon request.

14. INCIDENTAL SUPPORT COSTS
Incidental support costs are available outside the scope of this contract. The costs will be negotiated separately with the ordering activity in accordance with the guidelines set forth in the FAR.

15. APPROVAL OF SUBCONTRACTS
The ordering activity may require that the Contractor receive, from the ordering activity's Contracting Officer, written consent before placing any subcontract for furnishing any of the work called for in a task order.
16. DESCRIPTION OF IT/IAM PROFESSIONAL SERVICES AND PRICING

Sr. IT Security Consultant

- Demonstrate advanced understanding of business processes, internal control risk management, IT controls and related standards
- Identify and evaluate complex business and technology risks, internal controls which mitigate risks, and related opportunities for internal control improvement
- Understand complex business and information technology management processes
- Execute advanced services and supervise staff in delivering basic services
- Assist in the selection and tailoring of approaches, methods and tools to support service offering or industry projects
- Understand clients' business environment and basic risk management approaches
- Demonstrate a general knowledge of market trends, competitor activities, Securance Consulting products and service lines
- Actively participate in decision making with engagement management and seek to understand the broader impact of current decisions
- Generate innovative ideas and challenge the status quo
- Build and nurture positive working relationships with clients with the intention to exceed client expectations
- Facilitate use of technology–based tools or methodologies to review, design and/or implement products and services
- Identify opportunities to improve engagement profitability
- Participate in and actively support mentoring relationships within practice

Qualifications

- 3+ system security, controls, or information management experience
- BA/BS in information technology, business administration, or related field preferred
- CISSP, CISM, or CISA certification a plus
- Prior Big 4 or other consulting experience desired
- Prior business development, marketing, or sales experience
- Excellent verbal and written communication
- Industry experiences in financial services, high–tech, and /or healthcare preferred
- Willingness to travel

$114.85 Per Hour

Minimum /General Experience: Required to have 10+ years experience

Minimum Education: Bachelor’s Degree or equivalent experience

Certifications include: CISA, CISSP, CBCP, GIAC, MCSE, & SANS

Must have minimum # of CPE hours required by their Certification.
USA COMMITMENT TO PROMOTE SMALL BUSINESS PARTICIPATION PROCUREMENT PROGRAMS

PREAMBLE

(Name of Company) provides commercial products and services to ordering activities. We are committed to promoting participation of small, small disadvantaged and women-owned small businesses in our contracts. We pledge to provide opportunities to the small business community through reselling opportunities, mentor-protégé programs, joint ventures, teaming arrangements, and subcontracting.

COMMITMENT

To actively seek and partner with small businesses.

To identify, qualify, mentor and develop small, small disadvantaged and women-owned small businesses by purchasing from these businesses whenever practical.

To develop and promote company policy initiatives that demonstrate our support for awarding contracts and subcontracts to small business concerns.

To undertake significant efforts to determine the potential of small, small disadvantaged and women-owned small business to supply products and services to our company.

To insure procurement opportunities are designed to permit the maximum possible participation of small, small disadvantaged, and women-owned small businesses.

To attend business opportunity workshops, minority business enterprise seminars, trade fairs, procurement conferences, etc., to identify and increase small businesses with whom to partner.

To publicize in our marketing publications our interest in meeting small businesses that may be interested in subcontracting opportunities.

We signify our commitment to work in partnership with small, small disadvantaged and women-owned small businesses to promote and increase their participation in ordering activity contracts. To accelerate potential opportunities please contact

Paul Ashe  
877.578.0215  
pashe@securanceconsulting.com

Stephanie Shipman  
877.578.0215  
sshipman@securanceconsulting.com

Ernie Hopkins  
877.578.0215  
ehopkins2@securanceconsulting.com
BEST VALUE
BLANKET PURCHASE AGREEMENT
FEDERAL SUPPLY SCHEDULE

(Insert Customer Name)

In the spirit of the Federal Acquisition Streamlining Act (ordering activity) and (Contractor) enter into a cooperative agreement to further reduce the administrative costs of acquiring commercial items from the General Services Administration (GSA) Federal Supply Schedule Contract(s) ____________________.

Federal Supply Schedule contract BPAs eliminate contracting and open market costs such as: search for sources; the development of technical documents, solicitations and the evaluation of offers. Teaming Arrangements are permitted with Federal Supply Schedule Contractors in accordance with Federal Acquisition Regulation (FAR) 9.6.

This BPA will further decrease costs, reduce paperwork, and save time by eliminating the need for repetitive, individual purchases from the schedule contract. The end result is to create a purchasing mechanism for the ordering activity that works better and costs less.

Signatures

<table>
<thead>
<tr>
<th>Ordering Activity</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securance LLC</td>
<td>Date</td>
</tr>
</tbody>
</table>
Securance LLC

BLANKET PURCHASE AGREEMENT

Pursuant to GSA Federal Supply Schedule Contract Number(s)____________, Blanket Purchase Agreements, the Contractor agrees to the following terms of a Blanket Purchase Agreement (BPA) EXCLUSIVELY WITH (ordering activity):

(1) The following contract items can be ordered under this BPA. All orders placed against this BPA are subject to the terms and conditions of the contract, except as noted below:

<table>
<thead>
<tr>
<th>MODEL NUMBER/PART NUMBER</th>
<th>*SPECIAL BPA DISCOUNT/PRICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>______________________</td>
<td>__________________________</td>
</tr>
<tr>
<td>______________________</td>
<td>__________________________</td>
</tr>
<tr>
<td>______________________</td>
<td>__________________________</td>
</tr>
</tbody>
</table>

(2) Delivery:

<table>
<thead>
<tr>
<th>DESTINATION</th>
<th>DELIVERY SCHEDULES / DATES</th>
</tr>
</thead>
<tbody>
<tr>
<td>____________</td>
<td>__________________________</td>
</tr>
<tr>
<td>____________</td>
<td>__________________________</td>
</tr>
<tr>
<td>____________</td>
<td>__________________________</td>
</tr>
</tbody>
</table>

(3) The ordering activity estimates, but does not guarantee, that the volume of purchases through this agreement will be _______________________.

(4) This BPA does not obligate any funds.

(5) This BPA expires on _______________ or at the end of the contract period, whichever is earlier.

(6) The following office(s) is hereby authorized to place orders under this BPA:

<table>
<thead>
<tr>
<th>OFFICE</th>
<th>POINT OF CONTACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securance LLC</td>
<td>Paul Ashe</td>
</tr>
<tr>
<td>6922 Linebaugh Avenue Suite – 101</td>
<td>Stephanie Shipman</td>
</tr>
<tr>
<td>Tampa, Florida 33625</td>
<td>Ernest Hopkins</td>
</tr>
</tbody>
</table>

(7) Orders will be placed against this BPA via Electronic Data Interchange (EDI), FAX, or paper.

(8) Unless otherwise agreed to, all deliveries under this BPA must be accompanied by delivery tickets or sales slips that must contain the following information as a minimum:

(a) Name of Contractor;
(b) Contract Number;

(c) BPA Number;

(d) Model Number or National Stock Number (NSN);

(e) Purchase Order Number;

(f) Date of Purchase;

(g) Quantity, Unit Price, and Extension of Each Item (unit prices and extensions need not be shown when incompatible with the use of automated systems; provided, that the invoice is itemized to show the information); and

(h) Date of Shipment.

