VCU Procurement Services

**Procurement Services**
University Purchasing

912 W Grace Street, 5th Floor
Box 980327
Richmond, Virginia 23284

804 828-1077
Fax: 804 828-7837
TDD: 1-800-828-1120
www.vcu.edu/procurement

Date: June 23, 2021

Wendy Foote
NTT Security AppSec Solutions Inc. dba WhiteHat Security
1741 Technology Drive, Suite #300
San Jose, CA 95110

RE: Contract #: 7286528JC
Renewal No.: Two (2) of Two (2)

Dear Ms. Foote,

Your firm's contract with Virginia Commonwealth University (VCU) for the WhiteHat Sentinel Application Vulnerability Scanner expires on June 30, 2021. VCU intends to exercise the renewal of this contract in accordance with the contract terms and conditions for the period July 1, 2021 through June 30, 2022.

Please facilitate obtaining the authorized WhiteHat Security, Inc. signature below to indicate acceptance of this renewal, and return the document to me within 10 business days. Your response may be emailed to aranthes@vcu.edu. If you have any questions, please contact me at (804) 828-1070.

___ Pricing remains the same as the previous contract period.

___ Attached is the revised pricing in accordance with the contract terms.

___ By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.

Sincerely,

Amy Anthes
Category Manager

Contract #: : 7286528JC

**RESPONSE:**

NTT Security AppSec Solutions Inc. dba WhiteHat Security

Name of Firm

DocuSigned by:

Wendy Foote

E6C9EB4D52254B4...

Signature

Wendy Foote

Name Printed

Senior Contracts Manager

Title

6/28/2021

Date

VCU Procurement Services

**Procurement Services**
University Purchasing

912 W Grace Street, 5th Floor
Box 980327
Richmond, Virginia 23284

804 828-1077
Fax: 804 828-7837
TDD: 1-800-828-1120
www.vcu.edu/procurement

Date: May 1, 2020

Wendy Foote
WhiteHat Security, Inc.
3970 Freedom Circle
Suite 200
Santa Clara, CA 95054

RE: Contract #: 7286528JC
Renewal No.: One (1) of Two (2)

Dear Ms. Foote,

Your firm's contract with Virginia Commonwealth University (VCU) for the WhiteHat Sentinel Application Vulnerability Scanner expires on June 30, 2020. VCU intends to exercise the renewal of this contract in accordance with the contract terms and conditions for the period July 1, 2020 through June 30, 2021.

Please facilitate obtaining the authorized WhiteHat Security, Inc. signature below to indicate acceptance of this renewal, and return the document to me within 10 business days. Your response may be emailed to aranthes@vcu.edu. If you have any questions, please contact me at (804) 828-1070.

____ Pricing remains the same as the previous contract period.

____ Attached is the revised pricing in accordance with the contract terms.

____ By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.

Sincerely,

Amy Anthes
Category Manager

Contract #: : 7286528JC

**RESPONSE:**

WhiteHat Security, Inc.
Name of Firm

DocuSigned by:
Wendy Foote
E6C9FB4D52254B4...
Signature

Wendy Foote
Name Printed

Senior Contracts Manager
Title

5/5/2020
Date

VCU Procurement Services

Date: June 18, 2019

**Procurement Services**
University Purchasing

912 W Grace Street, 5th Floor
Box 980327
Richmond, Virginia 23284

804 828-1077
Fax: 804 828-7837
TDD: 1-800-828-1120
www.vcu.edu/procurement

WhiteHat Security, Inc.
3970 Freedom Circle, Suite 200
Santa Clara, CA 95054

RE: Contract #: 7286528JC
Renewal No. Two
Current Purchase Order: EP2763840

Dear Mr. Perkins,

Your firm’s contract with Virginia Commonwealth University (VCU) for Application Vulnerability Scanner expires on June 30, 2019. VCU intends to exercise the renewal of this contract in accordance with the renewal terms of contract # 7286528JC

Your signature constitutes your firm’s acceptance of this renewal, to include the optional use language and the eVA registration requirement provisions below.

____ Pricing remains the same as the previous contract period.

____ Attached is the revised pricing in accordance with the contract terms.

____ By signing and submitting this contract renewal letter Contractor certifies that it will maintain the insurance coverages required at the time the contract was awarded. At renewal, Contractor shall have a new Certificate of Insurance listing VCU as the "Additional Insured", citing the contractor's name and contract number, mailed to VCU Risk Management, Box 843040, Richmond, VA.

Please return this document to me. Your response may be emailed to me at aranthes@vcu.edu. If you have any questions, please contact me at (804) 828-1070.

Sincerely,
Amy Anthes
Category Manager

Contract #: : WhiteHat Security Quote #Q00041784

**RESPONSE:**

WhiteHat Security, Inc.
Name of Firm

DocuSigned by:
Wendy Foote
E6C9EB4D52254B4...
Signature

Wendy Foote
Name Printed

Senior Contracts Manager
Title

7/16/2019
Date

VIRGINIA COMMONWEALTH UNIVERSITY

VCU

Make it real.

## COMMONWEALTH OF VIRGINIA
## STANDARD CONTRACT

**Contract Number: 7286528JC**

This contract entered into by WhiteHat Security, Inc., hereinafter called the "Contractor" and Commonwealth of Virginia, Virginia Commonwealth University (VCU), 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:

**PERIOD OF THE PERFORMANCE**: From the award of the contract through June 30, 2018 with four (4) successive one year renewal options.

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

The contract documents shall consist of:

(1) This signed form; and in order of precedence;
(2) The Negotiated Modifications dated May 8, 2017
(3) Negotiated RFP #7286528JC General Terms and Conditions, Special Terms and Conditions, and Special Terms and Conditions Information Technology dated June 14, 2017
(4) The WhiteHat Proposal Dated January 5, 2017
(5) RFP #7286528JC dated November 29, 2016 and Addendum #1 dated December 16, 2017
(6) Appendix A dated June 14, 2017
(7) Service Order(s)

All of which documents are incorporated herein by reference.

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

**CONTRACTOR:**
WhiteHat Security, Inc.

By:
Name Printed: Garrett McGonigal
Title: Senior Contract Manager
Date: June 23, 2017

**PURCHASING AGENCY:**
Virginia Commonwealth University

By: Karol Kain Gray
Name Printed: Karol Kain Gray
Title: Vice President for Finance and Budget
Date: 6/27/17

VIRGINIA COMMONWEALTH UNIVERSITY

VCU

# Request for Proposals

RFP #: 7286528JC

RFP Title #: Application Vulnerability Scanner

Issuing Agency: Virginia Commonwealth University

Using Dept.: Technology Services

Issue Date: November 29, 2016

Closing Date: January 6, 2017 at 11:00 AM

VIRGINIA ASSOCIATION
OF STATE COLLEGE &
UNIVERSITY PURCHASING
PROFESSIONALS

VASCUPP

A VASCUPP Member Institution

## Request for Proposals RFP #7286528JC

**Issue Date:** November 29, 2016

**Title:** Application Vulnerability Scanner

**Send all Proposals To:**
Virginia Commonwealth University
RFP #7286528JC
Attention: Jackie Colbert
912 W Grace St, 5th floor
Richmond, Virginia 23284

**Proposals Shall Be Received Until: January 6, 2017 at 11:00 AM**

**Direct ALL inquiries concerning this RFP to: Jackie Colbert, Information Technology Category Manager**
**jcolbert@vcu.edu**

**Questions concerning this RFP must be received via email no later than: December 8, 2016 at 2:00 PM EST**

This Request for Proposals & any Addenda are posted on the eVA website at: http://www.eva.virginia.gov

HARD-COPY, ORIGINAL PROPOSALS MUST BE RECEIVED IN VIRGINIA COMMONWEALTH UNIVERSITY'S DEPARTMENT OF PROCUREMENT SERVICES ON OR BEFORE THE DATE AND TIME DESIGNATED ON THIS SOLICITATION. ELECTRONIC SUBMISSIONS AND FACSIMILE SUBMISSIONS WILL NOT BE ACCEPTED IN LIEU OF THE HARD-COPY, ORIGINAL PROPOSAL. VENDORS ARE RESPONSIBLE FOR THE DELIVERY OF THEIR PROPOSAL. PROPOSALS RECEIVED AFTER THE OFFICIAL DATE AND TIME WILL BE REJECTED. THE OFFICIAL DATE AND TIME USED IN RECEIPT OF RESPONSES IS THAT TIME ON THE CLOCK OR AUTOMATIC TIME STAMP IN THE DEPARTMENT OF PROCUREMENT SERVICES.

**IF PROPOSALS ARE HAND DELIVERED OR SENT BY FEDEX, UPS, OR ANY OTHER PRIVATE COURIER, DELIVER TO THE ADDRESS NOTED ABOVE: VIRGINIA COMMONWEALTH UNIVERSITY, RFP #7286528JC, ATTENTION: Jackie Colbert, 912 W. GRACE ST., 5TH FLOOR, RICHMOND, VA 23298-0327.** IF USING US MAIL (NOT RECOMMENDED): IF PROPOSALS ARE MAILED VIA US MAIL ONLY, MAIL TO VIRGINIA COMMONWEALTH UNIVERSITY, RFP#7286528JC, ATTN: Jackie Colbert, PO BOX 980327, RICHMOND, VA 23298-0327. THE RFP NUMBER, DATE AND TIME OF PROPOSAL SUBMISSION DEADLINE, AS REFLECTED ABOVE, MUST CLEARLY APPEAR ON THE FACE OF THE RETURNED PROPOSAL PACKAGE.

In Compliance With This Request for Proposals And To All Conditions Imposed Therein and Hereby Incorporated By Reference, The Undersigned Offers And Agrees To Furnish The Goods/Services Described Herein In Accordance With The Attached Signed Proposal Or As Mutually Agreed Upon By Subsequent Negotiation. Furthermore, The Undersigned Agrees Not To Start Any Work Relative To This Particular Solicitation Until A Resulting Formal Signed Purchase Order Is Received By The Contractor From University's Department of Procurement Services. Any Work Relative To This Request for Proposals Performed By The Contractor Prior To Receiving A Formal Signed Purchase Order Shall Be At The Contractor's Own Risk And Shall Not Be Subject To Reimbursement By The University. **Signature below constitutes acknowledgement of all information contained through links referenced herein.**

**NAME AND ADDRESS OF** COMPANY:

_______________________ Date: _______________________

_______________________ By *(Signature In Ink)*: _______________________

__________ Zip Code __________ Name Typed: _______________________

E-Mail Address: _______________ Title: _______________________

Telephone: (____) _______________ Fax Number: (____) _______________

**Toll free, if available** **Toll free, if available**

DUNS NO.: _______________ FEI/FIN NO.: _______________

REGISTERED WITH eVA: ( ) YES ( ) NO SMALL BUSINESS: ( ) YES ( ) NO

VIRGINIA DSBSD CERTIFIED: ( ) YES ( ) NO MINORITY-OWNED: ( ) YES ( ) NO

DSBSD CERTIFICATION #: _______________ WOMEN-OWNED: ( ) YES ( ) NO

**A Pre-Proposal conference will be held. See Section V herein.**

**THIS SOLICITATION CONTAINS 31 PAGES.**

## TABLE OF CONTENTS

## I. PURPOSE:

The intent and purpose of this Request for Proposals (RFP) is to solicit proposals from qualified suppliers for an application vulnerability scanner for Technology Services at Virginia Commonwealth University (the lead issuing institution and hereafter referred to as "the University" or "VCU"), an agency of the Commonwealth of Virginia.

It is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institution or lead-issuing institution's affiliated foundations may access any resulting contract(s) if authorized by the Contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) may be extended to the entities indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify the lead-issuing institution in writing of any entities accessing the contract. No modification of this contract or execution of a separate contract is required to participate. The Contractor shall provide usage reports for all entities accessing the Contract upon request. Participating entities shall place their own orders directly with the Contractor(s) and shall fully and independently administer their use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the lead-issuing institution. The lead-issuing institution shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the lead-issuing institution is not responsible for the acts or omissions of any entity, and will not be considered in default of the Agreement no matter the circumstances.

Use of this contract(s) does not preclude any participating entity from using other contracts or competitive processes.

## II. GOVERNING RULES:

This solicitations is issued in accordance with the provisions of:

A. Purchasing Manual for Institution of Higher Education and their Vendors (https://vascupp.org)

B. Rules Governing Procurement of goods, Services, Insurance, and Construction by a Public Institution of Higher Education of the commonwealth of Virginia (https://vascupp.org)

## III. OPTIONAL USE CONTRACT:

The resulting contract(s) will be an optional use contract. VCU is in no way required to make purchases from the Contractor and may in its sole discretion purchase the identical and/or similar goods/services from other sources. Any estimates/quantities contained herein do not represent a purchase commitment by VCU.

## IV. THE UNIVERSITY:

Virginia Commonwealth University (VCU) is a large urban University located in Richmond, Virginia. The University has 13 schools and 1 college offering over 220 undergraduate, graduate, doctoral and certificate programs, and conducted over $270 million in sponsored research in fiscal year 2016. With more than 31,000 students and 21,000 full- and part-time employees in both VCU and VCU Health, the University is recognized as both one of the largest Universities in Virginia, and the largest employer in Richmond.

Additional information is available at:
http://documents.procurement.vcu.edu/purchasing/pdf_docs/forms/RFP_Website_Link_The_University.pdf

## V. PRE-PROPOSAL CONFERENCE:

An optional pre-proposal conference will be held at **2:00 PM on December 14, 2016** at the:

VCU Facilities and Financial Services Building
700 West Grace Street
Suite 2200
Richmond, Virginia 23220

Note: – Offerors should submit questions about the RFP via email by December 8, 2016 at 2:00 PM EST to jcolbert@vcu.edu.

**For directions and paid parking information visit:**
**http://business.vcu.edu/about-the-school/our-location/directions--parking/**

The purpose of the conference is to allow Offerors an opportunity to ask questions and obtain clarification relative to any facet of this solicitation.

While attendance at this conference is optional, Offerors who intend to submit a proposal are highly encouraged to attend and to have a copy of this solicitation to reference. Any questions and answers that are presented during the conference or any changes to the solicitation resulting from this conference will be issued in a written addendum to the solicitation.

- Offerors may participate in the optional pre-proposal conference via conference call by:
- - Using the following "Dial-In" numbers:
- - 866-842-5779 (United States & Canada);
- - 832-445-3763 (International);
- - Using Conference Code #: 8415263709
- - Dialing the appropriate "Dial-In" number at the scheduled time; and
- - Entering the "Conference Code" when prompted, followed by the "#."

Note: Offerors who participated in the pre-proposal conference via conference call shall submit an email to jcolbert@vcu.edu within one (1) business day of the pre-proposal conference, confirming the Offerors participation and the Offeror's contact information.

## VI. STATEMENT OF NEEDS:

A. Scope and Introduction

1. VCU currently manages its IT operations through a hybrid approach, where most infrastructure services are managed centrally through the central Office of Technology Services ("OTS"), and customer facing services are managed in a decentralized fashion by individual schools and departments. Among the decentralized services, application development and provisioning are usually managed by individual departments and schools, with support of these applications

collectively managed by both OTS and individual departmental groups. From a central services perspective, application provisioning guidance and general policies are available, but there is presently no streamlined process for verifiable implementation of the recommended and required controls.

2. In order to minimize variances in the provisioning of applications and to ensure quality and security of applications before deploying them into production, VCU is currently developing an application vulnerability management program that integrates key processes, personnel, and technology to address the aforementioned challenges. From a technical architecture perspective, a critical component in this initiative is an application vulnerability scanner. The application vulnerability scanner is expected to help VCU in identifying, prioritizing, and tracking vulnerabilities in both internally-developed and third-party applications in use at the University. This Request for Proposals (RFP) is designed to help VCU select an appropriate application vulnerability scanner that can be integrated into it's application vulnerability management program.
3. Initially, the application vulnerability program will have 100 developers at the University and up to 247 applications (excluding cloud applications).

B. The Contractor shall furnish, deliver, implement and provide ongoing maintenance and support, and training for the application vulnerability scanner.

1. The Contractor shall provide support for the product through phone, self-service ticketing systems, and / or email on normal business hours (M-F 8 AM – 5 PM EST). 24x7x365 phone or email support for system is strongly preferred.

2. The Contractor shall provide standard service level agreement indicating anticipated response times for service requests. At a minimum, the initial response time for support requests cannot exceed 3 business days.

3. The Contractor shall provide optional on-site training, support, or upgrade service for the product.

4. The Contractor shall provide options for request escalation for situation where rapid response or additional expertise is needed.

C. The application vulnerability scanner shall be covered by the most favorable commercial warranties the Contractor gives any customer for the system.

D. Mandatory Solution Requirements – The application vulnerability scanner shall at a minimum have the following specifications:

1. The application vulnerability scanner must provide up-to-date vulnerability data that allows the accurate detection of potential vulnerabilities in applications.
2. The application vulnerability scanner must provide a central management console that displays vulnerability and trending data for all tested application.
3. The application vulnerability scanner must have tiered management capability within the aforementioned central management console, where users of the console can be assigned roles and responsibilities based on individual responsibilities, and the principle of least privilege.
4. The application vulnerability scanner must have the ability to conduct Dynamic Application Security Testing (DAST) of an application in testing or production environment, while minimizing impact to application availability.

