



**COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT**

Contract No. UCPJMU5760

This contract entered into this 2nd day of March 2020, by Securance Consulting, LLC, hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

WITNESSETH that the Contractor and the Purchasing Agency, in consideration of the mutual covenants, promises and agreements herein contained, agree as follows:

SCOPE OF CONTRACT: The Contractor shall provide the services to the Purchasing Agency as set forth in the Contract Documents.

PERIOD OF PERFORMANCE: From April 2, 2020 through April 1, 2021 with four (4) one-year renewal options.

The contract documents shall consist of:


- (1) This signed form;
- (2) The following portions of the Request for Proposal FDC-1057 dated September 19, 2019:
 - (a) The Statement of Needs,
 - (b) The General Terms and Conditions,
 - (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
 - (d) Addendum One, dated October 9, 2019.
- (3) The Contractor's Proposal dated October 21, 2019 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
 - (a) Negotiations Summary, dated February 14, 2020.

IN WITNESS WHEREOF, the parties have caused this Contract to be duly executed intending to be bound thereby.

CONTRACTOR:
By: 
(Signature)

Paul Ashe
(Printed Name)

Title: President

PURCHASING AGENCY:
By: 
(Signature)

Doug Chester
(Printed Name)

Title: Buyer Senior



RFP # FDC-1057
Information Technology Security Auditing Services
Negotiation Summary for Securance Consulting, LLC
February 14, 2020

1. The pricing schedule is as follows:

Labor Category	Hourly Rate
Project Manager	\$128.00
Senior IT Security Consultant	\$124.00
IT Senior Consultant	\$120.00
IT Security Analyst	\$110.00

All rates in the pricing schedule are inclusive of travel.

2. Contractor has disclosed all potential fees. Additional charges will not be accepted.



**SECURANCE
CONSULTING**

the advantage of insight



DATE: 10/22/2019

RESPONSE TO REQUEST FOR PROPOSAL #FDC-1057 IT SECURITY AUDITING SERVICES

Contact for RFP Response:

Gillian Tedeschi
Director of Marketing
gtedeschi@securanceconsulting.com
P: 877.578.0215 ext. 111

Project Office
1320 Central Park Blvd., Suite 200
Fredericksburg, VA 22401

Redacted Copy

the advantage of insight

An abstract graphic composed of numerous small dots arranged in a series of overlapping, wave-like patterns that sweep across the lower half of the page. The dots are in shades of light green, dark green, and black, creating a sense of depth and movement. The overall effect is reminiscent of a stylized landscape or a data visualization.



TABLE OF CONTENTS

RFP COVER SHEET	1
COVER LETTER	2
PLAN AND METHODOLOGY FOR PROVIDING GOODS AND SERVICES	4
WRITTEN NARRATIVE STATEMENT	31
OFFEROR DATA SHEET	42
SMALL BUSINESS SUBCONTRACTING PLAN	43
PROPOSED COST	46

the advantage of insight



REQUEST FOR PROPOSAL

RFP# FDC-1057

Issue Date: September 19, 2019
Title: Information Technology (IT) Security Auditing Services
Issuing Agency: Commonwealth of Virginia
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Period of Contract: From Date of Award Through One Year (Renewable)

Sealed Proposals Will Be Received Until 2:00 PM on October 17, 2019 for Furnishing The Services Described Herein.

SEALED PROPOSALS MAY BE MAILED, EXPRESS MAILED, OR HAND DELIVERED DIRECTLY TO THE ISSUING AGENCY SHOWN ABOVE.

All Inquiries For Information And Clarification Should Be Directed To: Doug Chester, Buyer Senior, Procurement Services, chestefd@jmu.edu; 540-568-4272; (Fax) 540-568-7935 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED.

In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

Securance LLC

13904 Monroes Business Park

Tampa, FL 33635

By:

(Signature in Ink)

Name: Paul Ashe

(Please Print)

Date: 10/21/19

Title: President

Web Address: www.securanceconsulting.com

Phone: 877-578-0215

Email: pashe@securanceconsulting.com

Fax #: 813-328-4465

ACKNOWLEDGE RECEIPT OF ADDENDUM: #1 AA #2 _____ #3 _____ #4 _____ #5 _____ (please initial)

SMALL, WOMAN OR MINORITY OWNED BUSINESS:

☒ YES; ☐ NO; IF YES ☐ SMALL; ☐ WOMAN; ☒ MINORITY IF MINORITY: ☒ AA; ☐ HA; ☐ AsA; ☐ NW; ☐ Micro

October 22, 2019

Doug Chester, Buyer Senior
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Building
First Floor, Suite 1023
Harrisonburg, VA 22807

Thank you for considering Securance Consulting for your future IT security auditing needs. By partnering with Securance, James Madison University (JMU) will have the ability to enlist and gain the knowledge of our Senior IT Consultants, each with over 20 years' experience conducting the assessments JMU requires, who will deliver valuable insight into the current state of JMU's IT security measures and roadmaps for each project, detailing how JMU can achieve its future state goals of maintaining a strong security posture.

To achieve the desired outcome, JMU can expect the Securance team to:

- » Enhance the effectiveness of future assessments and demonstrate our commitment to JMU by including **24 hours of free management-level consulting** at the start of any contracted engagement. During this 24-hour block, we will interview and meet with JMU stakeholders to ensure that we fully understand the organization and its objectives.
- » Fully understand and comprehend JMU's objectives for each security audit.
- » Leverage its years of knowledge of the education industry and experience performing IT security audits for similar organizations, including [REDACTED].
- » Develop an approach tailored to JMU's business objectives and technology environment.
- » Arrive on premise prepared to begin working with JMU's team.
- » Provide constant updates of the project's status to JMU's Project Manager (PM).
- » Deliver a high-quality report without surprises (we will ensure you are aware of any urgent findings right away), containing actionable recommendations to improve JMU's overall security posture.