(9) The requirements of a proper invoice are specified in the Federal Supply Schedule contract. Invoices will be submitted to the address specified within the purchase order transmission issued against this BPA.

(10) The terms and conditions included in this BPA apply to all purchases made pursuant to it. In the event of an inconsistency between the provisions of this BPA and the Contractor’s invoice, the provisions of this BPA will take precedence.

**************************************************************************************************

************************************************************

************************************************************
BASIC GUIDELINES FOR USING
“CONTRACTOR TEAM ARRANGEMENTS”

Federal Supply Schedule Contractors may use “Contractor Team Arrangements” (see FAR 9.6) to provide solutions when responding to a ordering activity requirements.

These Team Arrangements can be included under a Blanket Purchase Agreement (BPA). BPAs are permitted under all Federal Supply Schedule contracts.

Orders under a Team Arrangement are subject to terms and conditions or the Federal Supply Schedule Contract.

Participation in a Team Arrangement is limited to Federal Supply Schedule Contractors.

Customers should refer to FAR 9.6 for specific details on Team Arrangements.

Here is a general outline on how it works:

- The customer identifies their requirements.
- Federal Supply Schedule Contractors may individually meet the customers needs, or -
- Federal Supply Schedule Contractors may individually submit a Schedules “Team Solution” to meet the customer’s requirement.
- Customers make a best value selection.
Appendix B
Securance Consulting is an information technology consulting firm dedicated to information security, technology risk analysis and regulatory compliance testing. Founded in 2002 by a former Ernst & Young consultant, we combine “Big 4” expertise with the personal attention and hands-on executive involvement that only a small business can offer.

**What Sets Us Apart**

- **Focus.** Technology risk management and information security are our specialities. They’re all that we do, and they’re what we do best.
- **Experience.** Our consultants’ expertise bridges the gap between internal audit and IT. We apply our knowledge of the latest technologies, standards and compliance requirements to meet business objectives.
- **Commitment.** We take the time to learn what a risk or vulnerability means for your technologies and the enterprise as a whole. Our deliverables include customized, actionable recommendations -- not textbook controls.
- **Efficiency.** We deliver draft reports within one week of completing fieldwork.

**Past Performance**

**Public Sector**

- **Colorado Office of the State Auditor** - IT Security Audits
- **Illinois State Board of Education** - IT Risk and Security Assessment
- **Louisville-Jefferson County Metro Government** - IT Audit Services
- **Milwaukee County** - HIPAA Privacy and Security Rule Risk Assessment
- **Orange County** - IT General Controls Audit
- **Pinellas County** - IT Security Assessment and PCI-DSS Compliance Review
- **University of Kentucky** - Application Security and HIPAA Compliance Review

**Private Sector**

- **Covidien** - IT Audit Services
- **Del Monte** - SOX Compliance Testing
- **DELL MEDITECH Solutions Group** - IT General Controls Audit of the MEDITECH Hosting Environment
- **Denny’s Corporation** - Vulnerability Assessments and Penetration Tests
- **FirstMerit Corporation** - IT Audit Services
- **General Mills** - IT Risk Matrix
- **Hallmark Cards** - Corporate VPN and Digital Website Vulnerability Assessments
- **Lowe’s** - Vulnerability Assessment and Penetration Test
- **Transocean** - Penetration Test and Social Media Security Consulting
- **World Fuel Services** - IT Risk Matrix and Penetration Assessment

**Core Competencies**

- Internal Audit Outsourcing and Co-Sourcing
- Information Technology (IT) Audits and Risk Assessments
- IT Policy and Procedure Review and Redesign
- IT Security Assessments
- Vulnerability Assessments and Penetration Tests
- Regulatory Compliance Testing
- Business Process Review, Redesign and Automation
- Business Continuity and Disaster Recovery Planning

**GSA Contracts**

**Schedule 70**

- Contract #GS-35F-0583X
- SIN 132 51 - IT Professional Services

**Schedule 520**

- Contract #GS-23F-0076X
- SIN 520 17 - Risk Assessment and Mitigation Services
- SIN 520 18 - Independent Risk Analysis
- SIN 520 8 - Complementary Audit Services

**Company Data**

- **DUNS** 041637542
- **Cage Code** 1XTH7
- Self-Certified SDB
- Certified MBE

**Sales Contact**

Dennis Harden, GSA Program Manager
T.: 877.578.0215 ext. 229 | dharden@securanceconsulting.com
Appendix C
NETWORK SECURITY REPORT
SECTION I: EXECUTIVE SUMMARY
  Introduction and Scope ........................................................................................................3
  Findings and Technical Vulnerability Legend ......................................................................5
  Summary of Findings ...........................................................................................................6
  Conclusion ..........................................................................................................................13

SECTION II: NETWORK SECURITY ASSESSMENT REPORT
  Background ..........................................................................................................................14
  Specific Objectives and Detailed Scope .............................................................................15
  Approach and Methodology ...............................................................................................16
  Findings and Recommendations .........................................................................................17
    Select IT Controls ...........................................................................................................17
    External Network Vulnerability Assessment ..................................................................19
    Internal Network Vulnerability Assessment ....................................................................28

SECTION III: SECURANCE VALUE
  Securance Value ................................................................................................................48
INTRODUCTION AND SCOPE
During February 2014, Securance Consulting conducted a Network Security Assessment for ABC Corporation (herein ABC). The overall objective of the engagement was to identify technology specific vulnerabilities, IT process related risks, and documented pathways for breaching the security of the Corporation’s network. The scope of the engagement included an assessment of the following:

- 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.

We designed an approach and applied our IT Governance, IT Security Policy and Procedure Review, Vulnerability Assessment, Network Device, Server Review, Wireless Network and Active Directory Review methodologies to ensure a comprehensive capture and review of the IT risks and technical vulnerabilities that existed within ABC’s in-scope technologies. The approach combined the use of manual audit techniques and the use of commercial and proprietary security tools designed to identify vulnerabilities in ABC’s external and internal networks. Our procedures included:

On-site interviews with key ABC IT personnel;
- Review of IT policies and procedures;
- Review of online and print configuration settings;
- Review of manuals, reference materials and Best Practice security guides;
- Network foot printing – Researching public information on the target, including technical listings (e.g., ARIN WHOIS, DNS Lookup, etc.) and public information (e.g., newsgroups, search engines, Weblogs, etc.);
Provided for:

ABC CORPORATION

- Scanning – Utilizing automated tools to identify specific systems and services, software and operating system version levels, hardware devices, firewall configurations and other information; and

- Enumeration – Identifying specific vulnerabilities and avenues of attack through both automated and manual means.

We did not perform any privilege escalation or exploitation of the identified vulnerabilities in an attempt to gain access to a system or compromise accounts/services. The tools utilized and our procedures, including the timing of our fieldwork, were configured and conducted to eliminate the possibility of any disruption to ABC’s Information Technology (IT) infrastructure.
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 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 to ABC’s IT network and network devices, and our conclusion regarding the security posture of the in-scope technologies and IT processes.

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.