5. The application vulnerability scanner must have the ability to conduct Static Application Security Testing (SAST) that supports (at a minimum) the testing of: Java, Javascript, C#, and PHP code.
6. The application vulnerability scanner must have the ability to clearly explain vulnerability details, potential impact, risk rating, and proposed remediation options, in a manner and timeframe that is actionable to developers and system administrators.
7. The application vulnerability scanner must have the ability to track the vulnerability state for each application, and offer long term trending data for the security state of an application.
8. The Contractor shall provide the option to deploy the application vulnerability scanner as a service in a hosted environment either directly to VCU or through a third party.
9. The application vulnerability scanner shall provide the ability to integrate the vulnerability data into multiple continuous integration platforms, bug trackers, and integrated development environments (IDEs).
10. The application vulnerability scanner shall have the ability to generate customizable reports of vulnerabilities based on individual applications, and for the organization as a whole.
11. The application vulnerability scanner shall provide the ability to schedule the automated assessment of applications.
12. The Contractor shall assist VCU in developing hiring and training processes for familiarizing developers with the product with the goal of maximizing product value and utilization.

E. Preferred Options and Services –The items listed below are not strict requirements for product selection, but are desired by the University, and will be given additional consideration.

1. Ability for vendor to offer Runtime Application Security Protection (RASP) option.
2. Ability for the aforementioned console to provide authentication to developers and security personnel via Jasig CAS single sign-on.
3. Ability to organize and group applications based on owners and / or business units.
4. Ability to generate customizable reports of vulnerabilities based on application owners and / or business units.
5. Ability to perform vulnerability assessments on multiple applications simultaneously.
6. Provision of a full featured Software as a Service solution for both DAST and SAST implementations.
7. Ability for vendor to offer an easy to use and intuitive executive dashboard that shows top vulnerable applications, trending data, and risk scores.
8. Ability for vendor to offer tiered management system that allows individual administration rights by single application administrator, application group administrator, and global administrator.
9. Ability for vendor to provide detailed explanation of the vulnerability including proof of concept exploit code, and suggested remediations based on the original code (i.e. rather than generic examples).
10. Ability to attach metadata to applications so that applications can be classified by arbitrary labels and categories.
11. Ability for vendor to provide prompt technical support via phone, chat, or email to application developers using the platform
12. Ability for the application vulnerability scanner to provide workflow automation that enables the automated notification of vulnerabilities and changes in risk posture.

F. Procurement Requirements:

1. Freight terms shall be F.O.B. Destination/Prepaid with inside delivery; additional charges shall not be allowed.
2. The terms and conditions of the RFP govern the resulting contract and not any Contractor terms and conditions or software license agreement.
3. The proposal prices shall include all costs for the equipment and services including all applicable freight and travel and living expenses; extra charges will not be allowed.
4. The initial contract term is from the award and continues for one (1) year after the implementation is complete and the system is accepted with four (4) annual, optional renewal terms.

## VII. PROPOSAL PREPARATION AND SUBMISSION INSTRUCTIONS:

A. Proposal Submission Instructions:

1. Complete and return Page 2 of the RFP. Proposals shall be signed by an authorized representative of the Offeror.
2. Complete and return signed addenda acknowledgments (if applicable).
3. Submit **one (1) original hard copy (paper)** of the entire proposal, including all attachments and proprietary information. The original proposal must be clearly marked on the outside of the proposal. Submit one (1) unsecured, electronic copy (on a disc or flash drive) of the entire proposal including all attachments and **INCLUDING ANY PROPRIETARY INFORMATION** and one (1) unsecured, electronic copy (on a disc or flash drive) of the entire proposal including all attachments and **EXCLUDING ANY PROPRIETARY INFORMATION**. These discs or flash drives must be clearly marked on the outside whether it includes or excludes proprietary information. The copies of the RFP in this Section are for Procurement Services.
4. Submit six (6) hard copies (paper copies) of the entire proposal, **INCLUDING ALL ATTACHMENTS AND ANY PROPRIETARY INFORMATION** and six (6) **unsecured electronic copies** (on a disc or flash drive) of the **entire** proposal, **INCLUDING ALL ATTACHMENTS AND ANY PROPRIETARY INFORMATION** for the Evaluation Committee Members.
5. Proposal Presentation:

   a. All information requested must be submitted. Failure to submit all information requested may result in the Purchasing Agency requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Proposals which are substantially incomplete or lack key information may be rejected by the purchasing agency. Mandatory requirements are those required by law or regulation or are such that they cannot be waived and are not subject to negotiation.

   b. All information requested by this Request for Proposals on the ownership, utilization and planned involvement of small businesses, women-owned businesses and minority-owned businesses must be submitted. If an Offeror fails to submit all information requested, the Purchasing Agency may require prompt submission of missing information after the receipt of Contractors proposals.

   c. Proposals should be prepared simply and economically, providing a straightforward, concise description of capabilities to satisfy the requirements of the RFP. Emphasis should be placed on completeness and clarity of content.

   d. Proposals should be organized as specified in the RFP. All pages of the proposal should be numbered. The proposal should contain a table of contents, which cross-references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find the RFP requirements are specifically addressed.

e. Each copy of the proposal should be bound or contained in a single volume where practical. All documentation submitted with the proposal should be contained in that single volume.

6. If applicable, the outside of the Proposal must be marked to clearly denote proprietary information is contained in the documents. ***Written notice of proprietary information must be submitted as the first page of the Offeror's Proposal***. Notice must specifically identify the applicable portions of the Offeror's Proposal that contain data or materials to be protected and shall state the reasons why protection is necessary. In addition, the specific (i.e. specific words, figures or paragraphs) proprietary or trade secret material submitted must be identified on the applicable page(s) within the Offeror's Proposal, by some distinct method, such as highlighting, underlining, etc. The classification of an entire Proposal document, line item prices and/or total Proposal prices as proprietary or trade secrets is not acceptable and may result in rejection and return of the Proposal. Ownership of all data, materials and documentation originated and prepared for VCU pursuant to the RFP shall belong exclusively to the University and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the Offeror must invoke the protections of Section 43F of The Governing Rules, in writing, either before or at the time the data or other material is submitted.

7. Communications regarding this Request for Proposals (RFP) shall be formal from the date of the issuance for this RFP, until either a Contractor has been selected or the University Procurement Services Department rejects all proposals. Formal communications shall be directed to the University Procurement Department only. Informal communications including but not limited to, request for information, comments or speculations, regarding this RFP to any University employee other than Procurement Services Department representative may result in the offending Offeror's Proposal being rejected.

8. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to conduct an oral presentation of their proposal to VCU. Oral presentations are an option and may or may not be required. Should an oral presentation be required, VCU will designate the date and location for the presentation; the date is critical and alternative dates will not be available. Offerors who are invited to conduct an oral presentation shall include the individual(s) who would be the primary point of contact for VCU, on the Offerors presentation team. VCU reserves the right to re-score proposals following oral presentations.

9. The version of the solicitation issued by the Virginia Commonwealth University Purchasing Department as amended by any addenda is the mandatory controlling version of the document. Any modification of or additions to the solicitation by the Offeror shall not modify the official version of the solicitation issued by the Virginia Commonwealth University Purchasing Department unless accepted in writing by the University. Such modifications or additions to the solicitation by the Offeror may be cause for rejection of the proposal; however, Virginia Commonwealth University reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a proposal. If the modifications or additions are not identified until after the award of the contract, the controlling version of the solicitation document shall still be the official state form issued by the Purchasing Department.

10. Additional information is available at:

    http://go.vcu.edu/procurement-purchasing

B. SPECIFIC PROPOSAL REQUIREMENTS:

Proposals should be as thorough and detailed as possible so that VCU may properly evaluate your capabilities to provide the required goods/services. Offerors are required to submit the following items as a complete proposal:

1. The return of the entire RFP cover sheet and all addenda acknowledgments, if any, signed and filled out as required.
2. Proposed Price. Describe in detail the proposed license model for the application vulnerability scanner. Indicate in the Pricing Schedule, Section VIII of the RFP the proposed price to include all costs associated with the license(s), any hardware or appliances, implementation, hosting, maintenance, and training to include all proposed products and services. Additional charges shall not be allowed.
3. Describe the proposed plans and approach for providing the products and services as specified in the RFP. Consider the technical requirements in Section VI, Statement of Needs, Items A through E in the context of implementation and ongoing support, costs of upgrade and replacement, implementation timeline expectations, and costs of warranty and maintenance. Specifically indicate what is included in the offer to provide the required products and services by responding to all Items in Section VI, Statement of Needs, Items A through F. In addition, provide information for the Items listed below, but do not limit information to these Items:

   a. Utilization of the words "shall" or "must" in Section VI, Statement of Needs, Items A through E indicates mandatory technical requirements:

   Does / Shall your company comply with the mandatory technical requirements as presented in Section IV, Statement of Needs, Items A through E?

   Yes ____ No _____

   If "NO," identify the specific requirement and the reason for non-compliance.

   Utilization of the words "should" or "may" in Section VI, Statement of Needs, Items A through E indicates a non-mandatory requirement.

   Does / Shall your company comply with the non-mandatory technical requirements as presented in Section VI, Statement of Needs, Items A through E (i.e. "should" becomes "shall")?

   Yes ____ No _____

   If "NO," identify the specific requirement and the reason for non-compliance.

   b. The vendor will provide a full list of supported programming languages and frameworks for the SAST product. See Section VI.D.5.

   c. Provide a full list of supported continuous integration platforms, bug trackers, and IDEs. See Section VI.D.9.

   d. Describe in detail the proposed hiring and training processes. See Section VI.D.12.

   e. Describe in detail the proposed maintenance and support. See Section VI.B.

   f. Describe in detail the optional on-site training that your company is proposing.

g. Submit a copy of the warranty. State the start of the warranty period and the end of the warranty period.

h. Provide an implementation schedule indicating how long after the award of the contract it shall take your company to allocate the resources and deliver and install the system for use at VCU.

i. Describe the process for problem resolution for the proposed products and services.

j. Does your company agree with the Procurement Requirements in Section VI.F.?

Yes _____ No ______

If "NO," identify the specific term and condition(s) and the reason for non-compliance.

4. Submit information about the qualifications and experience that your company has to provide the Application Vulnerability Scanner products and services.

   a. Describe the firm's qualifications and experience providing the required products and services during the last three (3) years. Information provided should include, but is not limited to, comparable accounts in higher education and the scope of the services. Include information for a minimum of three (3) similar accounts, describing the types of projects and the scope of the services provided. Please include contact information with the name, address, email address and current phone number.

   b. Specify the proposed personnel your company intends to assign to the project and provide proof of the expertise for the proposed system. Information needed includes but is not limited to the names, qualifications, and experience of professional IT services technicians to be assigned to the project. Resumes of staff to be assigned to the project may be used.
   c. Does the offer include a single primary point of contact for the VASCUPP institutions for sales, support and problem resolution? If so, please provide the name and contact information.
   d. Information demonstrating the Contractor's financial stability to include:
      1) Full name, address, and telephone number of the organization;
      2) Date the firm was established;
      3) Ownership (e.g. public company, partnership, subsidiary, etc.);
      4) If incorporated, provide the state of incorporation;
      5) Number of full-time employees on January 1st for the last three (3) years or for the duration the firm has been in business, whichever is less.
   e. Provide a list of institutions of higher education with which the firm has a signed term contract.
   f. Provide the amount of annual sales the firm has with each VASCUPP Member Institution. A list of VASCUPP Members can be found at: [http://www.vcu.edu/procurement/coopcon.htm](http://www.vcu.edu/procurement/coopcon.htm).

5. Small, Women-Owned and Minority-Owned Business Commitment:

   Firm must complete and submit Appendix I unless the firm is a Department of Small business and Supplier Diversity (DSBSD) certified small business. DSBSD certified small businesses must include their certification number on the coversheet of this RFP, but are not required to complete Appendix I.

6. Invoicing and Payment:

Firm must complete and submit Appendix II.

## VIII. **PRICING SCHEDULE:**

A. Offerors shall provide all costs associated with license price, set-up, implementation, hosting, training and maintenance to include all items described in Section VI. STATEMENT OF NEEDS for the proposed application vulnerability scanner solution. Offerors shall provide additional costs associated with the STATEMENT OF NEEDS, as appropriate. Offerors shall complete and submit the Pricing Schedule below:

B. Description Price

1. Total license price for the first year $ ____________________

   a. individual license unit price, if applicable

      $ ____________________

   b. discount for the license(s) price

      ____________________%

2. Total hardware or appliance price for the first year $ ____________________

   a. individual hardware or appliance price

      $ ____________________

   b. discount for hardware or appliance price

      ____________________%

3. Fixed price for implementation $____________________

   a. List the job titles and hourly rates that total to the fixed price for implementation

4. Hosting price for the first year $ ____________________

5. Maintenance and support or upgrade for the first year $ ____________________

6. Hiring and training price for the first year $ ____________________

7. Optional On-Site Training $ ____________________

8. Total price for Section VIII.B. $ ____________________

## IX. EVALUATION AND AWARD CRITERIA:

Proposals will be evaluated based upon the information provided in the Offeror's Proposal using the following criteria: Offeror's qualifications and experience (10 points); methodology/approach to providing the requirements stated herein (55 points); pricing (25 points); and the Offeror's status as a Virginia certified SWaM Business or the Offeror's plans to utilize Virginia DSBSD-certified SWaM Businesses in the Offeror's performance of the contract (10 points). Negotiations shall be conducted with Offerors so selected. After negotiations have been conducted with each Offeror so selected, the VCU shall select the Offeror which, in its opinion, has made the best offer, and shall award the contract to that Offeror. VCU reserves the right to make multiple awards from the solicitation. The University may cancel this Request for Proposals or reject Proposals at any time prior to an award, and is not required to furnish a statement of the reason why a particular Proposal was not deemed to be the most advantageous (Governing Rules Section 49.D). Should the University determine in writing and in its sole discretion that only one Offeror has made the best proposal, a Contract may be negotiated and awarded to that Offeror. The award document will be a Contract incorporating by reference all the requirements, terms and conditions of the RFP, and the Offeror's response thereto. VCU reserves the right to award to multiple offerors, should such an award benefit the University.

Notice of Award(s) or Notice of Intent to Award may be accessed electronically at http://www.eva.virginia.gov.

## X. REPORTING AND DELIVERY REQUIREMENTS:

**By submitting a Proposal, Offerors certify that all information provided in response to the Request for Proposals is true and accurate. Failure to provide information required by this Request for Proposals will ultimately result in rejection of the Proposal.**

It is the policy of the Commonwealth of Virginia that 42% of its purchases be made from small businesses to contribute to the establishment, preservation, and strengthening of small businesses, and businesses owned by women and minorities, and to encourage their participation in VCU procurement activities. The Commonwealth encourages Contractors to provide for the participation of small businesses and businesses owned by women and minorities through partnerships, joint ventures, subcontracts or other contractual opportunities.

**Use of Subcontractors**: If the Offeror intends to use subcontractors to perform any portion of the work described in this RFP, the Offeror must clearly so state. VCU is placing an increased emphasis on its SWaM (Small, Women, and Minority Owned) business program and is interested in identifying any potential opportunities that may be available to engage SWaM vendors to be certified by the Virginia Department of Small Business and Supplier Diversity (DSBSD) through new or existing contracts. **Identify and list any such opportunities that your firm would commit to if awarded this Contract in Appendix 1- Participation in VCU Procurement Transactions Small Businesses and Businesses Owned by Women and Minority**. The Offeror's response must include a description of which portion(s) of the work will be sub-contracted out and the names and addresses of potential Subcontractor(s) under the Contract.

### REPORT ON THE PARTICIPATION OF SMALL BUSINESSES AND BUSINESSES OWNED BY WOMEN AND MINORITIES

Unless the Contractor is a DSBSD certified small business, the Contractor shall submit quarterly reports on the direct involvement of Department of Small Business and Supplier Diversity (DSBSD) certified

SWaM Businesses in the performance of the Contract. The report shall specify the actual dollars spent to date with Small Businesses, Women-Owned Businesses, and Minority-Owned Businesses based upon the Contractor's commitment for utilization of DSBSD SWaM Businesses.

The Contractor shall provide this information to:

Virginia Commonwealth University
Procurement Services Office
Attn: SWaM Coordinator
912 W. Grace Street, POB 980327
Richmond, VA 23284
Email: swamreporting@vcu.edu

Failure to submit the required information will be considered a contract compliance issue and will be addressed accordingly. In addition, failure to submit the required information will result in invoices being returned without payment.

## XI. GENERAL TERMS AND CONDITIONS:

A. PURCHASING MANUAL: This RFP is subject to the provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and their Vendors and any revisions thereto, which are hereby incorporated into this contract in their entirety. A copy of the manual is available for review at the VCU Procurement Services Office. In addition, the manual may be accessed electronically at http://procurement.vcu.edu/ or a copy can be obtained by calling VCU Procurement Services at (804) 828-1077.

B. APPLICABLE LAW AND COURTS: This RFP and any resulting Contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The Contractor shall comply with all applicable federal, state and local laws, rules and regulations.

C. ANTI-DISCRIMINATION: By submitting their Proposals, Offerors certify to the Commonwealth and to VCU that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and Section 2.2-4311 of the *Virginia Public Procurement Act.* If the award is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. (*Code of Virginia*, § 2.2-4343.1).

In every Contract over $10,000 the provisions in 1. and 2. below apply:

1. During the performance of this Contract, the Contractor agrees as follows:

a) Virginia Commonwealth University is an equal opportunity/affirmative action institution providing access to education and employment without regard to age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability. As such, the Contractor will not discriminate against any employee or applicant for employment because of age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability or any other basis prohibited by state law related to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the Contractor. The Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

b) The Contractor, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, will state that such Contractor is an equal opportunity employer.

c) Notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting these requirements.

2. The Contractor will include the provisions of 1. above in every subcontract or purchase order over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

D. <u>ETHICS IN PUBLIC CONTRACTING</u>: By submitting their Proposals, Offerors certify that their Proposals are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other Offeror, supplier, manufacturer or subcontractor in connection with their Proposal, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

E. <u>IMMIGRATION REFORM AND CONTROL ACT OF 1986</u>: By submitting their Proposals, Offerors certify that they do not and will not during the performance of this Contract employ illegal alien workers or otherwise violate the provisions of the Federal Immigration Reform and Control Act of 1986.