Our knowledge of and experience with conducting a wide range of IT security audit services is unmatched. As a full-service cybersecurity and compliance firm, we will provide the value add of enterprise cybersecurity expertise and knowledge of multiple client IT environments to the engagement. Finally, to ensure sustained improvement, we will provide JMU with a knowledge transfer session to share the details of our process with JMU's staff.



From the detailed nature of our assessment, to the comprehensiveness of our deliverables, to the in-depth knowledge transfer and remediation retesting we will conduct following each applicable assessment, JMU will not find a firm whose analyses and results are more accurate and exhaustive than ours. Discussions with our clients over the past 17 years have confirmed that Securance's superior work product represent significant long-term savings.

Thank you for including Securance in your evaluation process. If you have any questions upon review of our proposal, please do not hesitate to contact me.

Professional regards,

Paul Ashe, CPA, CISA, CISSP
President and Authorized Representative of Securance LLC



PLAN AND METHODOLOGY FOR PROVIDING GOODS AND SERVICES

IV. Statement of Needs, C.1.

Describe your company's plan to provide certified professional staff (CISA, CISSP, CISM, MCP, CCNA, and ISSMP) to perform a wide range of IT audits under the direction of the Director of staff of JMU's Audit and Management Services (AMS).

Securance will staff JMU's future projects with consultants who hold the following credentials:

- | | |
|----------|-------------|
| » CEH | » MCITP |
| » CCNA | » MCTS |
| » CISA | » MCSA |
| » CISSP | » MCSE |
| » CPA | » Security+ |
| » Linux+ | |

Proposed Scope

The proposed team of Paul Ashe, Ray Resnick, Bill Tisch, Chris Cook, Parves Kamal, and Ibrahim Badrawi has reviewed the scope of the RFP and the addenda released by JMU and is prepared to perform the following tasks as JMU requires:

1. Management Consulting

Securance begins each engagement with 24 hours of free management consulting. During this time, we will meet with JMU stakeholders to gain an understanding of the technology environment and project scope and refine objectives.

2. External Vulnerability Scanning

- » Assess Internet presence:
 - » Identify public IP space
 - » Identify all running services on each system, via comprehensive port scanning in stealth mode
 - » Identify all vulnerabilities on each device, system or server, running all tools in stealth mode
- » Review results with JMU's Project Management

3. Wireless Network Assessment

- » Review the configuration of the controller, focusing on the security of user-manipulated configuration settings
- » Assess the location of wireless access points and routers, signal strength, and security measures in place to prevent unauthorized access to the network
- » Identify rogue access points
- » Identify and review encryption protocols
- » Review network segmentation and user access controls
- » Using a WiFi Pineapple tool, attempt to penetrate the wireless network via a rogue access point

Plan and Methodology for Providing Goods and Services

Proposed Scope — IV. Statement of Needs, C.1.

4. Firewall and Router Security Assessments

- » Perform a firewall configuration review:
 - » Gain an understanding of the firewall's placement in the network topology
 - » Gain an understanding of how the firewall is administered and managed
 - » Review administrative and access controls to ensure your firewall is protected on multiple fronts
 - » Perform a line-by-line review of the firewall's configuration
 - » Identify problem, redundant, and circular rules
 - » Perform a vulnerability scan of devices
 - » Review logs manually
 - » Analyze traffic patterns
 - » Identify potential virus and hack attempts
 - » Assess use of insecure protocols
- » Perform a router | switch configuration review:
 - » Gain an understanding of the device's placement in the network topology
 - » Gain an understanding of how the device is administered and managed
 - » Ensure device is running most-up-to-date firmware version
 - » Assess use of default manufacturer passwords, use of insecure protocols, and access control lists
 - » Perform an unauthenticated and | or authenticated vulnerability scan of the device
 - » Perform a line-by-line review of the device's configuration
 - » Review logs using manual and automated techniques to verify login procedures are followed and up to date

5. Server Configuration Assessment

- » Gain an understanding of the role the server plays in the IT environment (i.e., enterprise application server, file server, infrastructure application server, or storage server)
- » Gain an understanding of the organization's security objectives
- » Assess the organization's server build and configuration standards
- » Perform a vulnerability analysis of the host server
- » Assess the server's hardened security posture state against the organization's objectives
- » Assess the server's configuration against the Center for Internet Security (CIS) benchmarks

6. Database Architecture Security Assessment

- » Gain an understanding of the database server's role in the IT environment, the application it supports, and that application's functionality
- » Gain an understanding of the organization's security objectives
- » Assess the organization's build and configuration standards for database servers
- » Perform a vulnerability analysis of the database server, reviewing both universal and database-specific security controls
- » Review the operating system that hosts the database:
 - » Perform a vulnerability analysis of the operating system
 - » Assess the operating system's configuration against the Center for Internet Security (CIS) benchmarks
- » Assess the database's overall security posture against the organization's security objectives

Plan and Methodology for Providing Goods and Services

Proposed Scope — IV. Statement of Needs, C.1.