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 eight (8) 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.
Internal Internet Protocol (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:

No. 4: Internal IP Network Vulnerability Assessment – We performed a detailed scan against five (5) internal IP address blocks and identified thirty-eight (38) high and two hundred and ninety-three (293) medium-priority vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated network breach. The charts on page ten (10) provide 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. 5: Database Vulnerability Assessments – We performed a detailed scan against three (3) production databases and identified two (2) critical and fifteen (15) medium-priority vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated network breach. The chart on page eleven (11) 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. 6: Use of MS SQL Server “sa” Account – During the security testing of the database environment, we were informed that the software development team at ABC has used this account to connect applications to backend MS SQL server databases. The practice of using the “sa” account to connect an application to a database is considered a poor software development technique. In addition, it significantly decreases the security posture of the technology organization. This practice also means that the “sa” account password is widely known within the development team and, perhaps, other technology professionals.

No. 7: Wireless Access Points – We identified three (3) wireless access point SSIDs that belong to and are managed by ABC. The access points SSIDs are “comdevcom,” “tops,” and “tvsm.” The “tops” and “tvsm” access points appear to be managed by departments and are not configured with adequate security. To the extent that a specific department requires wireless access, it should leverage the organization’s wireless network “comdevcom” and adhere to the level of security implemented on the “comdevcom” network.
No. 8: Wireless Network “comdevcom” Encryption – The level of security and data encryption implemented on the “comdevcom” wireless network is WAP2-Personal. This is considered mid-level encryption and should be increased. We recommend that ABC implement a higher level of encryption to protect the data that is being transmitted over the wireless network. At a minimum, we recommend the use of WAP2-Enterprise.

No. 9: Wireless Network “comdevcom” Device Management – We identified four (4) Cisco access points with the SSID of “comdevcom.” Two of these access points appear to be configured to allow channel hopping. In addition, all four (4) of these devices must be individually managed, increasing the likelihood of a misconfiguration that could expose the internal network to a security breach. We recommend an upgrade to an enterprise wireless appliance that can be centrally managed, operate as a seamless wireless network and provide improved security.

No. 10: Active Directory (AD) Domain Account Policies – Per review of the AD domain account password configurations, we identified configuration settings that do not meet best practice recommended settings and increase the risk of unauthorized users gaining access to system resources and data. Specifically, we noted the following risks:

- Password history is not maintained – users can reuse passwords indefinitely;
- Password complexity is not enabled – non-complex passwords are easy to guess by unauthorized users;
- The account lockout threshold is set to zero (0) – this setting indicates the number of failed logon attempts before user accounts are locked out. A value of “0” allows an unlimited number of failed logon attempts;
- Account lockout duration has not been configured – this indicates the amount of time an account will remain locked out when the lockout threshold is exceeded. The current configuration does not lockout accounts;
- The AD “Administrator” account and “Guest” account have not been renamed – Default accounts are typically the first target of an unauthorized user attempting to gain access to system resources and data. The “Administrator” account has escalated system privileges, creating a higher level of risk; and
- The ability to prevent transfer of passwords in clear text is disabled, allowing passwords to be transferred within the network in clear text. This compromises the security of network passwords.

We recommend that ABC modify the AD domain account policies to best practice security configurations. Combined, the above deficiencies significantly increase the risk of unauthorized users gaining access to system resources or data.
No. 11: Active Directory User Account Analysis – Per review of user accounts settings, we identified user accounts that should be deleted from the server and other user account configuration deficiencies that should be modified. A summary of the findings is presented in the details of this report and a detailed listing of the specific user accounts that need removal has been provided to the system administrator via the technician’s report. We recommend these deficiencies be reviewed and remediated.

Remainder of this page left blank intentionally.
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.
Internal Network Unique System Vulnerabilities

- **Identified twenty-three (23) high vulnerabilities including, but not limited to:**
  - Multiple vulnerabilities that allow arbitrary code to be uploaded to remote hosts.
  - Multiple Open SSH vulnerabilities, which can expose sensitive information.
  - Multiple Apache vulnerabilities, which can lead to access control bypass attacks.
  - Privileged access escalation and remote code execution vulnerabilities.

- **Identified forty-three (43) medium vulnerabilities including, but not limited to:**
  - Multiple denial of service (DoS) attacks.
  - Multiple SSL and SSH vulnerabilities, which can lead to information exposure.
  - Inadequate security over Guest and Local user accounts.
  - Remote desktop protocol vulnerabilities.
  - Multiple vulnerabilities that lead to information disclosure.
Database Unique System Vulnerabilities

- Identified one (1) Critical Vulnerability, including:
  - An SQL Server 2005 Service pack 3 is missing.

- Identified five (5) Medium Vulnerabilities, including:
  - Mixed authentication use.
  - Two (2) vulnerabilities related to multiple stored procedures.
  - The C2 audit mode is not configured.
  - Guest user accounts exist on the databases.
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.
BACKGROUND
During February 2014, Securance Consulting conducted a Network Security Assessment for ABC Corporation (ABC). The overall objective of the engagement was to identify technology specific vulnerabilities, IT process related risks, and documented pathways of breaching the security of ABC’s network. The scope of this engagement included an assessment of the following:

• 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 controls and to identify technical vulnerabilities within ABC’s internal and external networks. The scope of the review included an assessment of the following processes, networks, systems, and technologies:

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

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

• Firewall Configuration Review:
  o Checkpoint ASA Firewall

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

• Database Security Assessment:
  o DATABASE 01
  o DATABASE 02
  o DATABASE 03

• Internal Wireless Network

• Active Directory System
APPROACH AND METHODOLOGY
To achieve the objectives of this engagement, within the defined scope, we performed our 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 ABC Information Technology personnel;
• Review of available policies and procedures;
• On-site physical walkthrough of the data center; and
• Access point configuration review:
  o 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 information technology (IT) policies and procedures, general IT administration and physical security, are submitted to assist in improving the security posture of ABC’s information technology environment.

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 Corporation’s (ABC) 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
Provided for:

ABC CORPORATION

- 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 Device, 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 user access, removing user access and changing a user’s 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. Finding and technical vulnerability legend is provided on page five (5).
Management’s Response:

Remainder of this page left blank intentionally.
External Network Unique Vulnerabilities

Critical: 1
High: 3

External Network Total Vulnerabilities

Critical: 1
High: 7

Remainder of this page left blank intentionally.
## Threat Level | Server | Vulnerability Description | Fix / Recommendation
--- | --- | --- | ---
Critical | 2xx.xxx.xxx.xxx | **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.securityfocus.com/bid/1811/discuss); [http://www.osvdb.org/285](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.xxx, 2xx.xxx.xxx.xxx | **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.  


--- | --- | --- | ---
High | 2xx.xxx.xxx.xxx, 2xx.xxx.xxx.xxx, 2xx.xxx.xxx.xxx | **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.
No. 3: Firewall Rule Configuration Vulnerabilities

We performed a detailed scan against one (1) perimeter firewall and identified and identified nine (9) high and seven (7) medium risk vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an externally originated firewall breach.

The chart on the following page provides a snapshot of the vulnerabilities identified, prioritized by level of severity. The pages that follow summarize unique vulnerabilities and the recommended solutions. In many cases, the recommended solution requires a modification of the firewall rule.