F. <u>DEBARMENT STATUS:</u> By submitting their Proposals, Offerors certify that they are not currently debarred by the Commonwealth of Virginia from submitting proposals on contracts for the type of goods and/or services covered by this solicitation, nor are they an agent of any person or entity that is currently so debarred.

G. <u>ANTITRUST:</u> By entering into a Contract, the Contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of the action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.

H. <u>MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS</u>: Failure to submit a Proposal on the official VCU Form provided for that purpose may be a cause for rejection of the Proposal. Modification of, or additions to, the General Terms and Conditions of the solicitation may be cause for rejection of the Proposal; however, the Commonwealth reserves the right to decide, on a case by case basis, in its sole discretion, whether to reject such a Proposal.

I. <u>PAYMENT</u>:

1. To Prime Contractor:

   a) Invoices for items ordered, delivered and accepted shall be submitted by the Contractor directly to the payment address shown on the purchase order/Contract. All invoices shall show the VCU Contract number and/or purchase order number; social security number (for individual Contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).

   b) Any payment terms requiring payment in less than thirty (30) days will be regarded as requiring payment thirty (30) days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than thirty (30) days, however.

   c) All goods or services provided under this Contract or purchase order, that are to be paid for with public funds, shall be billed by the Contractor at the contract price, regardless of which public institution is being billed.

   d) The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.

   e) Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, VCU shall promptly notify the contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A Contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this Section do not relieve VCU of its prompt payment obligations with respect to those charges that are not in dispute (Code of Virginia, § 2.2-4363).

2. To Subcontractors:

   a) Contractor awarded a contract under this RFP is hereby obligated:

      i. To pay the Subcontractor(s) within seven (7) days of the Contractor's receipt of payment from VCU for the proportionate share of the payment received for work performed by the Subcontractor(s) under the contract; or

      ii. To notify VCU and the Subcontractor(s), in writing, of the Contractor's intention to withhold payment and the reason.

   b) The Contractor is obligated to pay the Subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the Contractor that remain unpaid seven (7) days following receipt of payment from VCU, except for amounts withheld as stated in 2. above. The date of mailing of any payment by U.S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier Contractor performing under the primary contract. A Contractor's obligation to pay an interest charge to a Subcontractor may not be construed to be an obligation of VCU.

J. <u>PRECEDENCE OF TERMS</u>: Paragraphs A-J of these General Terms and Conditions shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.

K. QUALIFICATIONS OF OFFERORS: VCU may make such reasonable investigations as deemed proper and necessary to determine the ability of the Offeror to perform the services/furnish the goods and the Offeror shall furnish to VCU all such information and data for this purpose as may be requested. VCU reserves the right to inspect Offeror's physical facilities prior to award to satisfy questions regarding the Offeror's capabilities. VCU further reserves the right to reject any Proposal if the evidence submitted by, or investigations of, such Offeror fails to satisfy VCU that such Offeror is properly qualified to carry out the obligations of the Contract and to provide the services and/or furnish the goods contemplated therein.

L. TESTING AND INSPECTION: VCU reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.

M. ASSIGNMENT OF CONTRACT: A Contract shall not be assignable by the Contractor in whole or in part without the written consent of the VCU Director of Procurement Services.

N. CHANGES TO THE CONTRACT: Changes can be made to the Contract in any one of the following ways:

1. The parties may agree in writing to modify the scope of the Contract. An increase or decrease in the price of the Contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the Contract.

2. The VCU Procurement Services Department may order changes within the general scope of the Contract at any time by written notice to the Contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The Contractor shall comply with the notice upon receipt. The Contractor shall be compensated for any additional costs incurred as the result of such order and shall give VCU a credit for any savings. Said compensation shall be determined by one of the following methods:

a) By mutual agreement between the parties in writing; or

b) By agreeing upon a unit price or using a unit price set forth in the Contract, if the work to be done can be expressed in units, and the Contractor accounts for the number of units of work performed, subject to the VCU's right to audit the Contractor's records and/or to determine the correct number of units independently; or

c) By ordering the Contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the Contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The Contractor shall present VCU with all vouchers and records of expenses incurred and savings realized. VCU shall have the right to audit the records of the Contractor as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to VCU within thirty (30) days from the date of receipt of the written order from VCU. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the Contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this Contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and Their Vendors. Neither the existence of a claim or a dispute resolution process, litigation or any other provision of this Contract shall excuse the Contractor from promptly complying with the changes ordered by the VCU Procurement Service Office or with the performance of the Contract generally.

O. DEFAULT: In case of failure to deliver goods or services in accordance with the Contract terms and conditions, VCU after due oral or written notice, may procure them from other sources and hold the Contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies which VCU may have in law or equity.

P. USE OF BRAND NAMES: Unless otherwise provided in this RFP, the name of a certain brand, make or manufacturer does not restrict Offerors to the specific brand, make or manufacturer named, but conveys the general style, type, character, and quality of the article desired. Any article, which the public body, in its sole discretion, determines to be the equal of that specified, considering quality, workmanship, economy of operation, and suitability for the purpose intended, shall be accepted. The Offeror is responsible to clearly and specifically identify the product being offered and to provide sufficient descriptive literature, catalog cuts and technical detail to enable VCU to determine if the product offered meets the requirements of the solicitation. This is required even if offering the exact brand, make or manufacturer specified. Unless the Offeror clearly indicates in its proposal that the product offered is an "equal" product, such proposal will be considered to offer the brand name product referenced in the RFP.

Q. TRANSPORTATION AND PACKAGING: By submitting their Proposals, all Offerors certify and warrant that the price offered for FOB Destination includes only the actual freight rate costs at the lowest and best rate and is based upon the actual weight of the goods to be shipped. Except as otherwise specified herein, standard commercial packaging, packing and shipping containers shall be used. All shipping containers shall be legibly marked or labeled on the outside with purchase order number, commodity description, and quantity. Further, Offeror shall bear the risk of loss until the goods and equipment until VCU accepts Delivery of them.

R. INSURANCE: By signing and submitting a Proposal under this RFP, the Offeror certifies that if awarded the Contract, it will have the following insurance coverages at the time the Contract is awarded. For construction contracts, if any Subcontractors are involved, the subcontractor will have workers' compensation insurance in accordance with §§ 2.2-4332 and 65.2-800 et seq. of the *Code of Virginia*. The Offeror further certifies that the Contractor and any Subcontractors will maintain these insurance coverages during the entire term of the Contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

Minimum Insurance Coverages and Limits Required for Most Contracts:

1. Worker's Compensation - Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify VCU of increases in the number of employees that change their workers' compensation requirements under the *Code of Virginia* during the course of the Contract shall be in noncompliance with the Contract.

2. Employers Liability - $100,000.

3. Commercial General Liability - $1,000,000 per occurrence. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products

and completed operations coverage. VCU must be named as an additional insured and so endorsed on the policy.

4. Automobile Liability - $1,000,000 per occurrence. (Only used if motor vehicle is to be used in the contract.)

S. ANNOUNCEMENT OF AWARD: Upon the award or the announcement of the decision to award a contract as a result of this RFP, VCU will publicly post such notice electronically at http://www.eva.virginia.gov for a minimum of ten (10) days.

T. DRUG-FREE WORKPLACE: During the performance of this Contract, the Contractor agrees to (i) provide a drug-free workplace for the Contractor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the contractor's workplace and specifying the actions that will be taken against employees for violation of such prohibition: (iii) state in all solicitations or advertisements for employees placed by or on behalf of the Contractor that the Contractor maintains a drug-free workplace: and (iv) include the provisions of the foregoing clauses in every Subcontract or purchase order of over $10,000, so that the provisions will be binding upon each Subcontractor and/ or Vendor.

For the purposes of this section, *"drug-free workplace*" means a site for the performance of work done in connection with a specific Contract awarded to a Contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the Contract.

U. NONDISCRIMINATION OF CONTRACTORS: A Bidder, Offeror, or Contractor shall not be discriminated against in the solicitation or award of this Contract because of race, religion, color, sex, national origin, age, disability, or against faith-based organizations or any other basis prohibited by state law relating to discrimination in employment. If the award of this Contract is made to a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this Contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

V. eVA BUSINESS-TO-GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS: The eVA Internet electronic procurement solution, website portal www.eVA.virginia.gov, streamlines and automates government purchasing activities in VCU. The eVA portal is the gateway for vendors to conduct business with VCU Institution and other public bodies. All Vendors desiring to provide goods and/or services to VCU shall participate in the eVA Internet e-procurement solution by completing the free eVA Vendor Registration. All Bidders or Offerors must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the bid/proposal being rejected.

Vendor Transaction Fees are determined by the date the original purchase order is issued and are as follows:

1. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:

   a) DSBSD-certified Small Businesses: 1%, capped at $500 per order.

b) Businesses that are not DSBSD-certified Small Businesses: 1%, capped at $1,500 per order.

2. For orders issued July 1, 2014 the vendor transaction fees can be found at www.eVA.virginia.gov

The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Department of General Services, approximately thirty (30) days after the corresponding purchase order is issued and payable thirty (30) days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

W. FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA). The Selected Offeror/Vendor acknowledges that for the purposes of this Contract it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this Contract for University's and its students' benefit, and will not share such data with or disclose it to any third party except as provided for in this Contract, required by law, or authorized in writing by the University.

## XII. SPECIAL TERMS AND CONDITIONS:

A. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this proposal, no indication of such sales or services to Virginia Commonwealth University will be used in product literature or advertising. The Contractor shall not state in any of the advertising or product literature that the Commonwealth of Virginia or any agency or institution of the Commonwealth has purchased or uses its products or services.

B. AUDIT: The Contractor shall retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The agency, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.

C. AVAILABILITY OF FUNDS: It is understood and agreed between the parties herein that the agency shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

D. PROPOSAL ACCEPTANCE PERIOD: Any proposal in response to this solicitation shall be valid for sixty (60) days. At the end of the sixty (60) days, the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.

E. PROPOSAL PRICES: Proposal prices shall be in the form of a firm unit price for each item during the contract period.

F. CANCELLATION OF CONTRACT: The purchasing agency reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon sixty (60) days written notice to the Contractor. In the event the initial contract period is for more than twelve (12) months, the resulting contract may be terminated by either party, without penalty, after the initial twelve (12) months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

G. SPECIAL EDUCATIONAL OR PROMOTIONAL DISCOUNTS: The Contractor shall extend any special educational or promotional sale prices or discounts immediately to the Commonwealth during the term of the contract. Such notice shall also advise the duration of the specific sale or discount price.

H. DRUG FREE WORKPLACE: The Contractor acknowledges and certifies that it understands that the following acts by the Contractor, its employees and/or agents performing services on state property are prohibited:

1. The unlawful manufacture, distribution, dispensing, possession or use of alcohol or other drugs; and
2. Any impairment or incapacitation from the use of alcohol or other drugs (except the use of drugs for legitimate medical purposes).
3. The Contractor further acknowledges and certifies that it understands that a violation of these prohibitions constitutes a breach of contract and may result in default action being taken by the Commonwealth in addition to any criminal penalties that may result from such conduct.

I. EXTRA CHARGES NOT ALLOWED: The proposal price shall be for complete installation ready for Commonwealth's use, and shall include all applicable freight and installation charges; extra charges will not be allowed.

J. FINAL INSPECTION: At the conclusion of the work, the Contractor shall demonstrate to the authorized owners representative that the work is fully operational and in compliance with contract specifications and codes. Any deficiencies shall be promptly and permanently corrected by the Contractor at the Contractor's sole expense prior to final acceptance of the work.

K. IDENTIFICATION OF PROPOSAL: The proposal package should be identified as follows:

From: ______________________________ ______________ ______________
Name of Offeror Due Date Time

______________________________ ________________________________________
Street or Box Number RFP No.

______________________________ ________________________________________
City, State, Zip Code +4 RFP Title

Name of Contract / Purchase Officer or Buyer: Jackie Colbert

The package should be addressed as directed on Page 2 of the solicitation.

If a proposal is not clearly identified, the Offeror takes the risk that the proposal may be inadvertently opened and the information compromised which may cause the proposal to be disqualified. Proposals may be hand delivered to the designated location in the office issuing the solicitation. No other correspondence or other proposals should be placed in the envelope.

LATE PROPOSALS: To be considered for selection, proposals must be received by the issuing office by the designated date and hour. The official time used in the receipt of proposals is that time on the automatic time stamp machine in the issuing office. Proposals received in the issuing office after the date and hour designated are automatically disqualified and will not be considered. The University is not responsible for delays in the delivery of mail by the U.S. Postal Service, private couriers, or the intrauniversity mail system. It is the sole responsibility of the Offeror to insure that its proposal reaches the issuing office by the designated date and hour.

L. INDEMNIFICATION: Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the Contractor/any services of any kind or nature furnished by the Contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use the materials, goods, or equipment in the manner already and permanently described by the Contractor on the materials, goods, or equipment delivered.

M. LIMITATION OF LIABILITY: To the maximum extent permitted by applicable law, the Contractor will not be liable under this contract for any indirect, incidental, special or consequential damages, or damages from loss profits, revenue, data or use of the supplies, equipment and/or services delivered under this contract. This limitation of liability will not apply, however, to liability arising from: (a) personal injury or death; (b) defect or deficiency caused by willful misconduct or negligence on the part of the Contractor; or (c) circumstances where the contract expressly provides a right to damages, indemnification or reimbursement.

N. PRIME CONTRACTOR RESPONSIBILITIES: The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

O. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for four (4) successive one (1) year periods under the terms and conditions of the original contract except as stated in 1. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew should be provided approximately 60 days prior to the expiration date of each contract period:

1. If the Commonwealth elects to exercise the option to renew the contract for an additional one (1) - year period, the contract price(s) for the additional one (1) year shall not exceed the contract price(s) of the previous contract period increased/decreased by more than the percentage increase/decrease of the All Items category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

P. SUBCONTRACTS: No portion of the work shall be subcontracted without prior written consent of the purchasing agency. In the event that the Contractor desires to subcontract some part of the work specified herein, the Contractor shall furnish the purchasing agency the names, qualifications and experience of their proposed subcontractors. The Contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract.

Q. WARRANTY (COMMERCIAL): The Contractor agrees that the supplies or services furnished under any award resulting from this solicitation shall be covered by the most favorable commercial warranties the Contractor gives any customer for such supplies or services and that the rights and remedies provided therein are in addition to and do not limit those available to the Commonwealth by any other clause of this solicitation. A copy of this warranty should be furnished with the proposal.

R. POLICY OF EQUAL EMPLOYMENT: Virginia Commonwealth University is an equal opportunity/affirmative action employer. Women, Minorities, persons with disabilities are encouraged to apply. The University encourages all vendors to establish and maintain a policy to insure equal opportunity employment. To that end, Offerors should submit along with their proposals, their policy of equal employment.

S. eVA BUSINESS-TO-GOVERNMENT CONTRACTS AND ORDERS: The solicitation/contract will result in purchase order(s) with the eVA transaction fee specified below assessed for each order.

1. For orders issued July 1, 2011 thru June 30, 2013, the Vendor Transaction Fee is:

a) DSBSD-certified Small Businesses: 0.75%, Capped at $500 per order.

b) Businesses that are not DSBSD-certified Small Businesses: 0.75%, Capped at $1,500 per order.

2. For orders issued July 1, 2013, and after, the Vendor Transaction Fee is:

a) DSBSD-certified Small Businesses: 1%, Capped at $500 per order.

b) Businesses that are not DSBSD-certified Small Businesses: 1%, Capped at $1,500 per order.

The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Department of General Services, approximately 30 days after the corresponding purchase order is issued and payable 30 days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

The eVA Internet electronic procurement solution, website portal www.eva.virginia.gov, streamlines and automates government purchasing activities in the Commonwealth. The portal is the gateway for vendors to conduct business with state agencies and public bodies.

Vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet e-procurement solution and agree to comply with the following: If this solicitation is for a term contract, may provide an electronic catalog (price list) or index page catalog for items awarded. The format of this electronic catalog shall conform to the eVA Catalog Interchange Format (CIF) Specification that can be accessed and downloaded from www.eVA.virginia.gov. Contractors should email Catalog or Index Page information to eVA-catalog-manager@dgs.virginia.gov.

T. GRAMM-LEACH-BLILEY ACT: The Contractor shall comply with the Act by implementing and maintaining appropriate safeguards to protect and prevent unauthorized release of student, faculty and staff nonpublic information. Nonpublic information is defined as social security numbers, or financial transactions, bank, credit and tax information.

U. DETERMINATION OF RESPONSIBILITY: The Contract will be awarded to the responsive and responsible Offeror with a Proposal, conforming to the RFP, will be most advantageous to VCU, technical and financial factors considered. A responsible Offeror is one who affirmatively demonstrates to VCU that it has adequate financial resources and the requisite capacity, capability, and facilities to perform the Contract, has a satisfactory record of performance on other comparable projects, has a satisfactory record of integrity and business ethics, and is otherwise qualified and eligible to receive award under the solicitation and laws and regulations applicable to the procurement. VCU reserves the right to investigate the capabilities of Offeror, confirm any part of the information furnished by an Offeror, and require other evidence to determine that the Offeror is responsible.

V. REJECTION OF PROPOSALS & WAIVER OF MINOR INFORMALITIES/IRREGULARITIES: VCU reserves the right to reject any or all Proposals in part or in total for any reason, to accept any Proposal if considered best for its interest, and to waive informalities and minor irregularities in Proposals received, commensurate with best public procurement practices.