7. Network Scanning Process Assessment

- » Perform an internal network vulnerability assessment
 - » Identify internal network segment in scope for testing
 - » Identify hosts to specifically exclude from testing
 - » Identify all running services on each system via comprehensive port scanning in stealth mode
 - » Identify all vulnerabilities on each device, system or server, running all tools in stealth mode
 - » Review results of initial scans with JMU's personnel

8. Web Application Security Assessment

- » Perform unprivileged (i.e., without credentials) and privileged (i.e., with standard credentials) web application testing:
 - » Identify web applications
 - » For privileged testing, request a set of standard user credentials and a set of administrative user credentials for each application
 - » Assess the hosting server and associated web server's configurations
 - » Perform a security review of the back-end database
 - » Perform unprivileged web application vulnerability testing
 - » Pending testing and authorization, attempt to modify application content
 - » Perform privileged web application vulnerability testing using the credentials provided by JMU
 - » Pending testing and authorization, attempt to modify application content

9. Active Directory Security Assessment

- » Gain an understanding of the design of the directory services and any trust between organizations
- » Extract Active Directory data for analysis, including a review of the following settings:
 - » Domain structure
 - » Trusted and trusting domains
 - » User attributes:
 - » Accounts allowed to dial in
 - » Discretionary access controls for containers
 - » User and object rights and privileges
 - » Audit policy
 - » Account last logons
 - » Changes to registry key values
 - » Active Directory host configuration
- » Compare Active Directory configuration and security to industry standards and best practices

Plan and Methodology for Providing Goods and Services

Proposed Scope — IV. Statement of Needs, C.1.

10. Penetration Testing

- » Perform an external network penetration test:
 - » Assess Internet presence:
 - » Identify public IP space
 - » Identify all running services on each system, via comprehensive port scanning in stealth mode
 - » Identify all vulnerabilities on each device, system or server, running all tools in stealth mode
 - » Review results of initial scans with JMU's personnel
 - » Perform automated and manual penetration activities based on feedback from JMU's PM
 - » Review results with JMU's Project Management
- » Perform an internal network vulnerability assessment and penetration test:
 - » Identify internal network segment in scope for testing
 - » Identify hosts to specifically exclude from testing
 - » Identify all running services on each system via comprehensive port scanning in stealth mode
 - » Identify all vulnerabilities on each device, system or server, running all tools in stealth mode
 - » Review results of initial scans with JMU's personnel
 - » Perform automated and manual penetration activities based on feedback from JMU's PM
 - » Review results with JMU's Project Management

11. Telecommunications

- » Perform a configuration review of the hosting server or appliance
 - » Interview the device administrator(s)
 - » Perform a line-by-line configuration review
 - » Assess the state of control over the device
 - » Perform a vulnerability scan of the device
 - » Assess the use of insecure protocols
 - » Assess the firmware version
- » Perform a management software review
 - » Conduct interviews and walkthroughs
 - » Review user and administration documentation
 - » Review governing policies and procedures
 - » Evaluate the operating effectiveness of supporting general controls
 - » Review operating systems-specific security procedures

12. Remediation Retesting

- » Discuss with JMU personnel items that have been remediated from the vulnerability assessment report
- » Develop and execute a strategy to verify the remediation effort's success

Plan and Methodology for Providing Goods and Services

Proposed Scope — IV. Statement of Needs, C.1.

13. Performance of Knowledge Transfer

To ensure our assessment provides high value, is fully understandable, and the information obtained is sustained, we will conduct a knowledge transfer session with appropriate JMU staff. This session will provide answers as to why and how Securance performed specific tasks, so JMU staff are able to repeat the task at will.

14. Reporting

- » Management report, including:
 - » Executive summary — A summary of methods, findings, and recommendations of your assessment
 - » Introduction and scope
 - » Summary of findings
 - » Heat map (impact and probability)
 - » Prioritized risk rankings, actionable recommendations, cost justification, and time frame
 - » Conclusion
 - » Detailed assessment report — A comprehensive report that provides a detailed account of all engagement activities
 - » Background
 - » Specific objectives and detailed scope
 - » Approach and methodology
 - » Findings and recommendations
 - » Remediation roadmap
- » Technician's report — Raw data extracts from utilized security tools

Plan and Methodology for Providing Goods and Services

Methodology — External and Internal Network Vulnerability Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]

[REDACTED]

- [REDACTED]
 - [REDACTED]
 - [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]
 - [REDACTED]

[illegible][illegible]

[REDACTED]

[REDACTED]

(S) [REDACTED]
[REDACTED]
[REDACTED]

(S) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(S) [REDACTED]
[REDACTED]
[REDACTED]

(S) [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

(S) [REDACTED]
[REDACTED]

(S) [REDACTED]
[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — External and Internal Network Vulnerability Assessment — IV. Statement of Needs, C.1.

[REDACTED]



_____, _____, _____

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology continued Wireless Network Assessment — IV. Statement of Needs, C.1.

[REDACTED]



Plan and Methodology for Providing Goods and Services

Methodology — Firewall Security Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Router Security Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Server Configuration Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Database Architecture Security Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Network Scanning Process Assessment — IV. Statement of Needs, C.1.

Please see our internal network vulnerability assessment methodology on pages 9-11.

Methodology — Web Application Security Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Penetration Testing — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Penetration Testing — IV. Statement of Needs, C.1.

C) Vulnerability Assessment (continued)

[illegible][illegible]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Penetration Testing — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]
 [REDACTED]
 [REDACTED]

§ 87(2)(b)

§ 87(2)(b) [REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Penetration Testing: APT Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Penetration Testing: APT Assessment — IV. Statement of Needs, C.1.

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Telecommunications Security Assessment — IV. Statement of Needs, C.1.