**Risk:**
ABC’s external network is at risk of being compromised by an attacker, due to the firewall configuration. Depending upon the type of breach executed, the network or systems on the network 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 high and medium risk 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. Finding and technical vulnerability legend is provided on page five (5).

**Management’s Response:**
Firewall Configuration Vulnerabilities

- High: 9
- Medium: 5

Remainder of this page left blank intentionally.
<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Server</th>
<th>Vulnerability Description</th>
<th>Fix</th>
<th>Recommendation</th>
</tr>
</thead>
</table>
| High        | 2xx.xxx.xxx.xxx   | **Risky Microsoft services can enter your network** – Your network is accessible from the outside using the following Microsoft services:  
  - netbios_gm  
  - netbios_ns  
  These services provide file and printer sharing for Microsoft Windows machines. They are a vector for worms and viruses, and they potentially expose your network and data.  
  *REF: NIST Publication 800-41* |     | Add the following rule as one of the first rules:  
  - From Any to Any with service NBT:DROP |
| High        | 2xx.xxx.xxx.xxx   | **“Any” service between internal networks** – The * (“Any”) service is allowed to cross between your internal network segments. Allowing “Any” service to cross between different network segments is risky since the “Any” service includes many vulnerable services. It means that the different network segments are not properly separated from each other. The risk is highest if the “Any” service is allowed to cross a DMZ network into other network segments: If a DMZ server becomes infected with a worm or virus, the infection may spread to other parts of your network.  
  *REF: None* |     | Review all the rules that allow traffic with the *service, and limit them to those services you actually require. |
| High        | 2xx.xxx.xxx.xxx   | **“Any” service can exit your network** – Machines on your network can access the outside using the * (“Any”) service. Allowing “Any” service to exit your network is extremely risky since the “Any” service includes many vulnerable services. The largest threat is that of Trojan horses contacting their controller, followed by unintended information leakage, and spreading of malicious code like viruses and worms.  
  *REF: None* |     | Review all the rules that allow outbound traffic with the *service, and limit them to those services you actually require. |

**Remainder of findings eliminated for brevity of sample report.**
### Threat Level | Server | Vulnerability Description | Fix | Recommendation
--- | --- | --- | --- | ---
Medium | 2xx.xxx.xxx.xxx | "From somewhere to Any allow Any service" rules – we identified 2 rules that have the form “From A to Any with service Any: PASS.” These rules may be more open than necessary. Allowing access to all destinations gives access to all hosts within the perimeter (including the firewall itself) and all Internet hosts. The specific rules are provided in the technician’s report | Review the rules below to determine which destinations are necessary, and modify the rules according to the narrowest actual security needs. | • xxxxxx_access_in(1) • xxxxxx_access_out(2)  

Medium | 2xx.xxx.xxx.xxx | “Any” service from internal networks to DMZ – the *(“Any”)* service is allowed to cross from your internal network segments into the DMZ. Allowing "Any" service to cross into a DMZ network from other segments is risky since the "Any" service includes many vulnerable services. It means that the different network segments are not properly separated from each other. If an internal computer becomes infected with a worm or virus, the infection may spread into other parts of your network. | Review all the rules that allow traffic from the your internal network into the DMZ with the * service, and limit them to those services that are required. |  

Medium | 2xx.xxx.xxx.xxx | Over 256 IP addresses can be reached by SMTP – over 256 IP addresses on your network are reachable from the outside using the smtp service. This is a risk because smtp (Email) should only reach to your public mail servers. Email is a vector for viruses and worms. | Review the rules that allow smtp access from the outside and limit their destinations to your public mail servers. |  

Remainder of findings eliminated for brevity of sample report.
Firewall Optimization

Our analysis of the firewall rules identified opportunities to optimize the firewall rule configurations and improve rule set management. Specifically, we identified two (2) rules that can be deleted, five (5) rules that can be consolidated, twenty-eight (28) rules that are not logged and thirty-three (33) rules without remarks.

Risk:
The use of redundant or unnecessary rules compromises the performance of the firewall.

Recommendation:
We recommend that ABC perform the following activities:
• Review and remove the unused, covered, redundant and disabled rules;
• Perform rule consolidation; and
• Review all rules where logging is not enabled or remarked, to determine appropriateness of setting.
FINDINGS AND RECOMMENDATIONS – INTERNAL NETWORK VULNERABILITY ASSESSMENT

The following recommendations, which resulted from the internal network vulnerability assessment, are submitted to assist in improving the security posture of the targeted segments of ABC’s internal network.

No. 4: Internal Network Vulnerabilities

We performed a detailed scan against five (5) internal IP address blocks and identified thirty-eight (38) high and two hundred and ninety-eight (298) medium risk vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an internally originated network breach.

The charts on the following page 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 or system upgrade. Note that all high and medium findings relate to server and VPN IP ranges. All findings related to user VLAN ranges are considered low risk and are only provided in the technician’s report.

Risk:
ABC’s internal 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 other department systems.

Recommendation:
We strongly recommend that ABC immediately address all high risk 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. Finding and technical vulnerability legend provided on page forty-two (42).
Management’s Response:
Provided for:

ABC CORPORATION

Internal Network Unique Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td></td>
<td></td>
</tr>
<tr>
<td>43</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internal Network Total Vulnerabilities

<table>
<thead>
<tr>
<th></th>
<th>High</th>
<th>Medium</th>
</tr>
</thead>
<tbody>
<tr>
<td>38</td>
<td></td>
<td></td>
</tr>
<tr>
<td>293</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Remainder of this page left blank intentionally.
**Threat Level** | **Server** | **Vulnerability Description** | **Fix | Recommendation**
---|---|---|---
High | 10.xx.x.xx | **EMC Replication Manager ired.exe RunProgram Message Handling Arbitrary Command Execution** - The remote host is running EMC Replication Manager Client Control Daemon. The remote version of this software is affected by a remote command execution vulnerability.

As a result, arbitrary code can be executed on the remote host. An unauthenticated attacker can exploit this flaw by sending a specially crafted packet to the remote host. Successful exploitation would result in remote code execution with the privileges of the daemon itself.

*REF: OSVDB:56864* | Install the EMC Replication Manager patch as described on the EMC support website. The following EMC products resolve this issue:
- EMC Replication Manager 5.0 SP6 Security Patch
- EMC Replication Manager 5.1 SP6 Security Patch
- EMC Replication Manager 5.2 Security Patch
- EMC Replication Manager 5.2 SP1 Security Patch

High | 10.xx.x.xx | **PostgreSQL to_ascii() Function Remote Overflows** - According to its version number, the PostgreSQL server listening on this port is vulnerable to two buffer overflows in the to_ascii() function, which may allow an attacker who can query the remote database to execute arbitrary code, subject to the privileges under which the service operates.

*REF: CVE-2003-0901* | Upgrade to PostgreSQL 7.3.4 or newer.

High | 10.xx.x.xx  
• 10.xx.x.xx  
• 10.xx.x.xx  
• 10.xx.x.xx  
• 10.xx.x.xx  
• 10.xx.x.xxx  
• 10.xx.x.xxx  
• 10.xx.x.xxx | **Symantec Backup Exec for Windows Multiple Vulnerabilities** - The remote host is running a version of VERITAS Backup Exec Agent that is affected by multiple authentication bypass issues. It is possible to bypass authentication in the remote backup agent. An attacker can exploit these issues to manage the backup agent or to execute commands with high privileges.