W. PROTEST: Any Offeror who desires to protest the award or decision to award a Contract shall submit the protest in writing to:

Director of Procurement Services
Virginia Commonwealth University
912 West Grace, 5th Floor
Richmond, VA 23284

VCU will announce the award utilizing the Commonwealth of Virginia's e-Procurement system (eVA). The protest must be received no later than ten (10) days after the award or the announcement of the decision to award, whichever occurs first. However, if the protest of any actual or potential Offeror depends in whole or in part upon information contained in public records pertaining to the procurement transaction that are subject to inspection under the Rules Governing Procurement of Goods, Services, Insurance, and Construction by a Public Institution of Higher Education of the Commonwealth of Virginia Governed by Subchapter 3 of the Restricted Higher Education Financial and Administrative Operations Act,, Chapter 4.10 (§23-38.88 et seq) of Title 23 of the Code of Virginia, §34, then the time within which the protest shall be submitted shall expire ten (10) days after those records are available for inspection by such Offeror under §34, or at such later time as provided in this section.

VCU Notices of Award(s) or Notices of Intent to Award may be accessed electronically at http://www.eva.virginia.gov.

No protest shall lie for a claim that the selected Offeror is not a responsible Offeror.

The written protest shall include the basis for the protest and relief sought.

The VCU Director of Procurement Services shall issue a decision in writing within ten (10) days of receipt stating the reasons for the action taken. This decision shall be final unless the Offeror appeals within ten (10) days of receipt of the written decision by instituting legal action as provided in Section 54 of the Governing Rules.

Nothing in this paragraph shall be construed to permit a proposer to challenge the validity of the terms or conditions of the RFP.

"Days" as used in this paragraph refer to calendar days. If a deadline falls on a Saturday or Sunday, the next business day shall be considered to be the deadline.

## XIII. **SPECIAL TERMS AND CONDITIONS INFORMATION TECHNOLOGY:**

A. QUALIFIED REPAIR PERSONNEL: All warranty or maintenance services to be performed on the items specified in this solicitation as well as any associated hardware or software shall be performed by qualified technicians properly authorized by the manufacturer to perform such services. The Commonwealth reserves the right to require proof of certification prior to award and at any time during the term of the contract.

B. SOURCE CODE: In the event the contractor ceases to maintain experienced staff and the resources needed to provide required software maintenance, the Commonwealth shall be entitled to have use, and duplicate for its own use, a copy of the source code and associated documentation for the software products covered by the contract. Until such time as a complete copy of such material is provided, the Commonwealth shall have exclusive right to possess all physical embodiments of such contractor owned materials. The rights of the Commonwealth in this respect shall survive for a period of twenty years after the expiration or termination of the contract. All lease and royalty fees necessary to support this right are included in the initial license fee as contained in the pricing schedule.

C. SOFTWARE UPGRADES: The Commonwealth shall be entitled to any and all upgraded versions of the software covered in the contract that becomes available from the contractor. The maximum charge for upgrade shall not exceed the total difference between the cost of the Commonwealth's current version and the price the contractor sells or licenses the upgraded software under similar circumstances.

D. THIRD PARTY ACQUISITION OF SOFTWARE: The contractor shall notify the procuring agency in writing should the intellectual property, associated business, or all of its assets be acquired by a third party. The contractor further agrees that the contract's terms and conditions, including any and all license rights and related services, shall not be affected by the acquisition. Prior to completion of the acquisition, the contractor shall obtain, for the Commonwealth's benefit and deliver thereto, the assignee's agreement to fully honor the terms of the contract.

E. TITLE OF SOFTWARE: By submitting a proposal, the offeror represents and warrants that it is the sole owner of the software or, it not the owner, that it has received all legally required authorizations from the owner to license the software, has the full power to grant the rights required by this solicitation, and that neither the software nor its use in accordance with the contract will violate or infringe upon any patent, copyright, trade secret, or any other property rights of another person or organization.

F. WARRANTY AGAINST SHUTDOWN DEVICES: The contractor warrants that the equipment and software provided under the contract shall not contain any lock, counter, CPU references, virus, worm, or other device capable of halting operations or erasing or altering data or programs. Contractor further warrants that neither it, nor its agents, employees, or subcontractors shall insert any shutdown device following delivery of the equipment and software.

G. SECTION 508 COMPLIANCE: All information technology which, pursuant to this Contract, is purchased or upgraded by or for the use of any Commonwealth agency or institution or political subdivision of the Commonwealth (the “Technology”) shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. If requested, the Contractor must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. The requirements of this Paragraph along with the Non-Visual Access to Technology Clause shall be construed to achieve full compliance with the Information Technology Access Act, §§ 2.2-3500 through 2.2-3504 of the *Code of Virginia*.

H. NONVISUAL ACCESS TO TECHNOLOGY: All information technology which, pursuant to this Agreement, is purchased or upgraded by or for the use of any State agency or institution or political subdivision of the Commonwealth (the “Technology”) shall comply with the following nonvisual access standards from the date of purchase or upgrade until the expiration of this Agreement:

1. effective, interactive control and use of the Technology shall be readily achievable by nonvisual means;
2. the Technology equipped for nonvisual access shall be compatible with information technology used by other individuals with whom any blind or visually impaired user of the Technology interacts;
3. nonvisual access technology shall be integrated into any networks used to share communications among employees, program participants or the public; and
4. the technology for nonvisual access shall have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

Compliance with the foregoing nonvisual access standards shall not be required if the head of the using agency, institution or political subdivision determines that (i) the Technology is not available with nonvisual access because the essential elements of the Technology are visual and (ii) nonvisual equivalence is not available.

Installation of hardware, software, or peripheral devices used for nonvisual access is not required when the Technology is being used exclusively by individuals who are not blind or visually impaired, but applications programs and underlying operating systems (including the format of the data) used for the manipulation and presentation of information shall permit the installation and effective use of nonvisual access software and peripheral devices.

If requested, the Contractor must provide a detailed explanation of how compliance with the foregoing nonvisual access standards is achieved and a validation of concept demonstration.

The requirements of this Paragraph shall be construed to achieve full compliance with the Information Technology Access Act, §§ 2.1-807 through 2.1-811 of the Code of Virginia.

I. DATA AND INTELLECTUAL PROPERTY PROTECTION:

1. Definitions

a. "End User" means the individuals authorized by the University to access and use the Services provided by the Selected Firm/Vendor under this agreement.

b. "Personally Identifiable Information" includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "personal information" as defined in Virginia Code section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; "medical information" as defined in Virginia Code Section 32.1-127.1:05; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.

c. "Securely Destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.

d. "Security Breach" means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store or dispose of data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.

e. "Services" means any goods or services acquired by the University from the Selected Firm/Vendor.

f. "University Data" includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student and personnel data.

2. Rights and License in and to the University Data

The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Selected Firm/Vendor has a limited, nonexclusive license to use these data as provided in this agreement solely for the purpose of performing its obligations hereunder. This agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the agreement.

3. Intellectual Property Disclosure/Rights

a. Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by Selected Firm/Vendor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.

b. Selected Firm/Vendor warrants to the University that the University will own all rights, title and interest in any intellectual property created for the University as part of the performance of this agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Selected Firm/Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all intellectual property created for the University as part of the performance of this agreement to the University, and will execute any future assignments or other documents needed for the University to document, register, or otherwise perfect such rights. Nothing in this section is, however, intended to or shall be construed to apply to existing intellectual property created or owned by the vendor that the University is licensing under this agreement. For avoidance of doubt, the University asserts no intellectual property ownership under this clause to any pre-existing intellectual property of the vendor, and seeks ownership rights only to the extent Vendor is being engaged to develop certain intellectual property as part of its services for the University.

c. Notwithstanding the foregoing, for research collaboration pursuant to subcontracts under sponsored research agreements administered by the University's Office of Sponsored Programs, intellectual property rights will be governed by the terms of the grant or contract to the University to the extent such grant or contract requires intellectual property terms to apply to subcontractors.

4. Data Privacy

a. Selected Firm/Vendor will use University Data only for the purpose of fulfilling its duties under this agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by this agreement or as otherwise required by law.

b. University Data will not be stored outside the United States without prior written consent from the University.

c. Selected Firm/Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill Selected Firm/Vendor obligations under this agreement. Selected Firm/Vendor will ensure that employees who perform work under this agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this agreement.

d. The following provision applies only if Selected Firm/Vendor will have access to the University’s education records as defined under the Family Educational Rights and Privacy Act (FERPA): The Selected Firm/Vendor acknowledges that for the purposes of this agreement it will be designated as a “school official” with “legitimate educational interests” in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this agreement for University’s and its End User’s benefit, and will not share such data with or disclose it to any third party except as provided for in this agreement, required by law, or authorized in writing by the University.

5. Data Security

a. Selected Firm/Vendor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Selected Firm/Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Selected Firm/Vendor warrants that all electronic University Data will be encrypted in transmission (including via web interface) in accordance with industry best practices commensurate to the sensitivity of the information; such as controls outlined in the Moderate or High control baselines in the latest version of National Institute of Standards and Technology Special Publication 800-53.

b. If the Selected Firm/Vendor stores Personally Identifiable Information as part of this agreement, the Selected Firm/Vendor warrants that the information will be stored in accordance with industry best practices commensurate to the sensitivity of the information; such as controls outlined in the Moderate or High control baselines in the latest version of National Institute of Standards and Technology Special Publication 800-53.

c. Selected Firm/Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this agreement.

6. Employee Background Checks and Qualifications

Selected Firm/Vendor shall ensure that its employees who will have potential access to University Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of this agreement.

7. Data Authenticity and Integrity

Selected Firm/Vendor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. The Selected Firm will be responsible during the terms of this agreement, unless otherwise specified elsewhere in this agreement, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

8. Security Breach

a. Response. Upon becoming aware of a Security Breach, or of circumstances that are reasonably understood to suggest a likely Security Breach, Selected Firm/Vendor will timely notify the University consistent with applicable state or federal laws, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Selected Firm/Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.

b. Liability.

1) If Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor, including but not limited to providing notification to individuals whose

Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.

2) If Selected Firm/Vendor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor.

9. Response to Legal Orders, Demands or Requests for Data

a. Except as otherwise expressly prohibited by law, Selected Firm/Vendor will:

- immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Selected Firm/Vendor seeking University Data;
- consult with the University regarding its response;
- cooperate with the University's reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
- upon the University's request, provide the University with a copy of its response.

b. If the University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act) or request seeking University Data maintained by Selected Firm/Vendor, the University will promptly provide a copy to Selected Firm/Vendor. Selected Firm/Vendor will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response.

10. Data Transfer Upon Termination or Expiration

a. Upon termination or expiration of this agreement, Selected Firm/Vendor will ensure that all University Data are securely returned or destroyed as directed by the University in its sole discretion. Transfer to the University or a third party designated by the University shall occur within a reasonable period of time, and without significant interruption in service. Selected Firm/Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition. In the event that the University requests destruction of its data, Selected Firm/Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Selected Firm/Vendor might have transferred University data. The Selected Firm/Vendor agrees to provide documentation of data destruction to the University.

b. Selected Firm/Vendor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Selected Firm/Vendor's facilities to remove and destroy University-owned assets and data. Selected Firm/Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Selected Firm/Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating ` which if any of these are owned by or dedicated to the University. Selected Firm/Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

11. Audits

a. The University reserves the right in its sole discretion to perform audits of Selected Firm/Vendor at the University's expense to ensure compliance with the terms of this agreement. The Selected Firm/Vendor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which the Selected Firm/Vendor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If the Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data which has been identified to the Selected Firm/Vendor as having the potential to affect the accuracy of the University's financial statements, Selected Firm/Vendor will at its expense conduct or have conducted at least annually a:

- American Institute of CPAs Service Organization Controls (SOC 2) Type II audit, or other security audit with audit objectives deemed sufficient by the University, which attests the Selected Firm/Vendor's security policies, procedures and controls;
- vulnerability scan of Selected Firm/Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement; and
- formal penetration test of Selected Firm/Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement.

Additionally, the Selected Firm/Vendor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this agreement. The University may require, at University expense, the Selected Firm/Vendor to perform additional audits and tests, the results of which will be provided promptly to the University.

12. Compliance

a. Selected Firm/Vendor will comply with all applicable laws and industry standards in performing services under this agreement. Any Selected Firm/Vendor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Selected Firm/Vendor upon request.

b. Selected Firm/Vendor warrants that the service it will provide to the University is fully compliant with relevant laws, regulations, and guidance that may be applicable to the service, such as: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.

c. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to the Selected Firm/Vendor service provided to the University, the Selected Firm/Vendor will, upon written request, furnish proof of compliance with PCI-DSS within 10 business days of the request.

13. No End User agreements

This agreement is the entire agreement between the University (including University employees and other End Users) and the Selected Firm/Vendor. In the event that the Selected Firm/Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with University employees or other End Users, such agreements shall be null, void and without effect, and the terms of this agreement shall apply.

14. Survival

The Selected Firm/Vendor's obligations under Section XIII, Item I (DATA AND INTELLECTUAL PROPERTY PROTECTION) shall survive termination of this agreement until all University Data has been returned or securely destroyed.

## XIV. **CONTRACT ADMINISTRATION:**

Upon award of the contract VCU shall designate, in writing, the name(s) of the Contract Administrator(s) who shall work with the contractor in formulating mutually acceptable plans and standards for the delivery, installation and on-going service and/or maintenance that may be required.

A. The Contract Administrator shall use all powers under the contract to enforce its faithful performance. The Contract Administrator shall determine the amount, quality and acceptability of work and shall decide all other questions in connection with the work.

B. All direction and orders from VCU shall be transmitted through the Contract Administrator, or his designee. However the Contract Administrator shall have no authority to order changes in the work which alter the concept or scope of the work or change the basis for compensation to the contractor.

## XV. **ATTACHMENTS:**

A: Appendix I – Participation In State Procurement Transactions Small Businesses and Businesses Owned By Women and Minorities:

http://procurement.vcu.edu/media/procurement/pdf/document-library/RFP_Website_Link_Appendix_1.pdf

B: Appendix II – Invoicing and Payment

http://procurement.vcu.edu/media/procurement/pdf/document-library/RFP_Website_Link_Appendix_2.pdf

# WhiteHat Security

## WhiteHat Negotiation Questions for RFP #7286528JC
## Application Vulnerability Scanner
## Prepared for VCU
## May 8, 2017

Christopher Perkins
Regional Sales Director
571.481.0895
chris.perkins@whitehatsec.com

## WHITEHAT NEGOTIATION QUESTIONS FOR RFP #7286528JC - APPLICATION VULNERABILITY SCANNER

**You will find as part of the enclosed, both the answers to the questions you posed in connection with our most recent onsite during the Negotiation Phase of your RFP but, also, information around other questions VCU has asked in previous meetings (supporting documentation included).**

1. Please clarify the WhiteHat response to Section VI.F. Procurement Requirements. The Requirements are restated in the response to this section in the WhiteHat proposal. Does your company agree with the Procurement Requirements in Section VI.F.?

   VI.F.1 Yes __XX___ No ______
   VI.F.2 Yes _____ No __XX____
   VI.F.3 Yes __XX___ No ______
   VI.F.4 Yes __XX___ No ______

   WhiteHat agrees with items VI.F.1, VI.F.3 and VI.F.4 as written. With regard to Section VI.F.2, WhiteHat has provided a document entitled *VCU_RFP(XI-XIII)_General Terms_WH Comments(3May)* ("VCU General Terms Comments") that includes WhiteHat's comments to VCU's standard terms and conditions and sections from WhiteHat's standard terms and conditions that are applicable to the performance of WhiteHat services.

   If "NO," identify the specific term and condition(s) and the reason for non-compliance.

2. Utilization of the words "should" or "may" in Section VI, Statement of Needs, Items A through E indicates a non-mandatory requirement.
   Does / Shall your company comply with the non-mandatory technical requirements as presented in Section VI, Statement of Needs, Items A through E (i.e. "should" becomes "shall")?
   Yes __XX___ No ______
   If "NO," identify the specific requirement and the reason for non-compliance.

3. On page 7 of the WhiteHat proposal, the information about the warranty is not clear. Is the information submitted the entire warranty? What is the reference to Section 4.3? Is there warranty/indemnification to protect VCU from any third party infringement claims? Please provide a copy of the complete warranty.

   All of WhiteHat's warranties from its standard terms and conditions were provided in WhiteHat's initial RFP response. These warranties can be found in Section 7 of the VCU General Terms Comments document provided separately. WhiteHat is open to considering additional reasonable warranties proposed by VCU. While WhiteHat does not offer a non-infringement warranty, we do offer IP infringement indemnification – see Section 8 of the VCU General Terms Comments document.

4. Confirm that the offer from WhiteHat to provide the Application Vulnerability Scanner is not expired. Does WhiteHat agree to extend the offer until June 30, 2017?

   Yes, WhiteHat Security agrees to extend the offer until June 30, 2017.

5. Small, Women-Owned and Minority-Owned Business Commitment:
   Complete and submit Appendix I of the RFP. (Attached) VCU has a 42.0% SWaM expenditure goal.

   Provided separately as part of email transmission dated May 8, 2017.

6. Invoicing and Payment:
   Complete and submit Appendix I of the RFP. (Attached)

   Provided separately as part of email transmission dated May 8, 2017.

7. Please indicate how long after the contract award your firm can commit the proposed resources to the project.

   Immediately.

8. While VCU does have 247 Web Applications, the proposed price for the Sentinel Application Vulnerability Scanner solution is significantly over budget. At this time VCU is considering phasing in the number of Web Applications starting with the forward facing applications. Please come prepared to discuss reducing the number of applications, the DAST Pricing Weighted Average, and the size of the Web Applications. Also, it would be helpful to know what actual price differences there are between Platinum Support, Gold Support and other support offerings.

Provided separately as part of email transmission dated May 8, 2017, entitled VCU Pricing.

9. Is the pricing offered the most favorable pricing offered to any customer for the same volume at this particular time? What additional discounts or price breaks can be offered?

   WhiteHat maintains the pricing enclosed herein is consistent with pricing issued in circumstances similar to the scope VCU has outlined.