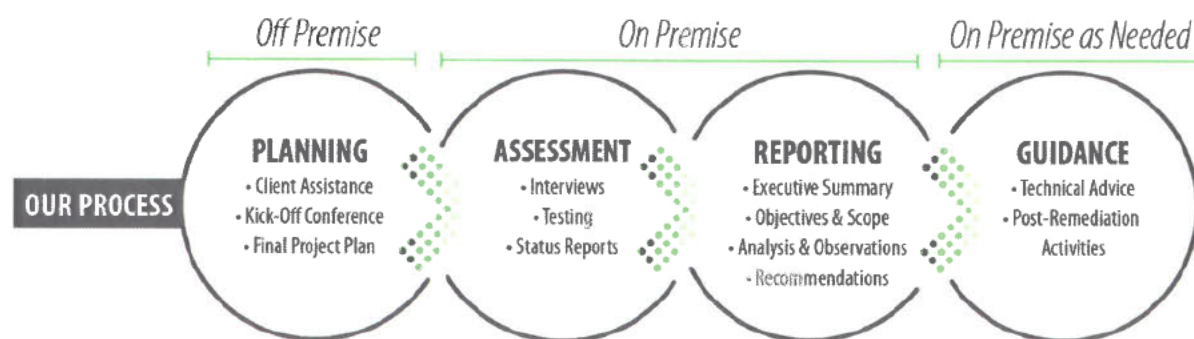
[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

Methodology — Project Management — IV. Statement of Needs, C.1.



Securance is dedicated to performing each contracted assessment as efficiently as possible. This begins with assigning Paul Ashe as the PM and single point of contact for JMU's team. In this role, Paul will be responsible for ensuring each project is a success. This will be achieved by providing JMU with status reports based on mutually agreed-upon schedules. The status reports will track project progress, list possible project risks, and provide updates to other information needed to ensure a successful project. Paul will manage Securance's team according to the roles and responsibilities in the organizational chart below.



Plan and Methodology for Providing Goods and Services

Methodology — Project Management — IV. Statement of Needs, C.1.

We anticipate that as part of the project, JMU's Project Manager will:

- » Ensure all client assistance requested items are provided in a timely manner and assist in scheduling JMU staff for interviews with Securance
- » Join project status meetings as necessary
- » Review reports to obtain a clear understanding of the findings and recommendations
- » Provide Securance with feedback relative to the tone and format of the report

Methodology for Identifying and Assigning Certified Staff to Projects

We believe the best way to measure our ability to complete task orders on time is through discussion with our current clients (see client references on page 42).

We guarantee we will:

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

Please refer to our consultant bios and sample resumes for key personnel on pages 32-41.

"Surge" Capabilities

Securance typically recruits for technical positions by placing ads on our website, on job sites, and in newspapers. However, we also maintain relationships with staffing firms, so that we can quickly recruit and mobilize resources to "surge" project staff, if necessary.

Plan and Methodology for Providing Goods and Services

IV. Statement of Needs, C.2.

Describe your company's past history working with institutions of higher education:

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

IV. Statement of Needs, C.2.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Plan and Methodology for Providing Goods and Services

IV. Statement of Needs, C.2.

Clients in the Commonwealth of Virginia

[REDACTED]	
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]



WRITTEN NARRATIVE STATEMENT

Specific Proposal Instructions, B.3.

A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.

Securance is a privately held professional services firm dedicated to independent assessments of IT security, risk, compliance, and operational efficiency. Since March 4, 2002, we have performed over 1,000 security assessments, answering the substantial growth of our clients' needs with uncompromising, high-quality services at a reasonable cost.

Founded by Paul Ashe, a former Southeast Area Security Expert for Ernst & Young, Securance seeks to deliver outstanding results to each and every client and ensure that projects are always done right. Through his experiences, Paul learned the challenges organizations from many industries face — and made it his mission to help them improve their IT security postures, compliance profiles, and risk management systems.

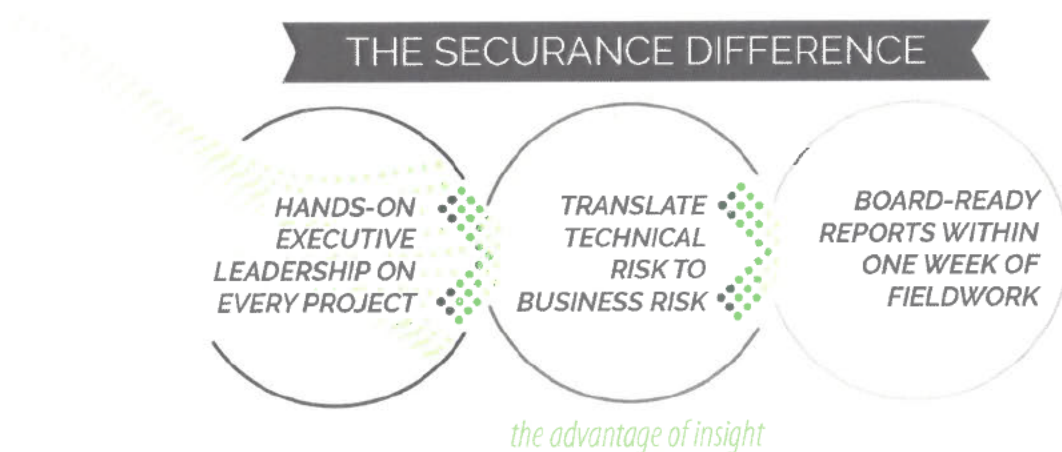
Securance has provided IT security auditing services to clients in every industry, including higher education institutions, school districts, boards of education, and all levels of government agencies.

Summary of Professional Services

- » Compliance (e.g., CJIS, NIST, HIPAA, PCI DSS, state privacy and security statutes)
- » Cybersecurity as a Service
- » Cybersecurity assessments
- » General and application controls assessments
- » Information security governance
- » Internal audit outsourcing | co-sourcing
- » IT risk assessments
- » Virtual CISO services
- » Vulnerability assessments and penetration testing

Areas of Expertise

- IT risk management in the following areas:
- » Application and database security
 - » Business continuity and disaster recovery planning
 - » Cloud security
 - » Incident response
 - » IT policy | procedure development
 - » IT process improvement
 - » Network security (LAN, WAN, wireless)
 - » Operating system security



Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Bios

A written narrative statement to include, but not be limited to, the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work.