*REF: CVE-2008-5407* | Apply the appropriate hotfix referenced in the vendor advisory.

Remainder of findings eliminated for brevity of sample report.
<table>
<thead>
<tr>
<th>Threat Level</th>
<th>Server</th>
<th>Vulnerability Description</th>
<th>Fix</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>10.xx.x.xx</td>
<td><strong>NTP ntpd Mode 7 Error Response Packet Loop Remote DoS</strong> - The version of ntpd running on the remote host has a denial of service vulnerability. It responds to mode 7 error packets with its own mode 7 error packets. A remote attacker could exploit this by sending a mode 7 error response with a spoofed IP header, setting the source and destination IP addresses to the IP address of the target. This would cause ntpd to respond to itself endlessly, consuming excessive amounts of CPU, resulting in a denial of service.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>10.xx.x.xxx</td>
<td><strong>LDAP NULL BASE Search Access</strong> - The remote LDAP server may disclose sensitive information. The remote LDAP server supports search requests with a null, or empty, base object. This allows information to be retrieved without any prior knowledge of the directory structure. Coupled with a NULL BIND, an anonymous user may be able to query your LDAP server using a tool such as 'LdapMiner'.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>10.xx.x.xx</td>
<td><strong>SSL Anonymous Cipher Suites Supported</strong> - The remote host supports the use of anonymous SSL ciphers. While this enables an administrator to set up a service that encrypts traffic without having to generate and configure SSL certificates, it offers no way to verify the remote host's identity and renders the service vulnerable to a man-in-the-middle attack. Note: This is considerably easier to exploit if the attacker is on the same physical network.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Upgrade to NTP 4.2.4p8 or later.*

*If the remote LDAP server supports a version of the LDAP protocol before v3, consider whether to disable NULL BASE queries on your LDAP server.*

*Reconfigure the affected application if possible to avoid use of weak ciphers.*

*Remainder of findings eliminated for brevity of sample report.*
FINDINGS AND RECOMMENDATIONS – DATABASE VULNERABILITY ASSESSMENT

The following recommendations, which resulted from the database vulnerability assessment, are submitted to assist in improving the security posture of the targeted databases.

No. 5: Database Vulnerability Assessments

We performed a detailed scan against three (3) databases and identified one (1) critical and fifteen (15) medium risk vulnerabilities. The scan results revealed technical vulnerabilities that increase the likelihood of an internally originated database breach.

The charts on the following page 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.

Risk:
The selected databases are at risk of being compromised by an attacker. Depending upon the type of breach executed, systems could be rendered unresponsive, and data could be compromised.

Recommendation:
We strongly recommend that ABC immediately address all critical risk 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. Finding and technical vulnerability legend provided on page forty-two (42).

Management’s Response:
Database Unique Vulnerabilities

Critical: 1
Medium: 5

Database Total Vulnerabilities

Critical: 2
Medium: 15

Remainder of this page left blank intentionally.
## Provided for:
ABC CORPORATION

### Priority | Database | Vulnerability Description | Fix | Recommendation
---|---|---|---|---
**Critical**
- DATABASE 01
- DATABASE 02
**SQL Server 2005 – Servicepack 3 is missing** – SQL Server 2005- Servicepack 3 is missing. The service pack is designed to address<br>
*REF: None*
- Install Servicepack 3 for SQL Server 2005.

**Medium**
- DATABASE 03
- DATABASE 01
- DATABASE 02
**Multiple stored procedures** – There appears to be an excessive number of stored procedures on each of the databases. Stored procedures assist in achieving a consistent implementation of logic across applications. The SQL statements and logic needed to perform a commonly performed task can be designed, coded, and tested once in a stored procedure. Each application needing to perform that task can then simply execute the stored procedure. Coding business logic into a single stored procedure also offers a single point of control for ensuring that business rules are correctly enforced. If access to execute stored procedures is not adequately restricted, the risk of database and data corruption increases. Specifically, we identified the following number of stored procedures on each database:
  - DATABASE 02: 53
  - DATABASE 03: 55
  - DATABASE 01: 53

*REF: None*
- We recommend ABC review all stored procedures on the tested databases for appropriateness. If stored procedure is not used for a specific business purpose, we recommend removing or disabling the stored procedures.

- DATABASE 03
- DATABASE 01
- DATABASE 02
**Guest user exists** – Guest user account exist on the server. Guest user accounts are typically the first and easiest targets.

*REF: None*
- Disable or remove guest user accounts.

*Remainder of findings eliminated for brevity of sample report.*
No. 6: Use of MS SQL Server “sa” Account

ABC Corporation’s (ABC) database environment primarily consists of MS SQL server. This database technology relies on the system administrator, “sa,” account to be managed. The “sa” account is considered the owner of the database and, as such, can be used to execute any function against the database. During the security testing of the database environment, we were informed that the software development team at ABC has used this account to connect applications to backend MS SQL server databases. The practice of using the “sa” account to connect an application to a database is considered a poor software development technique. In addition, it significantly decreases the security posture of the technology organization. This practice also means that the “sa” account password is widely known within the development team and perhaps by other technology professionals.

Risk:
With the default database administrator account, anyone with access and knowledge of the “sa” account password could perform any function against the database system, including completely deleting the database, deleting or modifying critical database tables, or adjusting the data within a database system.

Recommendation:
Due to the wide use of the “sa” account in the environment, it is impractical to immediately address this risk properly. However, we recommend undertaking a project to identify all internally developed applications that use the “sa” account. After the population of applications has been determined, the Database Administrator (DBA) should immediately change the “sa” password to adhere to the organization’s password policy. The DBA should then share this information with as few development staff as necessary. The password change represents a near-term fix and does not comprehensively address the risk. A more complete approach is to schedule individual projects to remediate this risk by connecting to database systems using a more secure approach. The order of priority should be determined by the criticality of the database system, not the level of effort required to improve the database connection approach within an application.

In addition, we recommend the implementation of a set of software development standards that prohibits the use of an administrator account (i.e., “sa”) to establish a database connection from an application to a database system. The standards should align with the development standards published by the Software Engineering Institute. This will facilitate a mechanism for management to gauge the development department’s improvement against the software maturity model.
Management’s Response:

Remainder of this page left blank intentionally.
FINDINGS AND RECOMMENDATIONS – INTERNAL WIRELESS NETWORK ASSESSMENT

The following recommendations, which resulted from the wireless network assessment, are submitted to assist in improving the security posture of ABC’s wireless network.

No. 7: Wireless Access Points

We identified three (3) wireless access point SSIDs that belong to and are managed by ABC. The access point’s SSIDs are “comdevcom,” “tops,” and “tvsm.” The “tops” and “tvsm” access points appear to be managed by departments and are not configured with adequate security. In addition, there are numerous vulnerabilities associated with the “tops” access point.

Risk:
While these access points are not rogue, they are insecure, and their signals bleed into adjacent parking lots; this represents a landing location for a potential hacker to park and attempt uninterrupted exploits against ABC’s network. In addition, unauthorized users can use these access points as a launch point for attacks against other enterprise networks. This creates a potential liability to ABC, if a third party network is breached while using an ABC access point.