10. Please elaborate on the coverage.

    Provided separately as part of email transmission dated May 8, 2017, entitled Datasheet Customer Support.

11. Confirm that the Clarification Response dated March 10, 2017 is incorporated into the Negotiation Response by reference.

    Yes, WhiteHat Security's Clarification Response dated March 10, 2017, is incorporated into the Negotiation Response via email transmission.

# WhiteHat Sentinel Customer Support

## Optimizing your use of WhiteHat Sentinel with fast, reliable support

WhiteHat empowers you to protect critical data, ensure compliance, reduce risk and accelerate the deployment of secure applications and websites. By providing accurate, comprehensive, and risk-based application security assessments as a software-as-a-service, we deliver the visibility, flexibility, and guidance that organizations need to prevent web attacks.

WhiteHat Support services ensure that you are effectively leveraging all the web application security information that WhiteHat Sentinel delivers. With over 40,000 web applications under management, many in the Fortune 500 companies, WhiteHat's customer support team has superior technical experience in application security, delivering the resources you need to reduce risk, and improve security processes.

WhiteHat Security's highly trained security teams provide enterprise-class software security support. Our engineers know web servers, web applications, and web application software development, including hands-on experience with leading software development frameworks, design patterns, and implementation practices, as they relate to security. There are three levels of support available to Sentinel customers: Standard, Gold, and Platinum.

### HIGHLIGHTS

Keep your business running in production with quick response times. WhiteHat Sentinel assesses live production applications safely, without impacting performance or your bottom line. Whenever you need expert assistance, we are just a click, email, or phone call away.

Access our Customer Success Center instantly to log, track and update cases online. The Customer Success Center also offers the latest security information, FAQs, training information, and product documentation.

## Support Levels

### STANDARD

Standard Support is included with all WhiteHat Sentinel subscriptions. It provides multiple contact options, such as access to our secure Customer Success Center, email access, or via a direct phone number.

**Customer support hours are**
**12:00 AM – 7:00 PM PST, Monday through Friday, excluding holidays.**

### GOLD

The Gold Support is designed for enterprise customers who require a highly personalized, proactive support relationship. Aligning people, processes and technology to achieve operational readiness is a key goal of this program. Gold support includes integrating technology with organizational processes, website deployment, change management, and support escalation to reach and remain at a state of operational readiness. To meet these objectives, Gold Support includes:

- An assigned Customer Success Manager (CSM)
- Priority response times and service level agreements (SLAs)
- Regularly scheduled meetings with your CSM to ensure operational efficiency
- Quarterly Business Reviews designed to maximize the value of your purchase
- Custom vulnerability exploit and remediation review

**Customer Success Manager**

Your assigned Customer Success Manager (CSM) is a highly skilled security professional who facilitates support requirements and escalates resolution requests to ensure that your issues are resolved quickly. Based on monthly business reviews, the CSM will manage your service requirements, including the review of open vulnerabilities and the management of each case to ensure proper closure. Each CSM serves as a cross-functional, cross-company advocate, who guides your organization in best practices and enables you to make rapid progress to align your security program with your business goals. The CSM coordinates support services and collaboration between WhiteHat Security, your web application business owners, developers, and security teams.

**Custom Vulnerability Exploit and Remediation Review**

WhiteHat Security will work with your developers to classify and understand the root causes and weaknesses of the discovered website vulnerabilities. Our security engineers are available to talk to your developers, provide a proof of concept, and help them understand the best remediation options available and how other web technology leaders are addressing these issues.

## PLATINUM

Platinum Support is ideal for commercial, government, enterprise, or global organizations utilizing the WhiteHat Sentinel family of products to deploy a comprehensive application security program across the software development lifecycle, and for organizations having stakeholders across multiple divisions or countries.

Platinum Support provides the highest level of a personalized support relationship with WhiteHat Security by providing both a Customer Success Manager (CSM) and giving you direct access to senior Threat Research Center (TRC) security engineers. Platinum level support also includes an annual onsite strategic process review. Platinum Support includes:

- Annual onsite strategic process review
- Quarterly vulnerability review
- Direct access to senior security engineers
- An assigned Customer Success Manager (CSM)
- Priority response times and service level agreements (SLA)
- Custom vulnerability exploit and remediation review
- 24/7/365 access to the Customer Success Center
- WhiteHat Sentinel interface training

### Annual Onsite Strategic Process Review

WhiteHat Security will provide a senior security engineer to spend three days onsite at your facility to help your team develop and execute strategic website risk management plans tailored to your specific business environment. During an annual review, for example, strategies can be developed that enable different business stakeholders – including risk management and compliance, product management and software development teams – to share ideas with WhiteHat experts and strategize on best practices for web security.

Annual Onsite Strategic Process Reviews cover:

- Vulnerability data discovered during the ongoing Sentinel assessments.
- Reports with remediation statistics and metrics.
- Mitigation techniques and security best practices.
- Overview of the current web security landscape and how it affects your organization.

### Direct Access to Senior Security Engineers

WhiteHat provides you direct access by phone and email to senior security engineers. WhiteHat will respond to your requests for assistance within two business hours on Mondays through Fridays from 6:00 AM and 7:00 PM PST, excluding WhiteHat holidays.

Platinum Support includes:

### Quarterly Vulnerability Review

Once per quarter, WhiteHat conducts a detailed review of high risk vulnerabilities discovered. The objective is to help your organization streamline the remediation process. During this review, a WhiteHat security engineer will give live demonstrations of the vulnerabilities, to show how high-risk vulnerabilities can threaten your business. By clearly understanding how each vulnerability can be exploited and understanding the risk associated with each vulnerability, you will be able to prioritize, manage, and mitigate your website risk more effectively.

## Support Features

| SUPPORT FEATURES | STANDARD | GOLD | PLATINUM |
|---|---|---|---|
| Customer Support Web Portal<br>• Case Management<br>• Security Documentation<br>• Knowledgebase & FAQs | ● | ● | ● |
| Sentinel Interface Training<br>• (Onsite training not included in any service level.) | ● | ● | ● |
| Service Request Response Time:<br>(cases submitted during business hours: M-F 12:00 AM – 7:00 PM PST) | Next Business Day | 1 hour - Critical (24x7)<br>4 hours - Serious | 1 hour - Critical (24x7)<br>4 hours - Serious |
| Priority Resolution Service Level Agreements (SLA)<br>• Severity Critical - 1 business day<br>• Severity Serious - 3 business days | | ● | ● |
| Quarterly Business Reviews | | ● | ● |
| Custom Vulnerability Exploitations and Remediation Reviews (PoC) | | ● | ● |
| Annual Onsite Strategic Process Reviews (T&E not included) | | | ● |
| Quarterly Vulnerability Reviews | | | ● |
| Direct Line Senior Security Engineers (12AM – 7PM) including holidays | | | ● |

WhiteHat SECURITY.

WhiteHat
SECURITY

Virginia Commonwealth University
VCU

# WhiteHat Security
# RFP #7286528JC – Application Vulnerability Scanner
# Prepared for VCU
# March 10, 2017

Christopher Perkins
Regional Sales Director
571.481.0895
chris.perkins@whitehatsec.com

## VCU'S ORAL PRESENTATION QUESTIONS

**You will find as part of the enclosed, both the answers to the questions you posed in connection with our most recent onsite during the Oral Presentation Phase of your RFP but, also, information around other questions VCU has asked in previous meetings (supporting documentation included).**

**How do you manage the varying personalities from a Customer Service & Technical Perspectives?**

Answer can be found in Ryan O'Leary's, VP Threat Research Center Video Testimonial to the VCU Security Team & Supporting Staff.
https://www.youtube.com/watch?v=dQJzq8zzl8A&feature=youtu.be

**How is it in a bullpen environment can we ensure consistency in the approach/process/methodology by which the customer is served by the TRC?**

Answer can be found in Ryan O'Leary's, VP Threat Research Center Video Testimonial to VCU Security Team & Supporting Team.
https://www.youtube.com/watch?v=dQJzq8zzl8A&feature=youtu.be

**Having pioneered Dynamic Application Security Testing 15 years ago, what things are you doing to stay ahead of your competition? Where is WhiteHat and its services headed?**

Answer can be found in Setu Kulkarni's, VP Product Management, Video Testimonial.
https://www.youtube.com/watch?v=dQJzq8zzl8A&feature=youtu.be

**Why WhiteHat, Why a Software-as-a-Service Model vs. a Tool Approach?**

Answer can be found in Craig Hinkley's, CEO, Video Testimonial to the VCU Security Team & Supporting Staff.
https://www.youtube.com/watch?v=dQJzq8zzl8A&feature=youtu.be

**Since vulnerabilities are assigned status values in a persistent findings model (i.e. 'Open,' 'Closed,' etc.), how does WhiteHat provide VCU with the ability to accept certain vulnerability findings as acceptable risks that do not require immediate attention/remediation? How can these acceptable risks be tracked by VCU?**

In addition to 'Open' and 'Closed,' clients have the ability to flag vulnerabilities as 'Accepted,' whereby a vulnerability finding can be separately flagged for the purpose of reporting and data analysis. Any time a vulnerability is categorized as 'Accepted,' VCU will also have the ability to assign a Tag to the vulnerability, for the purpose of tracking why the vulnerability was identified as an acceptable risk for VCU. All findings will continue to age based on first identification, until such time as they are successfully closed.

**How deep does WhiteHat's Mobile testing capability go? Specifically, how does WhiteHat address Dex Byte Code?**

During Mobile testing, WhiteHat will decompile the binary into the Dex Byte Code and review for the presence of any hardcoded sensitive data. However, WhiteHat does not conduct a line-by-line review of that byte code.

**What is the SLA for response times on the 'Ask a Question' component of service?**

There is no *standard* SLA for response times for this service component. Responses from the Threat Research Center take no longer than 24 hours. However, almost all response times are significantly faster than 24 hours, as the TRC is staffed 24x7. Typical response time is same-day, usually a few hours or less, depending upon the questions asked and the time of day.

**Your solution should have project management components built in, where VCU's security teams and developer teams can address flaws found and record that treatment in one system for auditing purposes.**

All WhiteHat findings are "stateful" rather than stateless. This means that vulnerabilities remain 'Open' until corrected in subsequent testing, at which point in time the vulnerability will be updated to 'Closed.' This is in contrast to static results and reporting, which requires side-by-side or delta analysis. In addition to 'Open' and 'Closed,' clients are able to elect to accept vulnerability findings without remediating, which are then labeled as 'Accepted.' An audit log of all vulnerabilities is maintained for each individual finding.

**Your solution should also provide historical tracking in regards to what flaws were found and when.**

All WhiteHat findings are tracked from first discovery, and will age based on time passed since first identified. WhiteHat will provide aging metrics for vulnerabilities, and these metrics are also incorporated into WhiteHat dashboards for trending analysis.

**Your solution should be able to notify VCU whether a particular application is utilizing the vulnerable routines in a particular third-party library.**

WhiteHat is able to identify and analyze third party libraries and components, and Software Composition Analysis is available for all Sentinel Source (SAST) customers at no additional cost. If desired by clients, and assuming there are no contractual/licensing obstacles between clients and their third-party content providers (or between WhiteHat and content providers), WhiteHat is able to scan third party libraries as long as the referenced files are included within the branch of code that is targeted for testing.

**What is your proposed pricing and licensing model?**

Flexible SaaS model. Pricing is based on both an annual subscription model per application or an annual point based subscription system to provide the upmost scalability and flexibility – and includes but not limited to the following services:

| Service | WhiteHat Security |
|---|---|
| Free of false positives | WhiteHat Security engineers manually verify vulnerabilities to ensure accurate, actionable data that is free of false positives. |
| Custom configured web forms | WhiteHat Security provides intelligent, manual form execution. WhiteHat Security engineers manually configure forms – working to exercise the many form variations. For example, if 5 different completion paths exist, accordingly the engineer will work to assess the 5 site areas. |
| Production safe | WhiteHat Security technology is uniquely designed to operate in the production and pre-production environments. WhiteHat Security engineers tune and configure the testing service environment to ensure production safe testing. |
| Access to Web Application Security Experts | WhiteHat Security team members are recognized industry-wide for their contributions and expertise. We provide phone, email and chat access to the team in support of vulnerability concerns and resolution in an unlimited fashion at no additional cost! |
| Coverage for the 49 WASC Threat Vectors | WhiteHat Security uses WASC threat classes as our guidepost for performing assessment services. WhiteHat Sentinel Service provides the most complete coverage in the industry providing |

| | |
|---|---|
| | support for the full complement of WASC-defined vulnerabilities – business logic and technical. |

| | |
|---|---|
| Dedicated Customer Success Manager | The CSM is accountable for coordinating support services and provides a conduit between WhiteHat Security, your web application business owners, web developers teams. The CSM is an advocate for the customer. |
| Trend analysis | Historical vulnerability data enables measurement and tracking of secure code training, contract programmer services, and other remediation efforts. Vulnerability data is rated and presented by severity, threat, and web property asset valuation. Results can be measured providing helpful cost-justification for future initiatives. |
| Unlimited Assessments / Keep Pace with Code Changes | Service frequency is expressly intended to help customers mitigate gaps between annual and / or periodic pen-tests and keep pace with frequent code changes. The approach affords timely vulnerability identification and near real-time remediation. |
| Continuous threat updates | Continuous threat updates ensure identification of the latest exploits and up-to-date prevention. The solution is expressly intended to enable our customers to mitigate gaps between annual and / or periodic pen-tests. |
| Annual Onsite Strategic Process Reviews | WhiteHat Security will provide a senior security resource to review onsite with business owners, the security team, and others the overall security posture of your company. This review will discuss:<br>▪ Vulnerability data discovered during the ongoing Sentinel assessment<br>▪ Vulnerability statistics and measurements<br>▪ Mitigation techniques and Security best practices<br>▪ The current web security landscape |
| Static Code Analysis (SCA) | WhiteHat Sentinel Source is our static application security testing (SAST) product. It is used for scanning source code, identifying vulnerabilities, and providing detailed vulnerability descriptions and remediation advice, as well as precise ready-to-implement remediation solutions for particular exposures. |

PROPOSAL TERM SHEET

## WHITEHAT SENTINEL – PREMIUM EDITION

WhiteHat Sentinel Premium Edition (PE) is ideal for websites that are permanent, mission-critical, have multi-step 'forms, and have rigorous compliance requirements.

Fully PCI 6.6 compliant, Sentinel Premium Edition protects websites that might be the potential victim of a systematic, repeatable and targeted attack, and includes testing for both technical and business logic vulnerabilities.

Business Logic Testing includes creating a customized testing scheme developed and performed by WhiteHat Security Engineers, mapping out your web application (users, roles, and custom business workflow), identifying and validating account privileges across roles and between users, as well as prioritizing vulnerabilities based on your business goals and intentions.

## WHITEHAT SENTINEL – STANDARD EDITION

WhiteHat Sentinel Standard Edition (SE) is designed for websites that are permanent, but not necessarily mission-critical or sensitive in nature, and may have multi-step forms and authenticated user access.

WhiteHat engineers in the Threat Research Center will manually configure the Sentinel scanning engine to ensure proper coverage and safe testing. Additionally, security engineers at WhiteHat will monitor applications for changes that may require new configuration updates, and engineers will also configure Sentinel's proprietary Login Handler technology to ensure proper session management for the duration of testing.

## WHITEHAT SENTINEL – BASELINE EDITION

WhiteHat Sentinel Baseline Edition (BE) is intended for websites that are primarily static by nature, with little or no user interaction within the application itself. This may include permanent as well as temporary applications, and Baseline Edition scans are provided on an unlimited basis while maintaining production safety.

All vulnerabilities found among websites that are tested using WhiteHat Sentinel Baseline Edition are manually verified by security experts in

WhiteHat's Threat Research Center, and WhiteHat engineers are available to answer any vulnerability-specific questions on a 24/7 continuous basis.

## ALL SENTINEL EDITIONS INCLUDE:

- 100% Verified Vulnerabilities (150 Security Experts at Threat Research Center)
- Remediation Guidance for all verified vulnerabilities
- Unlimited Continuous and Concurrent Testing
- Concierge On-boarding and Administration
- Production Safe (Single Threaded and Benign) Testing
- Full Application Configuration for customized testing – including continuous monitoring and fine tuning
- Configurable Prioritization of Applications and Vulnerabilities
- 24/7 Dashboard access via the Internet
- Open XML API Integration
- Unlimited Role Based User Access
- Customized Trending Analysis and Benchmarking

## WHITEHAT SECURITY – STATIC (SOURCE CODE) TESTING SERVICES:

WhiteHat Sentinel Source is part of the WhiteHat Sentinel suite of vulnerability management solutions. Sentinel Source is a subscription-based Static Application Security Testing (SAST) solution, directly inspecting source code for vulnerabilities. WhiteHat has designed a solution from the ground up to address the unique characteristics of SAST. Source code assessment permits the discovery of vulnerabilities that are harder to detect in production, and by doing assessments in the development phase, vulnerabilities may be remediated earlier.

WhiteHat Sentinel Source directly assesses source code and gives developers accurate vulnerability data, enabling them to assess and fix code continuously throughout the software development lifecycle (SDLC). Sentinel Source includes verification of all vulnerabilities by the WhiteHat Threat Research Center (TRC).

WhiteHat Sentinel Source, when combined with WhiteHat Sentinel, delivers a proven, scalable and affordable enterprise website security platform (incorporating consistent testing methodologies, processes, and governance) across the SDLC - reducing the risk of exposure to website security breaches.

**Preservation of Intellectual Property:** No need for source code, the foundation of any business, to leave the premises. Sentinel Source was designed to fit within the way organizations work. WhiteHat deploys a H/W or VM appliance at the customer's site. Because assessments are done on the premises and only small code snippets are available to WhiteHat TRC engineers for verification, source code will not leave the developer's location – eliminating the possibility of IP loss or theft.