Securance Consulting only hires experienced IT 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. Every team is staffed with Senior IT Security Consultants, who have at least 20 years' experience performing diverse assessments for government and industry leaders.

Securance's proposed key personnel for JMU's future projects are as follows:

Paul Ashe, President and Engagement Manager **CPA, CISA, CISSP**

Paul, Founder and President of Securance Consulting, has provided hands-on project management to lead numerous engagements over the past 20 years. A former IT consultant for Ernst & Young, Paul has leveraged his knowledge and experience into an effective, time- and budget-conscious project management style. He conducts technology-specific assessments, including network and application vulnerability and penetration tests and detailed software and hardware configuration reviews, for clients in every industry. He is an expert in identifying and providing customized remediation recommendations for IT security vulnerabilities. Please see his complete resume on page 34.

Ray Resnick, Senior IT Security Consultant **CISSP, CEH, CCNA, Security+**

Ray, a Senior IT Consultant with over 20 years' experience, is an expert in IT security, threat and risk analysis, and regulatory compliance. He specializes in conducting network and application vulnerability and penetration assessments, developing cybersecurity controls, and implementing best practices aligned with state, local, and federal regulatory requirements. Ray's expertise also includes designing comprehensive strategies to mitigate IT risks, seal IT security gaps, and support proactive vulnerability management processes. Please see his complete resume on page 35.

Bill Tisch, Senior IT Security Consultant **LINUX+, CISSP, CISA, CEH, MCSA, MCSE, MCITP, MCTS**

Bill, a Senior IT Consultant with over 20 years' experience, an expert in cybersecurity, vulnerability assessment, and penetration testing in IT and operational technology environments. His experience includes testing network, application, and platform security; implementing and configuring firewalls, IDS/IPS, content filtering, and advanced malware protection solutions; and developing policies and procedures to facilitate compliance with regulatory requirements. Please see his complete resume on page 36.

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Bios

Chris Cook, Senior IT Security Consultant CISSP, CISA

Chris, a Senior IT Consultant with over 20 years' experience, helps public and private sector leaders identify threats, enhance controls, and make lasting improvements to their risk and security profiles. Chris is a subject matter expert in ISO and NIST compliance and 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 page 37.

Ibrahim Badrawi, IT Security Consultant CCNA, CVA

Ibrahim, an IT Security Analyst with over 12 years' experience in performing IT security audits, is an expert in network security management, vulnerability assessments and penetration testing, and quantifying organizational risk. He is highly experienced in aiding clients to strengthen their security postures through detailed assessments of network, application, and network device security. He has extensive experience conducting software and hardware configuration reviews and developing customized remediation plans to mitigate risks and security vulnerabilities. Please see his complete resume on page 38.

Parves Kamal, IT Security Consultant CEH, Security+, RHCSA, RHCE

Parves, an IT Security Analyst with over five years' experience in IT security, excels conducting security assessments, configuration reviews, and testing for threats and vulnerabilities in dense IT environments. He has extensive experience identifying and developing remediation strategies for compromised systems. Please see his complete resume on page 40.

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Key Personnel

Paul Ashe, CPA, CISA, CISSP — Engagement Manager and Senior IT Security Consultant

Education, Training, and Certifications

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

Experience: IT Security

Paul has been the lead IT professional on numerous security engagements over the past 20 years. He has significant experience strengthening client security postures and breaching MS Windows and Unix platforms and perimeter security devices. He is proficient in the use of over 75 security tools. His functional experience includes:

- » Security Infrastructure Management
- » Security Assessments
- » Risk and Threat Analysis
- » Vulnerability Assessments
- » Penetration Testing
- » VoIP Solutions
- » IDS/IPS Deployment
- » Best Practice Deployment
- » Hardware and Software Configuration Reviews
- » Physical Security Management
- » Web Application Testing
- » Application and Database Security
- » Secure Network and DMZ Architecture Development
- » Compliance Assessments (e.g., NIST, ISO, HIPAA)
- » Security Framework Development

Paul has formulated security policies and procedures addressing areas that include:

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

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

Recent Clients

[REDACTED] [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Key Personnel

Ray Resnick, CISSP, CEH, CCNA, Security+ — Senior IT Security Consultant

Education, Training, and Certifications

- » Certified Information Systems Security Professional
- » Certified Ethical Hacker
- » Cisco Certified Network Associate
- » CompTIA Security+
- » IBM Certified Database Professional
- » Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
- » Bachelor's of Science in Accounting

Experience: IT Security

Ray Resnick is a Senior IT Consultant with over 20 years' experience in IT security, risk analysis, and regulatory compliance. His expertise includes:

- » Vulnerability Assessment
- » Penetration Testing
- » Application and Database Security
- » Firewall and IDS | IPS Deployment
- » Security Evaluations
- » Risk and Threat Analysis
- » Network Monitoring
- » Best Practice Deployment
- » Information Security Awareness Training
- » NIST, ISO, PCI, HIPAA, and SOX Compliance

Professional Experience

Copper Collar Enterprises - Information Security Engineer

- » Performed compliance, vulnerability, penetration, and physical security assessments to mitigate exposure
- » Designed strategies to address security control gaps and areas of non-compliance
- » Created information security and risk management awareness training programs
- » Led project team in data migration to Amazon Web Services (AWS)
- » Set up, monitored, and trained users in the operation of SIEMs, DLPs, and vulnerability scanners
- » Developed business continuity | disaster recovery plans
- » Supervised installation and configuration of perimeter security devices, including firewalls and IDS | IPS