Recommendation:
We recommend the immediate removal of the “tops” and “tvsm” access points, as they represent unnecessary risk to ABC. To the extent a specific department requires wireless access, it should leverage the organization’s wireless network “comdevcom” and adhere to the level of security implemented on the “comdevcom” network.

Management’s Response:
No. 8: Wireless Network ‘comdevcom’ Encryption

The level of security and data encryption implemented on the “comdevcom” wireless network is WAP2-Personal. As noted in the diagram below, this is considered mid-level encryption and should be increased.

Risk:
The current level of encryption implemented on the wireless network is not designed to protect enterprise data. Given the reach of the wireless signal, an unauthorized user or attacker could capture enough packets to crack the current encryption and have full access to all wireless data communications. It is our understanding that Apple iPads are currently being implemented and communicating on the “comdevcom” wireless network. Potentially, any communication from any device on the “comdevcom” network can be sniffed and decrypted by an attacker or unauthorized person.

Recommendation:
We recommend that ABC implement a higher level of encryption to protect the data that is being transmitted over the wireless network. At a minimum, we recommend WAP2-Enterprise encryption.

Management’s Response:
No. 9: Wireless Network ‘comdevcom’ Device Management

We identified four (4) Cisco access points with the SSID of “comdevcom.” Two (2) of these access points appear to be configured to allow channel hopping. In addition, all four (4) of these devices must be individually managed because they are not bridged together to create one seamless wireless network.

Risk:
The current configuration requires the administrator to manually manage the configuration of each device. This increases the likelihood of a misconfiguration that could expose the internal network to a security breach. As evidenced by two (2) of the devices, they allow channel hopping. While this is not a security risk, it is an example of how having to manage multiple devices can create an unintended misconfiguration. In the event that such a misconfiguration occurs, the network can be easily compromised.

Recommendation:
We recommend an upgrade to an enterprise wireless appliance that can be centrally managed, operate as a seamless wireless network and provide improved security.

In the absence of an upgrade, the current solution should be re-designed to create one (1) wireless network (i.e., bridge the devices) that can be managed from one device. Additionally, the re-designed wireless network should be configured to prevent channel hopping.

Management’s Response:
Core Switch Configuration (Cisco 6509)

During the scanning of the internal network, the network performance degraded noticeably. In addition, we were informed that select server performance became sluggish. Based on our understanding of the internal network architecture and our experience with networks built with similar equipment, it is our opinion that the core switch’s (Cisco 6509) configuration may need to be reviewed by a Cisco Engineer, as it appears there may be a few routes that need to be adjusted.
FINDINGS AND RECOMMENDATIONS – ACTIVE DIRECTORY USER ACCOUNT ADMINISTRATION

The following recommendations, which resulted from the Active Directory (AD) user account administration assessment, are submitted to assist in improving the security posture of ABC’s AD system.

No. 10: Active Directory (AD) Domain Account Policies

During our review of the AD domain account password configurations, we identified configuration settings that do not meet best practice recommended settings and increase the risk of unauthorized users gaining access to system resources and data. Specifically, we noted the following risks:

- Password history is not maintained – users can reuse passwords indefinitely;
- Password complexity is not enabled – non-complex passwords are easy to guess by unauthorized users;
- The account lockout threshold is set to zero (0) – this setting indicates the number of failed logon attempts before user accounts are locked out. A value of “0” allows an unlimited number of failed logon attempts;
- Account lockout duration has not been configured – indicates the amount of time an account will remain locked out when the lockout threshold is exceeded. The current configuration does not lockout accounts;
- The AD “Administrator” account and “Guest” account have not been renamed – default accounts are typically the first target of an unauthorized user attempting to gain access to system resources and data. The “Administrator” account has escalated system privileges, creating a higher level of risk; and
- The ability to prevent transfer of passwords in clear text is disabled, allowing passwords to be transferred within the network in clear text, compromising the security of network passwords.

Risk:

Network password controls provide the primary defense against unauthorized access to ABC’s network resources, systems and data. Weak password controls increase the risk of unauthorized users gaining access to system resources and data.
Recommendation:
We strongly recommend that ABC consider enhancing the current password configurations to meet those of Best Practices. Specifically, we recommend the following AD domain policies:

- Set password history to remember thirteen (13) or more passwords;
- Enable password complexity requirements;
- Set the account lockout threshold to three (3);
- Set the reset account lockout counter in minutes to one thousand, four hundred and forty (1,440);
- Rename the Administrator account;
- Rename the Guest account; and
- Enable the setting to prevent transfer of passwords in clear text.

Management’s Response:
ACTIVE DIRECTORY DOMAIN ACCOUNT POLICY VALUES COMPARED AGAINST INDUSTRY AVERAGES
No. 11: Active Directory (AD) User Account Analysis

Per review of user accounts settings, we identified user accounts that should be deleted from the server, and other user account configuration deficiencies that should be modified. Specifically, we identified the following:

- There are forty-three (43) Local Security Groups, containing ninety-five (95) members defined on your domain. Forty-seven percent (47%) or twenty (20) of these groups are empty;
- There are five hundred and fifty-four (554) Global Security Groups, containing nine thousand three hundred and eleven (9,311) members defined on your domain. Fourteen percent (14%) or seventy-six (76) of these groups are empty;
- There are ten (10) Domain Universal Groups, containing eight hundred and seventy-nine (879) members defined on your domain. Twenty percent (20%) or two (2) of these groups are empty;
- Excluding disabled accounts, fifteen percent (15%) or one hundred ninety-one (191) of the user accounts have not logged on in the last thirty (30) days:
  - Fourteen percent (14%) or one hundred seventy-three (173) users have not logged on in the last sixty (60) days;
  - Thirteen percent (13%) or one hundred sixty-six (166) users have not logged on in the last ninety (90) days;
  - Twelve percent (12%) or one hundred fifty-two (152) users have not logged on in the last six (6) months; and
  - Nine percent (9%) or one hundred twenty-one (121) users have never been used.
- Excluding disabled accounts, nineteen percent (19%) or four (4) administrator accounts have not logged on in the last six (6) months.
  - One (1) administrator account has never been used.

Risk:
The majority of these items represent housekeeping tasks that should be performed to maintain a clean system. Allowing these items to remain provides an opportunity for an unauthorized user to attempt to breach the system using an inactive account. If an Administrator account is breached, the entire system and all systems that rely on Active Directory are at risk of being compromised by an unauthorized user.
Recommendation:
We recommend the following actions be taken:
• Review all groups with no members assigned. Remove all groups that are not necessary.
• Review all user and administrative accounts that have not recently logged in and remove from Active Directory if the account is not necessary; and
• Remove the administrator account that has never been used.