**Sentinel Source enables continuous update of attack vectors** via Rule Packs that identify and verify vulnerabilities – this ensures that developers stay up-to-date on the latest attacks.

**Easy to set up and use**: No need for in-house training or security expertise.

## SENTINEL SOURCE INCLUDES:

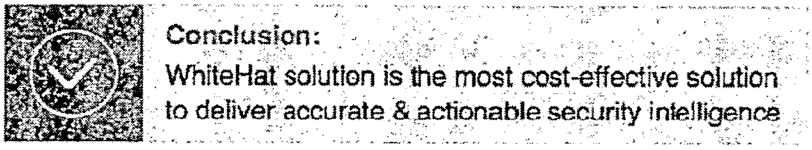
- Support for Java, .NET, PHP, JavaScript and Objective-C Languages
- 100% Verified Vulnerabilities (150 Security Experts at Threat Research Center)
- Remediation Guidance for all verified vulnerabilities
- Fully supported plugin integration with various SDLC programs, platforms and tools for optimal developer adoption
- Unlimited Testing
- Directed remediation and suggested patches for specific vulnerability classes
- Software Composition Analysis for third party and open source libraries
- Concierge Onboarding and Administration
- Full Application Configuration for customized testing
- Configurable Prioritization of Applications and Vulnerabilities
- 24/7 Dashboard access via the Internet
- Open XML API Integration
- Unlimited Role Based User Access
- Customized Trending Analysis and Benchmarking

## PRICING PROPOSAL

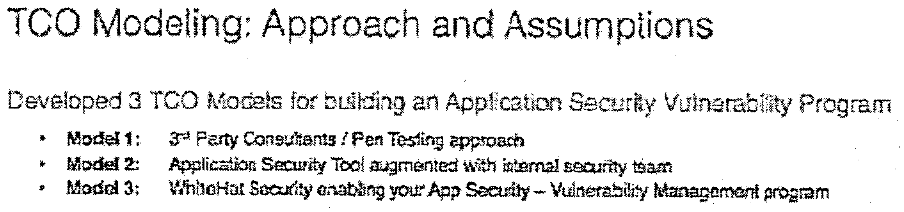
| Key Products | # of Units | Total price Customer |
|---|---|---|
| PE | 37 | 185,000 |
| SE | 123 | 307,500 |
| BE | 86 | 68,800 |
| Source - XSmall | 64 | 201,600 |
| Source - Small | 65 | 291,525 |
| Source - Med | 26 | 209,040 |
| Source – Large | 2 | 37,960 |
| Source – XLarge | 1 | 33,945 |
| Source – XXLarge | 2 | 112,420 |

WhiteHat SECURITY

| | | |
|---|---|---|
| Source – Jumbo | 1 | 62,050 |
| Platinum Support | 1 | 60,000 |
| TOTALS | | $1,569,840.00 |



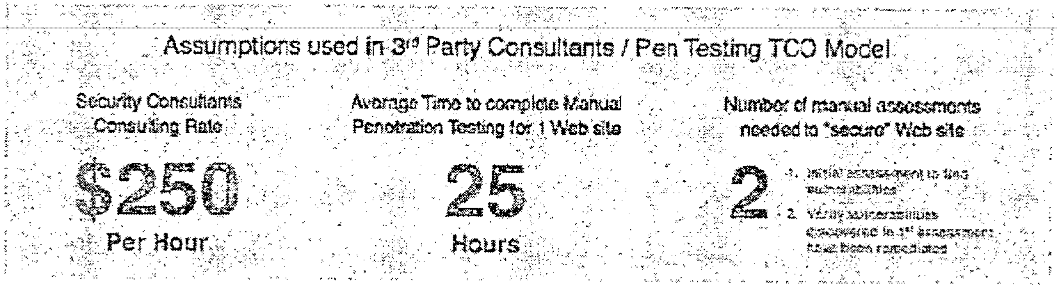
Conclusion:
WhiteHat solution is the most cost-effective solution to deliver accurate & actionable security intelligence



## TCO Modeling: Approach and Assumptions

Developed 3 TCO Models for building an Application Security Vulnerability Program

- **Model 1:** 3rd Party Consultants / Pen Testing approach
- **Model 2:** Application Security Tool augmented with internal security team
- **Model 3:** WhiteHat Security enabling your App Security – Vulnerability Management program



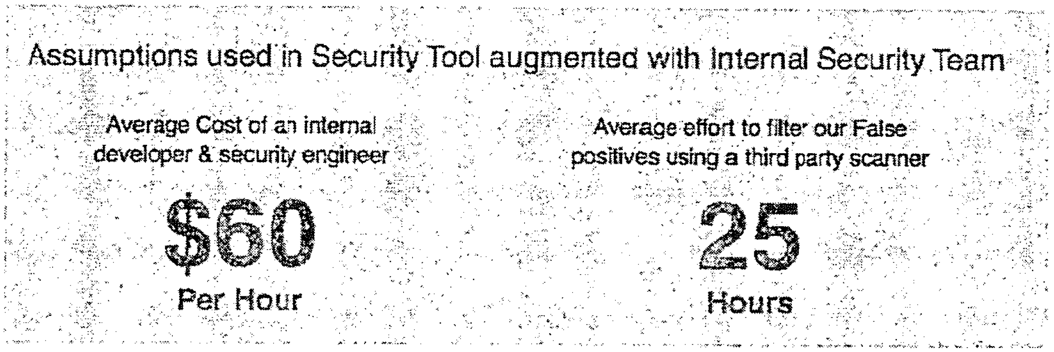
Assumptions used in 3rd Party Consultants / Pen Testing TCO Model

Security Consultants Consulting Rate
$250
Per Hour

Average Time to complete Manual Penetration Testing for 1 Web site
25
Hours

Number of manual assessments needed to "secure" Web site
2

1. Initial assessment to find vulnerabilities
2. Verify vulnerabilities discovered in 1st assessment have been remediated



Assumptions used in Security Tool augmented with Internal Security Team

Average Cost of an internal developer & security engineer
$60
Per Hour

Average effort to filter our False positives using a third party scanner
25
Hours

WhiteHat SECURITY

Time to manually find a vulnerability in source code

**60**
Hours

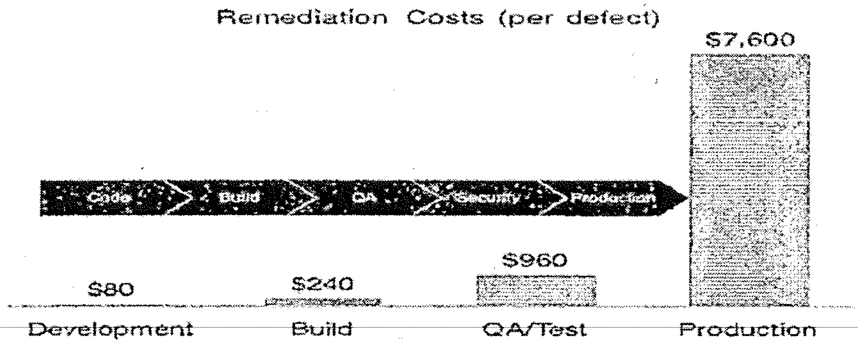
Time to do Software Composition Analysis Manually (SCA)

**8**
Hours

Average number of vulnerabilities in a web app for Insurance industry:

**12**
Vulnerabilities

WhiteHat 2016 Web Application Security Statistics Report: [illegible]



Sources: National Institute of Standards and Technology; Ponemon Institute

## PROPOSAL TERMS & CONDITIONS

- WhiteHat Security will work with VCU Legal to establish MSSA.
- Pricing Assumptions: 247 Web Applications | DAST Pricing Weighted Average: 15% PE, 50% SE, 35% BE
- Prepaid Payment Terms: Net 30.
- **Expiration: April 28, 2017.**

## EXECUTIVE SUMMARY

WhiteHat Security has been delivering SaaS based assessment solutions with proprietary technologies since 2003. The goal from the start was to offer the most complete and accurate web application solution that could scale to meet the needs of the world's largest organizations while requiring them to only have the security staff of smaller organizations.

Now that WhiteHat Sentinel is actively assessing more applications than any other platform in the world, resulting in the largest database of validated vulnerabilities of any kind worldwide, it is safe to say that the goal has been accomplished. WhiteHat Security is excited to propose the Sentinel risk management solution in response to VCU's Application Vulnerability Scanner RFP.

WhiteHat Security is the leading provider of Software as a Service based website risk management solutions that protect critical data, ensure compliance and narrow the window of risk. WhiteHat's security services combine proprietary scanning technology with custom testing by the industry's only Threat Research Centre (TRC) – **the largest team of its kind in the world**. The TRC is a team of over 150 web application security experts who act as a critical and integral component of the WhiteHat Sentinel website vulnerability management process.

As with all WhiteHat services, 100% of the vulnerabilities are manually verified virtually **eliminating** a problem with all automated scanning technology – **false positives** - greatly simplifying the remediation process for developers. Sentinel's self-service web based portal allows all stakeholders (management, security staff, developers, etc.) unlimited access to the same vulnerability information and at a level of detail that is tailored to the needs of each individual.

Over 15 years in the Application Security Testing space has afforded WhiteHat Security the opportunity to see first-hand the challenges being realized by security teams small and large alike. Through a partnership with WhiteHat Security, VCU will see first-hand why traditional approaches in securing assets at the application layer falls short in being able to scale, engender trust between DevOps and Security and, ultimately, provide an acceptable level of risk to organizations looking to address what has become the most vulnerable layer in the security stack – the application layer.

With the most recent accolade of being recognized as the most influential Security Vendor to CISOs in the market, we look forward to showcasing why it is through our Security-as-a-Service model **and the industry's only continuous, concurrent, production-safe scanning technology**, will VCU be able to claim it has provided its stakeholders and loyal clientele with the most secure, cost-effective method of protecting one's assets at the application layer in the market.

## COMPANY OVERVIEW WHITEHAT SECURITY

**How many years has your company been in business? Please list any major milestones such as significant acquisitions or the introduction or elimination of relevant lines of business.**

WhiteHat Security was founded in October 2001 and has been operating for 15 years.

WhiteHat SECURITY

**October 2016** – WhiteHat announced WhiteHat Sentinel Mobile Express™, a new addition to its mobile application security offerings powered by technology from mobile security solution pioneer NowSecure. The solution provides fast and accurate mobile application security testing using a combination of fully-automated static, dynamic, and interactive assessment technology and augmented by expert verification and analysis by WhiteHat Security's Threat Research Center (TRC). The new solution supports iOS, Android, and Swift applications, with detailed views and reporting integrated into the WhiteHat Sentinel platform.

**June 2016** - WhiteHat published its eleventh annual Website Security Statistics Report in May. This report provides a one-of-a-kind perspective on the state of website security and the issues that organizations must address in order to conduct business online safely. It is also the ONLY report that focuses exclusively on unknown vulnerabilities in custom web applications, code that is unique to an organization, and found in real-world websites.

**Mid-2015** - WhiteHat introduced the WhiteHat Security Index (WSI), a new feature in WhiteHat Sentinel that provides an immediate way for customers to understand how secure – or not – their websites are. It's the only report of its kind in the industry. An additional Peer Benchmarking dashboard enables users to determine the security of their web sites compared to industry peers.

WhiteHat Sentinel Source, WhiteHat's SAST solution, expanded its capabilities with Directed Remediation and Software Composition Analysis (SCA). The Directed Remediation capability offers targeted and customized code fixes for critical vulnerabilities, while the new SCA capability enables users to detect and remediate any vulnerabilities that are already known to exist in third-party libraries and open source code.

**August 2015** – WhiteHat announced the strategic partnership with Prevoty with product level integration that enables automatic mitigation of applications vulnerabilities via Prevoty's Runtime Application Self Protection (RASP) technology.

**August 2015**- WhiteHat Security was named a leader in the Gartner's Application Security Testing Magic Quadrant for the third year in a row.

**Late 2014** - WhiteHat expanded its TRC team to over 150 security experts total. In late 2014, the company established a research center in Belfast, Northern Ireland, and that team grew to over 50 security engineers by the end of 2015.

**August 2014** – WhiteHat Security was named a leader in the Gartner's Application Security Testing Magic Quadrant for the second year in a row.

**July 2013** – WhiteHat Security was named a leader in Application Security Testing by Gartner in July 2013.

**December 2012** – Launched Sentinel Mobile with support for iOS and Android.

**June 2012** – Launched Sentinel Source, a scalable Static Application Security Testing (SAST) solution.

**January 2012** – Launched Sentinel Baseline Edition (BE) Enterprise, which combines Asset Identification and Risk Profiling with Sentinel assessment services.

**June 2011** – Launched Sentinel PreLaunch (PL), which provides website vulnerability management and assessments for staging environments prior to production.

**June 2011** – Acquired Infrared Technology to add SAST, a static code application testing solution, into the Sentinel product family.

**April 2009** – Launched Sentinel Baseline Edition (BE), an Enterprise class entry-level web application security solution.

**December 2007** – Launched Sentinel Standard Edition (SE), an Enterprise class mid-level web application security solution that provides custom configurations.

**Describe your experience in working with companies similar to VCU.**

One of the greatest luxuries that WhiteHat Security offers us as employees is the ability to truly help companies become more secure. Over the years, we've taken our scalable SaaS model and greatly improved it, constantly refining due to the changing needs of both the security world as well as well as the security policy of the enterprises we work with.

The following is a good example of the experiences commonly shared by large enterprises that leverage WhiteHat:

1. Onboarding Phase – The on-boarding process is a critical juncture to establishing your trust and this process is where the end user gets to meet the support team. WhiteHat's Deployment Engineers are technical professionals with experience in the security industry, who review any open cases during the deployment phase and facilitate quick resolutions to ensure a seamless on-boarding experience. They provide end users with all the details needed to get the Sentinel service up and running. The information that is needed from the end user includes but is not limited to:

    a. Application URLs
    b. Credentials
    c. Assessment Schedule
    d. Mock Data
    e. Primary contacts / users
    f. Special testing instructions
    g. etc.

We typically start with either a WebEx or an onsite visit where we also discuss the Sentinel service and answer any questions the users may have.

2. Initial Assessment Phase – This is the initial two weeks after we've obtained the necessary assessment information. This is where all the applications that were set up are fully assessed, configured, and tested based on service line for vulnerabilities.

3. Results Overview Phase – After the initial assessment, we strongly encourage the end user to take some time and meet with us to discuss the vulnerabilities discovered. During this time, we will either present over WebEx or onsite, the issues that were found - often demonstrating them live at the request of the end user. We will go through what they are, how they were discovered, how they might impact the business, and answer any questions you may have about them.

4. Ongoing Maintenance Phase – After the initial assessments have been completed on the applications, the WhiteHat Security Threat Research Center (TRC) will constantly monitor the web applications as they are assessed based on the customer set schedule. Any changes to the application will be detected automatically, configured, assessed, verified, and reported to the Sentinel UI proactively. If anything is required by the end user, we will reach out to them and let them know exactly what is needed to ensure a thorough assessment. For example, if credentials are locked out or an associated hostname is needed.

5. Measuring Success Phase – This typically comes after several months of being under the WhiteHat service and often consists of measuring the success of the security program. We will work with the end users to provide metrics and trending of the overall data accumulated throughout the assessments. Example of this data include:

   a. Remediation Percentage
   b. Time to Fix issues
   c. Most common vulnerabilities
   d. Window of exposure
   e. WhiteHat Security Index (WSI) – WSI is a measure of a site's security posture, calculated from a comprehensive set of data signals including number of vulnerabilities, remediation rate, time-to-fix, window of exposure and many more.
   f. Peer Benchmarking - A comparison on key metrics including number of open vulnerabilities, average time-to-fix, and average remediation rates for your web applications against industry and global averages.

This data can then be compared to the industry averages across each of the major verticals. This begins the foundation of being able to answer questions like:

1. Are we getting better?
2. How do we compare to other people within the Entertainment industry?
3. What is our most common issue?
4. What are the possible consequences of having this issue?
5. How long does it take to fix a critical issue?

Throughout all of the phases, we maintain a strong information loop with our customers and greatly appreciate any feedback to continue the improvement of the Sentinel service.

**Describe any other relevant background information about your organization and your qualification to provide the request product/service.**

Key relevant background information includes:

- WhiteHat Security was first in the industry to deliver a Software as a Service (SaaS) solution for Dynamic Application Security Testing (DAST).
- We have the world's largest army of application security engineers in our Threat Research Center (TRC) of over 150 and growing. These security engineers act as an extension of your security team, by always being available to help you with any questions or concerns you may have in regards to the application security vulnerabilities.
- Performs approximately 300,000 assessments per month.
- Surpassed 40,000 websites under management by WhiteHat Sentinel in August 2016.
- WhiteHat Security operates 24x7x365

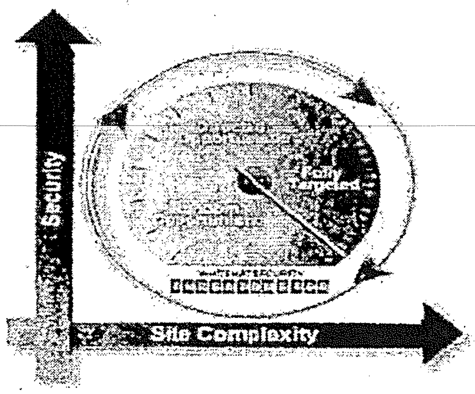
**Describe how multiple application security testing deployment solutions can be integrated into a unified architecture.**

- When leveraging multiple application security testing deployments, it is highly encouraged to create a single repository for vulnerability information, analysis, and management. This is especially useful when combining multiple layers of assessments, for example network scanning, infrastructure assessments, web application assessments, and source code analysis. There are GRC tools such as Archer, and Vulnerability Management systems like Coded, Kenna, and LockPath, even BI visualization engines like Tableau which can serve as a central location for all of this information.
- WhiteHat Sentinel integrates with all of these through various means, most

commonly via an XML API or CSV upload.