Verizon Communications - Database Administrator and Senior Systems Engineer

- » Managed installs, loads, data conversions, backups, and configurations to increase database performance
- » Wrote procedures, triggers, and database views to increase efficiency and security
- » Designed, tested, and implemented application and database fail-over architecture
- » Upgraded hardware and created UNIX-based tools to monitor application and security processes and logs
- » Performed application testing, patch management, system process monitoring, and server clustering configurations

Technical Skills

- » Platforms - MS Windows, Linux, UNIX, Hyper-V, and KVM
- » Security Tools - Commercially available and open-source tools, including Wireshark, nMap, Kali Linux Suite, Security Onion, Nessus, Splunk, and Snort

Recent Clients



Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Key Personnel

Bill Tisch, LINUX+, CISSP, CISA, CEH, MCSA, MCSE, MCITP, MCTS — Senior IT Security Consultant

Education, Training, and Certifications

- » Certified Information Systems Security Professional
- » Certified Information Systems Auditor
- » Certified Ethical Hacker
- » Microsoft Certified Solutions Associate
- » Microsoft Certified Solutions Expert
- » Microsoft Certified IT Professional Enterprise Administrator and Server Administrator
- » Microsoft Certified Systems Engineer
- » Microsoft Certified Technology Specialist
- » Microsoft Certified Systems Administrator
- » Certified Unicenter Administrator
- » Cloud+, Security+, Network+, Linux+, A+
- » Master of Science in Computer Information Systems
- » Bachelor's of Arts in Economics

Experience: IT Security

Bill is a Senior IT Consultant with over 20 years' experience in IT security, risk analysis, and best practice implementation. His expertise includes:

- » Security Assessments
- » Vulnerability Assessment
- » Penetration Testing
- » Firewall and IDS | IPS Deployment
- » Web Portal Testing
- » Application and Database Security
- » Risk and Threat Analysis
- » VPN Solutions

Professional Experience

SOPHOS - Security Engineer

- » Support company's portfolio of security technologies, including firewall, host based protection, url filtering, CASB, encryption, application control, and synchronized security.
- » Provide scoping and design for product implementations

Auto Club Insurance Company (AAA) - Senior Security Engineer

- » Managed company's security technologies, including email filtering and security, url filtering, IPS, firewall, advanced malware protection, and wireless network security.
- » Provided vulnerability management administration and reporting for internal and external audit requirements.
- » Performed PCI compliance requirements.

US Centcom - IA Security Analyst

- » Administrated messaging systems including, Exchange and Blackberry Enterprise Server.
- » Performed network monitoring, IAVA remediation, system compliance and vulnerability scanning, patch management, and host system security.
- » Supported the Computer Network Defense (CND) team, providing, IA scanning and auditing, incident handling and response, specifically targeted towards computer incident response and restoration of a secure operating environment, investigation of intrusion events and analysis of exploits.

Technical Skills

- » Platforms - MS Windows 2012 and 2008, Linux
- » Security Tools - vSphere, vCenter, ESXi, HBSS, EPO 5 - 4.5, Policy Auditor, IBM \ Q1 QRadar, ArcSight, Security Manager, Splunk, SEP v14, ESA IronPort, WSA, AMP for Endpoints, Nessus Cloud, Tenable.io, Metasploit

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Key Personnel

Chris Cook, CISSP, CISA — Senior IT Security Consultant

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

Experience: IT Security

Chris Cook, a Senior IT Consultant with Securance for the last 10 years, has 25 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
- » Application Vulnerability Assessments
- » Regulatory Compliance Reviews and Testing
- » NIST, ISO, PCI, HIPAA, and SOX Compliance

Professional Experience

Ericsson - Senior Security Analyst

- » Assessed application security. Formulated 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 automated vulnerability scanning programs that scanned network devices and collected results
- » Developed and delivered in-house IT security training programs.

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.

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Additional Personnel

Ibrahim Badrawi, CCNA, CVA — IT Security Consultant

Education, Training, and Certifications

- » Cisco Certified Network Associate
- » Certified Vulnerability Assessor
- » Splunk Certified Core User
- » Bachelor's of Science in IT Management
- » Associate's Degree in Applied Science | Network Administration

Experience: IT Security

Ibrahim Badrawi is an IT Security Consultant with over 12 years' experience in IT and cybersecurity. With a deep understanding of attack scenarios and vulnerabilities, he has expertise in automated and manual vulnerability and penetration testing procedures, as well as the ability to analyze test results and develop actionable remediation plans. His specific areas of expertise include:

- » Cyber Threat Intelligence (Kill Chain and Diamond Model)
- » Network Security Management
- » Vulnerability and Penetration Testing
- » Cybersecurity Risk Assessment
- » Best Practice Deployment (e.g., NIST, ISO)
- » Regulatory Compliance (e.g., CJIS, HIPAA, PCI, SOC)
- » Splunk Implementation and Configuration

Professional Experience

Garmin - Cybersecurity Analyst II

- » Assisted with internal and external cybersecurity audits
- » Implemented cybersecurity processes and procedures to protect systems against unauthorized access, modification, and destruction
- » Planned and implemented network and system security settings
- » Performed vulnerability assessments and penetration tests and analyzed results
- » Conducted security assessments of web and mobile applications
- » Performed regular assessments of cybersecurity controls against best practice standards
- » Developed cybersecurity test plans and assessment reports
- » Monitored compliance with risk mitigation strategies and governance policies and procedures using ISO, SOC, NIST, and PCI standards
- » Monitored security operations center (SOC) queue for potential event reporting and maintained logs

O&P Technology Corporation - Cybersecurity Analyst I

- » Categorized business assets and data to support the cybersecurity risk management process
- » Responsible for correlation rule tuning, incident classification, and prioritization
- » Monitored incoming event queues for potential security incidents
- » Supported, monitored, and managed the SIEM environment
- » Tasked with cybersecurity triage, analysis, and response to security alerts as part of the incident response team
- » Initiated appropriate courses of action and escalation in response to security alerts
- » Set up continuous monitoring using Splunk. Monitored daily traffic, events, and logs using Splunk and WireShark
- » Monitored systems, detecting, analyzing, and resolving all incidents and events reported by the SIEM and IPS