Management’s Response:
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:

TECHNICIAN’S REPORT
# Technician's Report Vulnerability Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2003-0693</td>
<td>OpenSSH &lt; 3.7.1 Multiple Vulnerabilities</td>
<td>10.0</td>
<td>High</td>
<td>A &quot;buffer management error&quot; 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.</td>
<td>Upgrade to OpenSSH 3.7.1 or later.</td>
<td>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.</td>
</tr>
<tr>
<td>2</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2003-0682</td>
<td>OpenSSH &lt; 3.7.1 Multiple Vulnerabilities</td>
<td>7.5</td>
<td>High</td>
<td>A &quot;buffer management error&quot; 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.</td>
<td>Upgrade to OpenSSH 3.7.1 or later.</td>
<td>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.</td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>----------------------</td>
<td>--------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>3</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2003-0695</td>
<td>OpenSSH &lt; 3.7.1 Multiple Vulnerabilities</td>
<td>7.5</td>
<td>High</td>
<td>Multiple &quot;buffer management errors&quot; 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.</td>
<td>Upgrade to OpenSSH 3.7.1 or later.</td>
<td><strong>Special Note:</strong> 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.</td>
</tr>
<tr>
<td>4</td>
<td>208.xx.xxx.xx</td>
<td>CVE-1999-0502*</td>
<td>Default Password (guest) for 'guest' Account</td>
<td>7.5</td>
<td>High</td>
<td>The account 'guest' has the password 'guest' set. An attacker may use it to gain further privileges on this system.</td>
<td>Set a password for this account or disable it.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-1483</td>
<td>OpenSSH X11 Forwarding Session Hijacking</td>
<td>6.9</td>
<td>Medium</td>
<td>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 sessions if the corresponding ports on the IPv4 interface are in use. See also : <a href="http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011">http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=463011</a> <a href="http://www.openssh.org/txt/release-5.0">http://www.openssh.org/txt/release-5.0</a></td>
<td>Upgrade to OpenSSH version 5.0 or later.</td>
<td><strong>Special Note:</strong> 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.</td>
</tr>
</tbody>
</table>
## Technician's Report Vulnerability Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference (<em>CVSS Severity Incomplete Approx.</em>)</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>6.8</td>
<td>Medium</td>
<td>Identified several open TCP/UDP ports. The following malware may be present on these ports: - TCP80: Back End, Executor, Hooker, RingZero</td>
<td>Confirm presence of malware and remove.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Manual Scoring Vectors</td>
<td></td>
<td></td>
<td>Open ports and potential malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Access: Network</td>
<td></td>
<td></td>
<td>Access Comp: Medium</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Access Comp: Medium</td>
<td></td>
<td></td>
<td>Auth: None</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Conf: Partial</td>
<td></td>
<td></td>
<td>Integ: Partial</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Avail: Partial</td>
<td></td>
<td></td>
<td>Open ports and potential malware</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2003-1567</td>
<td>5.8</td>
<td>Medium</td>
<td>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.</td>
<td>Disable these methods. Refer to the plugin output for more information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other References: OSVDB:877</td>
<td></td>
<td></td>
<td>HTTP TRACE / TRACK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:3726</td>
<td></td>
<td></td>
<td>Methods Allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:5648</td>
<td></td>
<td></td>
<td>HTTP TRACE / TRACK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:50485</td>
<td></td>
<td></td>
<td>Methods Allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2004-2320</td>
<td>5.8</td>
<td>Medium</td>
<td>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.</td>
<td>Disable these methods. Refer to the plugin output for more information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other References: OSVDB:877</td>
<td></td>
<td></td>
<td>HTTP TRACE / TRACK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:3726</td>
<td></td>
<td></td>
<td>Methods Allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:5648</td>
<td></td>
<td></td>
<td>HTTP TRACE / TRACK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:50485</td>
<td></td>
<td></td>
<td>Methods Allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2010-0386</td>
<td>4.3</td>
<td>Medium</td>
<td>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.</td>
<td>Disable these methods. Refer to the plugin output for more information.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other References: OSVDB:877</td>
<td></td>
<td></td>
<td>HTTP TRACE / TRACK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:3726</td>
<td></td>
<td></td>
<td>Methods Allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:5648</td>
<td></td>
<td></td>
<td>HTTP TRACE / TRACK</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OSVDB:50485</td>
<td></td>
<td></td>
<td>Methods Allowed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference (*CVSS Severity Incomplete Approx)</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>---------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>10</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2006-3918</td>
<td>Web Server Expect Header</td>
<td>4.3</td>
<td>Medium</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>11</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-5944</td>
<td>Cross-site scripting vulnerability</td>
<td>4.3</td>
<td>Medium</td>
<td>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.</td>
<td>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.</td>
</tr>
<tr>
<td>12</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Multiple Web Server Dangerous HTTP Method TRACE</td>
<td>4.3</td>
<td>Medium</td>
<td>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</td>
<td>Disable this method.</td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference (*CVSS Severity Incomplete Approx)</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>13</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2001-0361</td>
<td>SSH Protocol Version 1 Session Key Retrieval</td>
<td>4.0</td>
<td>Medium</td>
<td>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.</td>
<td>Disable compatibility with version 1 of the protocol. <strong>Special Note:</strong> 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.</td>
</tr>
<tr>
<td>14</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Inconsistent Hostname and IP Address</td>
<td>0.0</td>
<td>Low</td>
<td>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</td>
<td>Correct hostname and IP address.</td>
</tr>
<tr>
<td>15</td>
<td>208.xx.xxx.xx</td>
<td>CVE-1999-0524</td>
<td>ICMP Timestamp Request Remote Date Disclosure</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>Filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).</td>
</tr>
</tbody>
</table>
# Technician's Report Vulnerability Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference (*CVSS Severity Incomplete Approx)</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>16</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>SSH Server Type and Version Information</td>
<td>0.0</td>
<td>Low</td>
<td>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</td>
<td>N/A</td>
<td><strong>Special Note:</strong> 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.</td>
</tr>
<tr>
<td>17</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>SSH Protocol Versions Supported</td>
<td>0.0</td>
<td>Low</td>
<td>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:e1:77:73: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</td>
<td>N/A</td>
<td><strong>Special Note:</strong> 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.</td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference (*CVSS Severity Incomplete Approx)</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>----------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>------------------------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>18</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>HTTP Server type and version</td>
<td>0.0</td>
<td>Low</td>
<td>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)</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

Other References: OWASP-CM-006

Note: Manual Scoring Vectors

- Access: Network
- Access Comp: Low
- Auth: None
- Conf: None
- Integ: None
- Avail: None

| 19  | 208.xx.xxx.xx | CVE - None | Web Server Directory Enumeration | 0.0 | Low | It is possible to enumerate directories on the remote 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 |

<p>| 20  | 208.xx.xxx.xx | CVE - 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 |</p>
<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>HyperText Transfer Protocol (HTTP) Information</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Backported Security Patch Detection (WWW)</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>HTTP methods per directory</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference (*CVSS Severity Incomplete Approx)</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>----------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>24</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>RPC Services Enumeration</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>RPC portmapper Service Detection</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>OS Identification</td>
<td>0.0</td>
<td>Low</td>
<td>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</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## [ Technician's Report Vulnerability Details ]