## KEY BENEFITS OF WHITEHAT SENTINEL SERVICE

**Turn Key:** WhiteHat Sentinel is a SaaS based assessment solution. There are no hardware or software configuration requirements by the customer. The only information required to start the service are the hostnames of the application, the permitted scan schedule and authentication credentials if required. The process does not require any customer resources to produce impressive, actionable results.



**Manually Validated and Prioritized Results:** Unique to WhiteHat Security, all vulnerabilities are verified by the Threat Research Centre to eliminate false positives and are prioritized by threat and severity, so results are accurate and actionable.

**Unlimited and Continuous Assessments:** WhiteHat provides Sentinel as an annual service. Sentinel enables organizations to comprehensively assess their production websites as frequently as they deploy new code, whether it is a patch or a major release. Most of our customers are running assessments on a continuous, 24x7 basis.

**Unlimited User Access:** All Sentinel services include unlimited user access to the Sentinel portal. The level of user access is governed by the assigned Sentinel role and applications the user is granted access to. The customer can administer the accounts of all the Sentinel users via the Administration area of the Sentinel portal.

**Open RESTful API:** The Sentinel API allows users to integrate Sentinel information into their own applications with an extensible RESTful interface. The capacity to integrate Sentinel data into internal applications allows you to integrate with bug tracking, security information and event management (SIEM), and Web application firewall (WAF) products. The API currently supports vulnerability data, website configurations, and policy information.

**Individual Vulnerability Retesting:** Users of the portal with appropriate access can initiate the retest of individual vulnerabilities with a simple click of the mouse. If the vulnerability was automatically detected, the retest will occur immediately and the result will be published within minutes. If the vulnerability was manually detected, the retest will be placed in a queue and a security engineer will manually test the vulnerability and publish the results that same day. This allows developers to get quick feedback and more effectively remediate vulnerabilities.

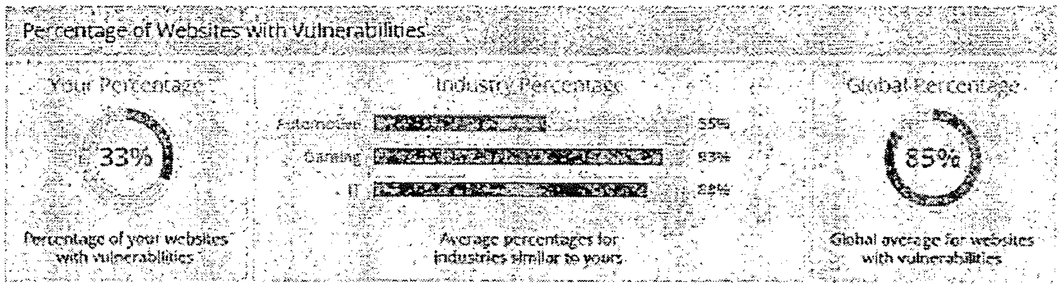
**Direct Access to TRC Engineers:** Each vulnerability description will include a detailed description of the vulnerability, how to remediate the vulnerability, and a list of external resources to get more information about that category of vulnerability. If a user has a question about any of this information or about anything related to the vulnerability, they can submit a question to the TRC engineers via a button in the Sentinel portal. This will initiate a logged conversation within the portal that will be displayed along with the vulnerability details.

**Email Alerts:** Sentinel users can elect to receive automatically generated emails from Sentinel that will provide a status of the applications they have access to, as well as all associated open vulnerabilities. This will ensure users are aware of all newly discovered vulnerabilities even if they don't regularly log into the Sentinel portal.

**Flexible Reporting:** PDF, CSV and XML reports can be generated within the Sentinel portal. The reports can be generated for single or multiple applications. Filters can be applied when generating the reports to control what content should be included in the report.

**Integration with SDLC:** Sentinel Source supports commonly used programming languages, and provides plug-ins and integrations with popular Integrated Development Environments (IDEs), Software Configuration Management (SCM) products, bug trackers like Jira, dependency management frameworks and build servers like Jenkins, as well as ALM tools with WhiteHat Integration Server. Developers can view custom vulnerability descriptions and remediation advice, directly ask a question to TRC engineers and use bug trackers to track vulnerabilities entirely within their IDE tool.

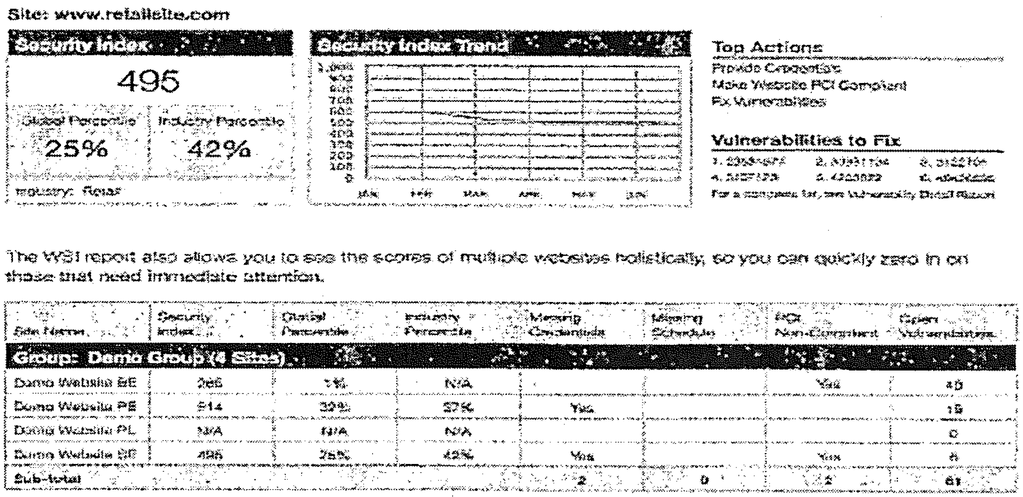
**Peer Benchmarking:** At WhiteHat, we have assessed tens of thousands of websites across a range of verticals, which offers us a unique perspective into the security posture of organizations of various sizes. Our peer benchmarking dashboard displays a comparison of ley metrics like number of open vulnerabilities, remediation rate, time to fix etc. for not just your websites, as compared to others in your industry or globally. This allows you to benchmark your security posture against industry peers – and this is the data that you can bring to the management and the board while making key security decisions.



Percentage of Websites with Vulnerabilities

| Your Percentage | Industry Percentage | Global Percentage |
|---|---|---|
| 33% | Automotive 55%<br>Gaming 93%<br>IT 28% | 85% |
| Percentage of your websites with vulnerabilities | Average percentages for industries similar to yours | Global average for websites with vulnerabilities |

**WhiteHat Security Index:** Sentinel's WhiteHat Security Index (WSI) enables you to understand the overall security status of your websites. It also provides you with a common metric to compare the security posture of each of your websites. Calculated from a comprehensive set of indicator data, including window of exposure, number of vulnerabilities, time-to-fix, remediation rate, and more, the WSI gives you an instant, visual overview of the robustness of your security posture.



Site: www.retailsite.com

Security Index

495

Global Percentile 25%

Industry Percentile 42%

Industry: Retail

Security Index Trend

Top Actions

Provide Credentials

Make Website PCI Compliant

Fix Vulnerabilities

Vulnerabilities to Fix

1. [illegible] 2. [illegible] 3. [illegible]
4. [illegible] 5. [illegible] 6. [illegible]

For a complete list, see Vulnerability Detail Report

The WSI report also allows you to see the scores of multiple websites holistically, so you can quickly zero in on those that need immediate attention.

| Site Name | Security Index | Global Percentile | Industry Percentile | Missing Credentials | Missing Schedule | PCI Non-Compliant | Open Vulnerabilities |
|---|---|---|---|---|---|---|---|
| **Group: Demo Group (4 Sites)** | | | | | | | |
| Demo Website BE | 265 | 1% | N/A | | | Yes | 45 |
| Demo Website PE | 514 | 39% | 57% | Yes | | | 15 |
| Demo Website PL | N/A | N/A | N/A | | | | 0 |
| Demo Website SE | 495 | 25% | 42% | Yes | | Yes | 8 |
| Sub-total | | | | 2 | 0 | 2 | 61 |

## WHITEHAT SENTINEL DAST – DYNAMIC ANALYSIS

WhiteHat Sentinel, built on a SaaS (Software-as-a-Service) – or Cloud-based technology platform, is the only solution to combine highly advanced proprietary scanning technology with custom testing by the Threat Research Center (TRC), a team of website security experts who act as a critical and integral component of the WhiteHat Sentinel website vulnerability management service.

Unique to WhiteHat Security, every vulnerability discovered by any WhiteHat Sentinel Service is manually verified for accuracy (by the TRC) and prioritized, virtually eliminating false positives and radically simplifying remediation. Sentinel DAST assessments are production safe and run continuously. This ensures that customers know the risk of their production web applications regardless of how frequently they are pushing changes. In addition, all WhiteHat Sentinel services satisfy, and exceed, PCI requirements for Web application security.

## SENTINEL PREMIUM EDITION (PE)

Ideal for Websites that are permanent, mission-critical, have rigorous compliance requirements and, in which, the company relies on serving its customers or business partners and has multi-step form-based processes.

- Continuous Automated & Manual Testing
- Fully customized and configured for safety / thoroughness
- All Results Manually Verified
- Authenticated Technical & Business Logic Vulnerabilities

## BUSINESS LOGIC VULNERABILITY TESTING

Concurrently to the Sentinel automated assessment, the business logic assessment begins after the web application has been on-boarded.

A team of security engineers will map out and test your web application's business logic and workflows, paying particular attention to privileges between and across roles and users. For example:

- Can an Employee User access administrative functionality?
- Can a user see information for any companies other than their own?
- Can a user elect a Benefits package that should not be available as an option?

This additional testing by our engineers ensures that your business-critical applications are being thoroughly assessed against any form of attack a malicious user may attempt. Vulnerabilities discovered during the business logic assessment are reported in the Sentinel Interface with specific details:

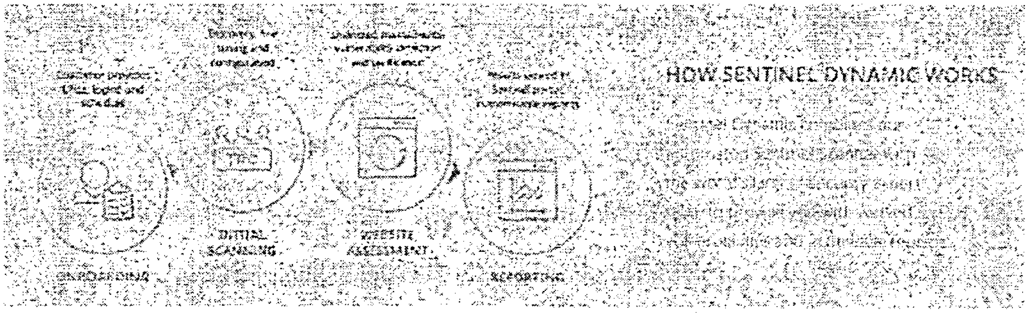
- A custom description of the vulnerability and how it is exploitable
- Steps to reproduce the vulnerability
- The location of the vulnerability
- Request and response details
- A vulnerability score aligned with PCI and CVSS
- Recommended solutions and best practice

WhiteHat SECURITY

VCU Virginia Commonwealth University

## PRODUCTION SYSTEM SAFETY

WhiteHat Sentinel DAST has been designed from the very beginning to be extremely safe for production web applications. Our maxim at WhiteHat Security is "Do No Harm" or, put more casually, we like to ask before running a scan: "Is this Important?" instead of asking afterwards, "Was that important?" By default, WhiteHat Sentinel operates "production-safe." This means that WhiteHat Sentinel only performs tests that it identifies as idempotent – that is, tests that will not permanently change the state of the system. So, you can be confident that WhiteHat Sentinel will safely scan your production business websites during production (business or high-traffic) hours. We have implemented three key features that are unique to WhiteHat Security that ensure that our testing remains completely safe for your production websites.



## CUSTOMIZED CONFIGURATIONS

The WhiteHat Threat Research Centre (TRC) manually reviews your web application and customizes Sentinel testing for safety and thoroughness. Every input, state changing request (POST request), or sensitive functionality is carefully analyzed by a human security engineer of the TRC. The security engineer will check this functionality for safety first, then for depth and coverage. This is especially applicable to administrative level functionality – things like create/delete user or groups. This kind of functionality is deemed unsafe to test in an automated fashion and Sentinel will be configured to not place these sensitive requests. A security engineer will test this functionality by hand instead in order to ensure the safety of the application.

Examples of functionality that is commonly deemed unsafe:

- Creation and deletion of users or data
- Contact us features that involve sending e-mail
- Updating/Editing Profile or account data
- Leaving comments or forum posts (Submit functionality)

When an input or area of functionality is deemed safe for automated testing, a security engineer will configure Sentinel submit valid data in order to get further into the application. For example:

The website has a registration page that requires a valid name and e-mail address to get to the next step of the registration process. A security engineer will recognize that these inputs are required and teach Sentinel to submit valid information in order to get

WhiteHat
SECURITY

WHITEHAT SENTINEL

# Application Security Testing RFP

VCU
VIRGINIA COMMONWEALTH UNIVERSITY

RFP #: 7286528JC
RFP Title #: Application Vulnerability Scanner
Issuing Agency: Virginia Commonwealth University
Using Dept.: Technology Services
Issue Date: November 29, 2016
Closing Date: January 6, 2017 at 11:00 AM

## Table of Contents

## Executive Summary

WhiteHat Security is pleased to provide VCU with the following RFP response.

In our RFP response, we are proposing WhiteHat's Sentinel SaaS Solution to meet your website application security and risk management needs. WhiteHat Security offers various levels of Sentinel services – WhiteHat Sentinel Premium Edition (PE), Standard Edition (SE), and Baseline Edition (BE) And Sentinel Source Services. WhiteHat Sentinel Services combine our proprietary scanning technology with ongoing customized configuration assessments by the WhiteHat Threat Research Center (TRC) to ensure accuracy. All vulnerabilities are Manually verified, virtually eliminating a problem that plagues all automated scanning technology – false positives – and efficiently simplifying the remediation process for developers.

The WhiteHat Sentinel PE Service includes Manual business logic assessments by the WhiteHat Threat Research Team to identify business logic flaws within an application. Uncovering business logic vulnerabilities can only be done by manually reviewing web applications to test key areas such as account structures and other contextual logic.

WhiteHat Sentinel is a turnkey SaaS solution requiring no hardware installation, software configurations, or hiring and training of additional security personnel. The web-based User Interface allows all users (management, security staff, developers, 3rd party consultants, etc.) unlimited or role based access to detailed vulnerability information with suggested recommendations and solutions to remediate the vulnerability and identify risk exposure over time. User access and privileges can be set at a level of detail that is tailored to the needs of each individual.

*KEY BENEFITS OF WHITEHAT SENTINEL SERVICE:*

- ***Assessments occur in Production*** – *It is critical to assess publicly facing web sites to minimize the window of exposure to vulnerabilities since this is where web application breaches occur.*
- ***Most Accurate Results*** – *All vulnerabilities are verified, including custom configurations of complex web applications and business logic testing.*
    - *All vulnerabilities are rated by a Severity and Threat scoring system including the CVSS scoring system.*

- ***Continuous and Concurrent Assessments*** – *Option to run assessments of all web applications either continuously (recommended: 24x7x365) or on a custom schedule.*
    - *"Continuous and Concurrent" is defined as the assessment of all web applications in parallel. Once assessment of all web applications is completed, the assessments will start over in a looping fashion.*
    - *Highly scalable to meet any number of web application in an Agile Software Development Life Cycle (SDLC).*
    - *Unlimited assessments.*
- ***Deepest security expertise*** – *WhiteHat Security has the deepest security expertise on the planet, from the co-founder of WASC and a board member of OWASP to the 150+ team of security engineers available to assess all your web applications and help to remediate vulnerabilities.*
    - *Access to security engineers at no additional cost*
- ***Easy-to-use solution & reporting***
    - *No configuration of hardware or software.*
    - *Web-based portal allows any number of users to access vulnerability results.*
    - *Vulnerability tracking over time shows every web application's risk and exposure.*

Thank you for providing WhiteHat Security with the opportunity to meet these requirements at VCU.

## VCU Statement of Needs

### *A. Scope of Introduction*

**1. VCU currently manages its IT operations through a hybrid approach, where most infrastructure services are managed centrally through the central Office of Technology Services ("OTS"), and customer facing services are managed in a decentralized fashion by individual schools and departments. Among the decentralized services, application development and provisioning are usually managed by individual departments and schools, with support of these applications collectively managed by both OTS and individual departmental groups. From a central services perspective, application provisioning guidance and general policies are available, but there is presently no streamlined process for verifiable implementation of the recommended and required controls.**

WhiteHat Security provides a cloud-based application security solution. For dynamic testing of web applications (DAST), applications are approached via the cloud. WhiteHat scanners will need to be provided with access to any non-public facing (internal) applications, but hosting location for the target applications is location-agnostic. For static source code testing (SAST), WhiteHat simply needs to be able to reach the location where code is being saved by development teams. WhiteHat can facilitate testing for code stored in multiple different locations, whether centralized, decentralized, or cloud-based.