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Additional Personnel

Ibrahim Badrawi, CCNA, CVA — IT Security Consultant (continued)

Interstate Hotels and Resorts - Cybersecurity Analyst

- » Identified and categorized physical and data assets to support the implementation of the Cybersecurity Risk Management Plan
- » Developed and briefed leadership on sustainable cybersecurity solutions to address areas of risk
- » Conducted Splunk manual health checks and identified license violations
- » Created Splunk dashboards to monitor server performance, CPU utilization, and disk usage
- » Conducted an annual review of contractor processes and procedures
- » Monitored and investigated network activities using Splunk, Snort, AlienVault, Nessus, and Nmap
- » Conducted vulnerability assessments and remediated vulnerabilities

Barclay's Bank - Cybersecurity Analyst

- » Monitored systems to support daily cybersecurity operations
- » Analyzed threat intelligence
- » Monitored and reported on network traffic flow, PCAP, logs, and sensors for evidence of cyber attack patterns and Advanced Persistent Threats
- » Performed network, database, and web application vulnerability assessments
- » Provided SOC support and worked with SIEM solutions
- » Performed analytical activities to support external threat monitoring, detection, event analysis, and incident reporting efforts

Technical Skills

- » Platforms - MS Windows, Linux, UNIX, Oracle Database, MS SQL Server, and relational databases
- » Security Tools - Commercially available and open-source tools, including Splunk, AlienVault, Nmap, pfSense, Nessus, Metasploit, Wireshark, and Snort
- » Security Analysis and Testing - SOC analysis, penetration testing, identity and access management (IAM) security assessment and testing, network forensics and packet analysis, root cause analysis

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Additional Resources

Parves Kamal, CEH, Security+, RHCSA, RHCE — IT Security Consultant

Education, Training, and Certifications

- » Master of Science, Information Assurance - St. Cloud State University (2017) #COMPOO1020320671
- » Bachelor of Science, Computer Security and Forensics - University of Bedfordshire (2012; Awarded with Honors) » Red Hat Certified System Administrator - License #160-133-666
- » Certified Ethical Hacker - License #ECC55978706460 » Red Hat Certified Engineer - License #160-133-666
- » CompTIA Security+ - License » Qualys Certified Specialist - Vulnerability Management
- » Proofpoint Accredited Administrator

Experience: IT Security

Parves has over seven years' experience in IT security operations and the implementation, integration, and operation of security technologies, such as SIEM, DLP, IDS/IPS, network analysis, anti-virus and anti-malware, and endpoint protection solutions. His areas of expertise and accomplishments include:

- » Experience in planning, developing, implementing, monitoring, and updating security programs and technical security solutions
- » Advanced knowledge of NIST and ISO standards and PCI and SOX compliance requirements
- » Technical expertise in network and system analysis, intrusion detection, and malware analysis
- » Advanced knowledge of authentication, end point security, IDS/IPS, DLP, IAM, and user behavior analytics solutions
- » Ability to identify and develop detailed recommendations to remediate network and system security vulnerabilities
- » Knowledge of LAN/WAN networking concepts, including TCP/IP, routing and switching, the OSI model, and scripting languages

Professional Experience

Synchrony Financial - Cybersecurity Senior SOC Analyst

- » Successfully trained 26 new SOC analysts in tools and processes.
- » Reviewed and validated incidents using Splunk Enterprise Security. Used Sourcefire to co-related events and tune alerts to decrease false positives.
- » Conducted active hunting using RSA Net Witness to support red and blue team exercises.
- » Used Tanium dynamic search query and the IOC/Trace module to identify technical vulnerabilities. Built several Tanium signals to send alerts regarding vulnerabilities and IOCs to Splunk Enterprise Security.
- » Used Forescout to detect and remediate rogue and unmanaged devices on the network.
- » Proactively used Proofpoint and other tools for dynamic email analysis to gather threat intelligence and actively respond to phishing attempts.
- » Monitored user behavior for lateral movement using Exabeam.
- » Acted as a mentor for Tier 1 Analysts and advised junior staff to assist to challenging technical issues.
- » Worked with multiple customer environments, both on premise and virtually. Provided recommendations to harden and improve security in customer environments.
- » Created scripts in Python to simplify and automate tasks.

Written Narrative Statement

Specific Proposal Instructions, B.3. — Consultant Resumes — Additional Personnel

Parves Kamal, CEH, Security+, RHCSA, RHCE — IT Security Consultant (continued)

Rackspace - Senior IT Security Analyst

- » Responsible for AWS security. Used Splunk to monitor configuration changes in AWS resources.
- » Maintained and monitored network security using various tools and technologies, including IDS | IPS, network sniffing tools, Wireshark, TCPDUMP, and Nmap. Conducted regular vulnerability and compliance scans and provided reports.
- » Conducted web application security assessments, testing for threats that included the OWASP Top 10.
- » Planned, implemented, and managed the vulnerability scanner environment. Acted as Subject Matter Expert and provided technical expertise and guidance regarding the vulnerability scanner environment.
- » Conducted senior-level log analyses, proactive monitoring, mitigation, and incident response. Investigated, handled, and created tickets and reports for security incidents.
- » Captured and analyzed network packets (PCAP) and developed detailed reports using Wireshark.
- » Analyzed security event data from IDS sensors and firewall traffic.
- » Identified suspicious and malicious malware using static and dynamic analyses.