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference <em>(CVSS Severity Incomplete Approx)</em></th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>IP Protocols Scan</td>
<td>0.0</td>
<td>Low</td>
<td>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</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Apache Banner Linux Distribution Disclosure</td>
<td>0.0</td>
<td>Low</td>
<td>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</td>
<td>If you do not wish to display this information, edit httpd.conf and set the directive 'ServerTokens Prod' and restart Apache.</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>TCP/IP Timestamps Supported</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference (*CVSS Severity Incomplete Approx)</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>--------------------------------------------------------</td>
<td>--------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>30</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Potentially sensitive resource discovered</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Manual Scoring Vectors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Access: Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Access Comp: Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Auth: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Conf: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Integ: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Avail: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Default web server page</td>
<td>0.0</td>
<td>Low</td>
<td>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</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Other References: OSVDB-3233</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Remove unnecessary default server pages.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Manual Scoring Vectors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Access: Network</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Access Comp: Low</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Auth: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Conf: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Integ: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-Avail: None</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Technician's Report Vulnerability Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference (*CVSS Severity Incomplete Approx.)</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>ETag header found on server</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td>Upgrade to the latest Apache server.</td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Apache version outdated</td>
<td>0.0</td>
<td>Low</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Technician's Report Vulnerability Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference (*CVSS Severity Incomplete Approx)</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>34</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>Directory indexing enabled</td>
<td>0.0</td>
<td>Low</td>
<td>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 &quot;hidden&quot; files or directories to remote users, or aid in more focused attacks. <strong>Path:</strong> /icons/</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-0910</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities</td>
<td>10.0</td>
<td>High</td>
<td>Unspecified vulnerability in PHP before 5.2.1 allows attackers to &quot;clobber&quot; certain super-global variables via unspecified vectors.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-0599</td>
<td>PHP &lt; 5.2.6 Multiple Vulnerabilities</td>
<td>10.0</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.6 or later.</td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-2050</td>
<td>PHP &lt; 5.2.6 Multiple Vulnerabilities</td>
<td>10.0</td>
<td>High</td>
<td>Stack-based buffer overflow in the FastCGI SAPI (fastcgi.c) in PHP before 5.2.6 has unknown impact and attack vectors.</td>
<td>Upgrade to PHP version 5.2.6 or later.</td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-2051</td>
<td>PHP &lt; 5.2.6 Multiple Vulnerabilities</td>
<td>10.0</td>
<td>High</td>
<td>The escapeshellcmd API function in PHP before 5.2.6 has unknown impact and context-dependent attack vectors related to &quot;incomplete multibyte chars.&quot;</td>
<td>Upgrade to PHP version 5.2.6 or later.</td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-5557</td>
<td>PHP 5 &lt; 5.2.7 Multiple Vulnerabilities - heap-based buffer overflow</td>
<td>10.0</td>
<td>High</td>
<td>Heap-based buffer overflow in ext/mbstring/libmbi/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.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>----------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>40</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2009-1955</td>
<td>Apache 2.x &lt; 2.2.12 Multiple Vulnerabilities - DoS memory consumption</td>
<td>7.8</td>
<td>High</td>
<td>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.</td>
<td>Either ensure that the affected modules / directives are not in use or upgrade to Apache version 2.2.12 or later.</td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>MySQL Community Server Multiple Vulnerabilities</td>
<td>7.8</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to MySQL Community Server version 5.0.45 or later.</td>
<td></td>
</tr>
<tr>
<td>42</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-0166</td>
<td>OpenSSL version 0.9.8c appears to be outdated</td>
<td>7.8</td>
<td>High</td>
<td>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.</td>
<td>Upgrade OpenSSL to the latest version.</td>
<td></td>
</tr>
</tbody>
</table>
## Technician's Report Vulnerability Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference (*CVSS Severity Incomplete Approx)</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>208.xx.xxx.xx</td>
<td>CVE - None</td>
<td>SQL Injection</td>
<td>7.5</td>
<td>High</td>
<td>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, typcast 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</td>
</tr>
</tbody>
</table>

| 44  | 208.xx.xxx.xx      | CVE-2007-0905 Multiple Vulnerabilities - bypass safe_mode and open_basedir restrictions | PHP < 5.2.1 | 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. |

| 45  | 208.xx.xxx.xx      | CVE-2007-0906 Multiple Vulnerabilities                | PHP < 5.2.1 | 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-2007-1885). |

| 46  | 208.xx.xxx.xx      | CVE-2007-0909 Multiple Vulnerabilities - execute arbitrary code | PHP < 5.2.1 | 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. |

---

**Suggested Solution | Fix Special Notes**

Upgrade to PHP version 5.2.1 or later.
<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>47</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1376</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - read and write to arbitrary memory locations</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1453</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - buffer overflow</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
</tr>
<tr>
<td>49</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1700</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - execute arbitrary code</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1825</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - buffer overflow</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
</tr>
<tr>
<td>51</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1885</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - execute arbitrary code</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference (*CVSS Severity Incomplete Approx)</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>--------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>52</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1887</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - buffer overflow</td>
<td>7.5 High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>53</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2007-1890</td>
<td>PHP &lt; 5.2.1 Multiple Vulnerabilities - execute arbitrary code</td>
<td>7.5 High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.1 or later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>54</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2006-5465</td>
<td>PHP &lt; 5.2 Multiple Vulnerabilities</td>
<td>7.5 High</td>
<td>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</td>
<td>Upgrade to PHP version 5.2.0 or later.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>55</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-2371</td>
<td>PHP 5 &lt; 5.2.7 Multiple Vulnerabilities - heap-based buffer overflow</td>
<td>7.5 High</td>
<td>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</td>
<td>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.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### [ Technician's Report Vulnerability Details ]

<table>
<thead>
<tr>
<th>No.</th>
<th>Affected IP Address</th>
<th>CVE Number/Reference (<em>CVSS Severity Incomplete Approx</em>)</th>
<th>Vulnerability</th>
<th>CVSS Score (version 2.0)</th>
<th>Severity Level</th>
<th>Vulnerability Details</th>
<th>Suggested Solution</th>
<th>Fix Special Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>56</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-3658</td>
<td>PHP 5 &lt; 5.2.7 Multiple Vulnerabilities - buffer overflow DoS</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>57</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-5624</td>
<td>PHP 5 &lt; 5.2.7 Multiple Vulnerabilities - bypass safe_mode restrictions</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>58</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-5625</td>
<td>PHP 5 &lt; 5.2.7 Multiple Vulnerabilities - write arbitrary files</td>
<td>7.5</td>
<td>High</td>
<td>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 &quot;php_value error_log&quot; entry in a .htaccess file.</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>No.</td>
<td>Affected IP Address</td>
<td>CVE Number/Reference</td>
<td>Vulnerability</td>
<td>CVSS Score (version 2.0)</td>
<td>Severity Level</td>
<td>Vulnerability Details</td>
<td>Suggested Solution</td>
<td>Fix Special Notes</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------</td>
<td>----------------------</td>
<td>---------------</td>
<td>--------------------------</td>
<td>----------------</td>
<td>-----------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>59</td>
<td>208.xx.xxx.xx</td>
<td>CVE-2008-5658</td>
<td>PHP 5 &lt; 5.2.7 Multiple Vulnerabilities - Directory traversal vulnerability in the ZipArchive</td>
<td>7.5</td>
<td>High</td>
<td>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.</td>
<td>Upgrade to PHP version 5.2.8 or later. Note that 5.2.7 was 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. <strong>Special Note:</strong> 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.</td>
<td></td>
</tr>
</tbody>
</table>