Ameriprise Financial - IT Security Analyst

- » Responsible for network monitoring and server compliance with configuration standards.
- » Evaluated and architected IT security solutions for the enterprise to improve defense-in-depth.
- » Produced custom Splunk TAs for forwarders, search peers, and indexer. Monitored and acquired data feeds from various technologies integrated with Splunk (firewalls, BlueCoat proxy, Windows, Linux, Imperva, etc.)
- » Deployed, configured, and monitored the DLP device. Created DLP role-based access controls, device policies, and application file access protection. Performed DLP inventory scans.
- » Secured Internet access using BlueCoat proxies. Engineered BlueCoat policies to follow the company's internal security policies and procedures.
- » Constructed actionable reports and alerts from RSA Security Analytics.
- » Installed and configured Symantec Enterprise Anti-Virus.
- » Administered and managed Symantec Endpoint Protection client deployments to workstations and servers.
- » Conducted network vulnerability assessments and developed remediation plans.
- » Provided consultative services at the time of PCI reviews and audits.

Technical Skills

- » Platforms - Linux, Windows, Red Hat, and UNIX
- » Programming Languages - Bash, Python, Perl, and PowerShell
- » Security Tools - Backtrack 4, BlueCoat, Cain & Abel, C|EH Modules, Ettercap, Exabeam, Forescout, Imperva, Nessus, Nmap, OPSView, OSSEC, Proofpoint, Quays, RSA, Snort, Splunk, SourceFire, Symantec Endpoint Protection, Tanium, Tripwire, Wireshark

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. **QUALIFICATIONS OF OFFEROR:** Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.
2. **YEARS IN BUSINESS:** Indicate the length of time you have been in business providing these types of goods and services.

Years 17 Months 7

3. **REFERENCES:** Indicate below a listing of at least five (5) organizations, either commercial or governmental/educational, that your agency is servicing. Include the name and address of the person the purchasing agency has your permission to contact.

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

4. List full names and addresses of Offeror and any branch offices which may be responsible for administering the contract.

Offeror: Securance LLC, 13904 Monroes Business Park, Tampa, FL 33635

5. **RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA:** Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the [CODE OF VIRGINIA](#), SECTION 2.2-3100 – 3131?

[] YES [X] NO

IF YES, EXPLAIN:

ATTACHMENT B

Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Offeror Name: Securance LLC **Preparer Name:** Paul Ashe

Date: 10/21/19

Is your firm a **Small Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes ☐ No ☒

If yes, certification number: _____ Certification date: _____

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes ☐ No ☒

If yes, certification number: _____ Certification date: _____

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes ☐ No ☒

If yes, certification number: _____ Certification date: _____

Is your firm a **Micro Business** certified by the Department of Small Business and Supplier Diversity (SBSD)? Yes ☐ No ☒

If yes, certification number: _____ Certification date: _____

Instructions: *Populate the table below to show your firm's plans for utilization of small, women-owned and minority-owned business enterprises in the performance of the contract. Describe plans to utilize SWaMs businesses as part of joint ventures, partnerships, subcontractors, suppliers, etc.*

Small Business: "Small business " means a business, independently owned or operated by one or more persons who are citizens of the United States or non-citizens who are in full compliance with United States immigration law, which, together with affiliates, has 250 or fewer employees, or average annual gross receipts of \$10 million or less averaged over the previous three years.

Woman-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more women who are U.S. citizens or legal resident aliens, or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more women, and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified women-owned businesses are also a small business enterprise.**

Minority-Owned Business Enterprise: A business concern which is at least 51 percent owned by one or more minorities or in the case of a corporation, partnership or limited liability company or other entity, at least 51 percent of the equity ownership interest in which is owned by one or more minorities and whose management and daily business operations are controlled by one or more of such individuals. **For purposes of the SWAM Program, all certified minority-owned businesses are also a small business enterprise.**

Micro Business is a certified Small Business under the SWaM Program and has no more than twenty-five (25) employees **AND** no more than \$3 million in average annual revenue over the three-year period prior to their certification.

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Small Business and Supplier Diversity (SBSD) to be counted in the SWAM program. Certification applications are available through SBSD at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at <http://www.sbsd.virginia.gov/> (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

*Securance is certified as a DBE through the Department of Small Business and Supplier Diversity with certification #701667. We are not certified as a SWaM, because Florida businesses are ineligible.

ATTACHMENT B (CNT'D)
Small, Women and Minority-owned Businesses (SWaM) Utilization Plan

Procurement Name and Number: RFP #FDC-1057 Information Technology Security Auditing Services Date Form Completed: 10/21/19

**Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses
for this Proposal and Subsequent Contract**

Offeror / Proposer:

Securance LLC
Firm

13904 Monroes Business Park, Tampa, FL 33635
Address

Paul Ashe, 877-578-0215
Contact Person/No.

Sub-Contractor's Name and Address	Contact Person & Phone Number	SBSD Certification Number	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)
N/A. Securance will not subcontract any of the work associated with this solicitation.					

(Form shall be submitted with proposal and if awarded, again with submission of each request for payment)

RETURN OF THIS PAGE IS REQUIRED

Specific Proposal Instructions, B.6.

Sales with VASCIPP Member Institutions

Identify the amount of sales your company had during the last twelve months with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: www.VASCUPP.org.

Securance has not performed any work in the last twelve months for any VASCUPP Member Institution.



PROPOSED COST

We have provided hourly rates by labor category below. All rates are inclusive of travel, lodging, and other billable on-site fees.

Labor Category	Hourly Rate
Project Manager	\$128
Senior IT Security Consultant	\$124
IT Security Consultant	\$120
IT Security Analyst	\$110

Charge Card Processing Fees

Not applicable. Securance does not accept credit card payments.



13904 Monroes Business Park • Tampa, FL 33635
www.securanceconsulting.com