**2. In order to minimize variances in the provisioning of applications and to ensure quality and security of applications before deploying them into production, VCU is currently developing an application vulnerability management program that integrates key processes, personnel, and technology to address the aforementioned challenges. From a technical architecture perspective, a critical component in this initiative is an application vulnerability scanner. The application vulnerability scanner is expected to help VCU in identifying, prioritizing, and tracking vulnerabilities in both internally-developed and third-party applications in use at the University. This Request for Proposals (RFP) is designed to help VCU select an appropriate application vulnerability scanner that can be integrated into its application vulnerability management program.**

Founded in 2001 and headquartered in Santa Clara, California, WhiteHat Security is the leader in application security, enabling businesses to protect critical data, ensure compliance, and manage risk. WhiteHat is different because we approach application security through the eyes of the attacker. Through a combination of technology, more than a decade of intelligence metrics, and the judgment of real people, WhiteHat Security provides complete web security at a scale and accuracy unmatched in the industry. WhiteHat Sentinel, the company's flagship product line, currently manages tens of thousands of websites. WhiteHat Sentinel is a software-as-a-service platform that enables your business to quickly deploy a scalable application security program across the entire software development lifecycle (SDLC). By combining our scalable application scanning platform with the world's largest threat research team, we identify where you are vulnerable with near zero false positives. WhiteHat Sentinel is incredibly easy to use – it requires no additional staff or software. No matter how much code, how many websites or how often they change, Sentinel can scale to meet any demand without slowing you down.

**3. Initially, the application vulnerability program will have 100 developers at the University and up to 247 applications (excluding cloud applications).**

Through WhiteHat Security's unique approach in protecting one's assets at the application layer, both the VCU Security Team, and the University's 100 developers, will be able to optimize its efforts in securing code along every stage of the SDLC, while in no way impeding the rapid development of new applications. VCU will see that WhiteHat Security provides the quickest time to value in the industry through its Security-as-a-Service in that of Sentinel.

**B. The Contractor shall furnish, deliver, implement and provide ongoing maintenance and support, and training for the application vulnerability scanner.**

**1. The Contractor shall provide support for the product through phone, self-service ticketing systems, and / or email on normal business hours (M-F 8 AM – 5 PM EST). 24x7x365 phone or email support for system is strongly preferred.**

Live vulnerability data and alerts: If you have 24x7 assessments enabled you will be alerted immediately when a vulnerability is discovered and have the full details available to begin remediation. Our Threat Research Center (TRC) is available 24 hours a day to answer any questions you, your team, or your developers may have about these vulnerabilities.

The ideal world when a critical issue is discovered is to have it immediately assigned out to a development team and begin remediation. If any questions or concerns are raised by the development team we are available to answer their questions! Support options include a 24/7 access to our Salesforce support portal, phone support, or email. All support options include the same follow-the-sun support model to ensure one-hour response for critical issues. WhiteHat staffs the Customer Support function 24x5. Platinum support includes access to a 24/7 pager notification on the weekends that connects the customer with the needed resource within an hour of the call. This mechanism has been proven with our largest customers, including onboarding new sites, any network or server impacting events, rendering assistance with critical vulnerabilities, or helping customers outside the Americas.

Response times for support ticket submissions is one hour for urgent issues and 4 hours for any other support requests 24/7. Urgent site assessment onboarding requests are completed within 4 hours and normal requests within one business day. Maintenance notifications are communicated to company administrators via email 72 hours prior to the performed maintenance. Outage notifications are provided immediately 24/7. Both announcements are available also in the support portal. Maintenance schedules are published 6 months in advance.

**2. The Contractor shall provide standard service level agreement indicating anticipated response times for service requests. At a minimum, the initial response time for support requests cannot exceed 3 business days.**

All WhiteHat customers receive one-hour SLA response to Sentinel outages. Other support SLA levels vary by contract level and topic, not to exceed one business day for low severity issues reported by Standard support customers. All support issues are handled with a four-hour SLA for Premium Gold support customers, and one-hour SLA for our Platinum support customers. This SLA is matched with round-the-clock staffing and a paging notification system to an on-call senior engineer who can assist with any customer emergencies.

**3. The Contractor shall provide optional on-site training, support, or upgrade service for the product.**

Upgrades are taken care of automatically by WhiteHat. Any training required to manage the onsite virtual appliance is delivered remotely. Onsite training for product usage, development security training, and many other topics can be purchased at any time.

**4. The Contractor shall provide options for request escalation for situation where rapid response or additional expertise is needed.**

Gold and Platinum support allocate a CSM to your account. The CSM will act as your single point of contact for ongoing management of your WhiteHat partnership as well as any escalations that are required. Your sales representative also acts as an escalation point and has a direct line to company senior management.

**C. The application vulnerability scanner shall be covered by the most favorable commercial warranties the Contractor gives any customer for the system.**

WhiteHat offers the following standard warranties:

**10. LIMITED WARRANTIES.**

**10.1 Conformance with Documentation.** WhiteHat warrants that the Services will substantially conform in all material respects in accordance with the Documentation. Customer will provide prompt written notice of any non-conformity and provide WhiteHat a reasonable opportunity, not to exceed thirty (30) days, to remedy such non-conformity. WhiteHat may modify the Documentation in its sole discretion, provided the functionality of the Services is not materially decreased during the Term.

**10.2 Service Availability.** WhiteHat warrants that the Services will meet the requirements set forth in Section 4.3 (Service Availability). In the event of a breach of the foregoing warranty, as Customer's sole and exclusive remedy, WhiteHat will provide the remedy set forth in Section 4.3.

**10.3 No Viruses.** WhiteHat warrants that the Services and the Training do not contain any computer code that is intended to (i) disrupt, disable, harm, or otherwise impede in any manner, the operation of Customer's software, firmware, hardware, computer systems or network (sometimes referred to as "viruses" or "worms"), (ii) permit unauthorized access to Customer's network and computer systems (sometimes referred to as "traps", "access codes" or "trap door" devices), or any other similar harmful, malicious or hidden procedures, routines or mechanisms which could cause such programs to cease functioning or to damage or corrupt data, storage media, programs, equipment or communications, or otherwise interfere with Customer's operations.

**10.4 Warranty Disclaimer.** EXCEPT AS PROVIDED IN THIS SECTION 10, WHITEHAT PROVIDES THE SERVICES AND TRAINING "AS IS" AND MAKES NO WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO THE SERVICES, TRAINING, REPORTS, DOCUMENTATION, TRAINING MATERIALS OR ANY OTHER RELATED DATA, AND SPECIFICALLY DISCLAIMS ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, USEFULNESS, ANY IMPLIED WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, TITLE OR FITNESS FOR A PARTICULAR PURPOSE AND ANY CONDITION OR WARRANTY ARISING FROM COURSE OF PERFORMANCE, DEALING OR USAGE OF TRADE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES IN CERTAIN CIRCUMSTANCES. ACCORDINGLY, SOME OF THE LIMITATIONS SET FORTH ABOVE MAY NOT APPLY. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THE TRAINING OR TRAINING MATERIALS AS A CITATION AND/OR AS A POTENTIAL SOURCE FOR FURTHER INFORMATION DOES NOT MEAN THAT WHITEHAT ENDORSES THE INFORMATION SUCH ORGANIZATION OR WEBSITE MAY PROVIDE OR THE RECOMMENDATIONS IT MAY MAKE.

**D. Mandatory Solution Requirements – The application vulnerability scanner shall at a minimum have the following specifications:**

**1. The application vulnerability scanner must provide up-to-date vulnerability data that allows the accurate detection of potential vulnerabilities in applications.**

The WhiteHat Sentinel service has created a continuous, real-time data feed and display for any vulnerabilities discovered throughout the software development life cycle (SDLC). For dynamic testing (DAST), the scanning technology runs "low and slow," which allows for safe testing of production applications, often on a continuous, 24x7 test schedule (although this can be adjusted to fit any scheduling requirements). As possible vulnerabilities are detected by WhiteHat's proprietary scanning technology, results are analyzed in real-time by WhiteHat security engineers in the Threat Research Center (TRC), and all confirmed vulnerabilities are immediately populated in the WhiteHat Sentinel user interface. For static testing of source code (SAST), testing is again scheduled on a repeating basis, with results immediately published to the WhiteHat Sentinel portal once confirmed by engineers in the TRC. For both SAST and DAST, vulnerability data is stateful, rather than stateless. This means that vulnerabilities are displayed as open/closed depending upon the most recent iteration of ongoing testing.

**2. The application vulnerability scanner must provide a central management console that displays vulnerability and trending data for all tested applications.**

Trending information on vulnerabilities, whether increasing over time or decreasing, can be used by organizations to pinpoint areas of need to reduce overall risk represented by website vulnerabilities.

**3. The application vulnerability scanner must have tiered management capability within the aforementioned central management console, where users of the console can be assigned roles and responsibilities based on individual responsibilities, and the principle of least privilege.**

All Sentinel services include unlimited user access to the Sentinel portal. The level of user access is governed by the assigned Sentinel role and applications the user is granted access. Customer can administer the accounts of all the Sentinel users via Administration area of the Sentinel portal. Access control is based on the concept of least privilege.

**4. The application vulnerability scanner must have the ability to conduct Dynamic Application Security Testing (DAST) of an application in testing or production environment, while minimizing impact to application availability.**

WhiteHat Security technology is uniquely designed to operate in the production and pre-production environments. WhiteHat Security engineers tune and configure the testing service environment to ensure production safe testing. The services purchased for production would be configured to be production safe (slower and uses benign tests only).

**5. The application vulnerability scanner must have the ability to conduct Static Application Security Testing (SAST) that supports (at a minimum) the testing of: Java, Javascript, C#, and PHP code.**

Our SAST offering can analyze a number of languages commonly used in the creation of web applications, including Java, JavaScript, ASP.NET, PHP and C#, the primary language used in the .NET framework.

**6. The application vulnerability scanner must have the ability to clearly explain vulnerability details, potential impact, risk rating, and proposed remediation options, in a manner and timeframe that is actionable to developers and system administrators.**

As part of the standard service, remediation advice is provided for every finding discovered during WhiteHat Sentinel assessments and is accessible using the web portal, API, and direct conversation with our Threat Research Center. We offer direct and unlimited access to our Threat Research Center for remediation guidance and advice, but do not offer any direct remediation services. We do have a wide network of partners that we are happy to refer you to in regards to remediation services. In addition, developers can get vulnerability descriptions and suggested remediation guidance as well directly ask-a-question and get responses to/from the TRC from within the IDE itself. Daily pen tests are performed and the remediation SLA is 24hrs for any vulnerability that may be found. With continuous scanning, WhiteHat can provide remediation times for each vulnerability, across 1,000s of site.

**7. The application vulnerability scanner must have the ability to track the vulnerability state for each application, and offer long term trending data for the security state of an application.**

The WhiteHat Security Index report assesses the risk of each individual application based on the vulnerabilities WhiteHat has identified for each, as well as comparing to global and industry percentiles. WhiteHat also provides executive dashboards to display application-specific information based on real-time data. These dashboards display trending data, information about the criticality and prevalence of vulnerabilities within the application, and offer insight into the overall health of individual applications from a security perspective. The dashboard reports can also be created for user-defined groups of applications, as well as for the entire portfolio of applications within scope of the engagement.

**8. The Contractor shall provide the option to deploy the application vulnerability scanner as a service in a hosted environment either directly to VCU or through a third party.**

The WhiteHat Security DAST scanning technology is housed in secure WhiteHat datacenters. The DAST scanner cannot be packaged and hosted elsewhere; scanning takes places by provisioning the WhiteHat scanners with access to target applications, either via secure satellite applicance (VM or Hardware), or by creating firewall rules to allow WhiteHat traffic. The SAST scanning technology is housed within a satellite appliance that can be deployed within the target network - direct or cloud-hosted - as long as the SAST satellite appliance can communicate back to WhiteHat and is able to reach the location where developers are saving their code.

**9. The application vulnerability scanner shall provide the ability to integrate the vulnerability data into multiple continuous integration platforms, bug trackers, and integrated development environments (IDEs).**

WhiteHat Security provides plug-ins and integrations for CI servers like Jenkins, bug trackers such as Jira, and ALM tools with WhiteHat Integration Server for both Sentinel Dynamic and Sentinel Source services. This enables support of continuous integration processes, DevOps workflows and application security testing at different stages of the Software Development Lifecycle (SDLC). In addition, Sentinel Source supports commonly-used repositories / Software Configuration Management (SCM) tools, IDEs, as well as dependency management frameworks for Software Composition Analysis (SCA). A WhiteHat API is also available for integration into custom enterprise development and other tools.

**10. The application vulnerability scanner shall have the ability to generate customizable reports of vulnerabilities based on individual applications, and for the organization as a whole.**

Since a significant subset of reporting and dashboard data is available via the WhiteHat Sentinel API, this data can be easily leveraged to produce custom reports/dashboards or integrate WhiteHat data into a much larger security data set for analysis.

**11. The application vulnerability scanner shall provide the ability to schedule the automated assessment of applications.**

All DAST and SAST services are provided by WhiteHat on a scheduled basis. For DAST, testing can be as often as continuous, due to the production safe nature of WhiteHat's scanning and testing methodology. Alternatively, structured test schedules can be configured (such as nightly, weekends only, specific test windows, etc.). For SAST, testing is also scheduled on a regular basis, and frequently as daily. There is no limit to the number of tests conducted for the duration of a licensed service engagement.

**12. The Contractor shall assist VCU in developing hiring and training processes for familiarizing developers with the product with the goal of maximizing product value and utilization.**

WhiteHat will provide training in the proper and efficient use of WhiteHat Sentinel services, including the user portal and any supported integrations. Additionally, WhiteHat is able to assist with determining areas of focus for development teams, in order to maximize value through targeted security training. WhiteHat is able to use client vulnerability and remediation data to better understand possible training needs, and offers both classroom and computer-based training services to improve value and utilization. WhiteHat will also offer vulnerability review sessions to help developers and security organizations better understand findings and results, and WhiteHat security engineers in the Threat Research Center are available 24x7 on an unlimited basis to answer any vulnerability-specific questions that may arise. For optimal utilization, WhiteHat also provides several integration points to keep developers at their normal workbench, and will work with client teams to help users consume WhiteHat data directly into existing systems and solutions.

**E. Preferred Options and Services –The items listed below are not strict requirements for product selection, but are desired by the University, and will be given additional consideration.**

**1. Ability for vendor to offer Runtime Application Security Protection (RASP) option.**

WhtieHat has partnered with Prevoty to provide a combined DAST and RASP solution. With the WhiteHat Sentinel-Prevoty integration, clients have the option of mitigating Sentinel detected vulnerabilities automatically by seamlessly integrating with Prevoty's Application Monitoring and Protection (AMP) solution. This WhiteHat Sentinel-Prevoty integration combines Prevoty's Runtime Application Self Protection (RASP) technology with WhiteHat's market proven Dynamic Application Security Testing (DAST) technology.

**2. Ability for the aforementioned console to provide authentication to developers and security personnel via Jasig CAS single sign-on.**

WhiteHat is configured to provide single sign-on services via SAML 2.0 (Federated).

**3. Ability to organize and group applications based on owners and / or business units.**

WhiteHat Sentinel allows end users to apply tags on all of their assets. Sentinel also supports the ability for customers to create "Asset groups" where they can group assets from both DAST and SAST. Users may then perform searches, lookups, reporting, etc. based on these asset groups. Clients may also grant user access and permissions with specific access based on group or individual application.

**4. Ability to generate customizable reports of vulnerabilities based on application owners and / or business units.**

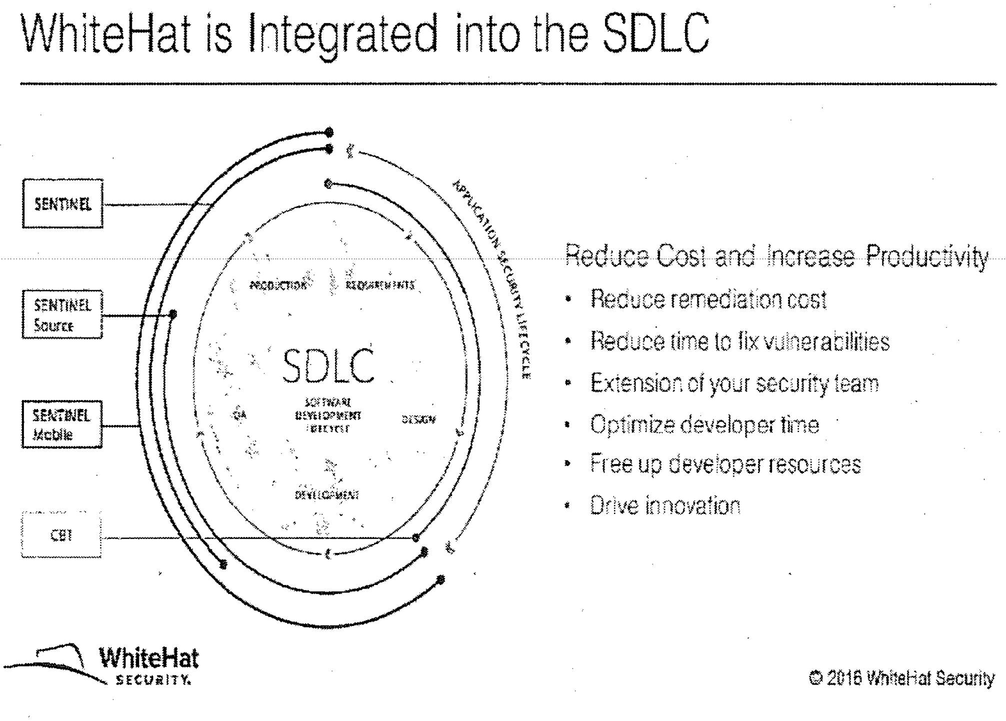
Since a significant subset of reporting and dashboard data is available via the WhiteHat Sentinel API, this data can be easily leveraged to produce custom reports/dashboards or integrate WhiteHat data into a much larger security data set for analysis.

**5. Ability to perform vulnerability assessments on multiple applications simultaneously.**

Sentinel Dynamic is designed to scan websites continuously and detect code changes to web applications automatically. All vulnerabilities are manually verified by the security engineers of our Threat Research Center (TRC), virtually eliminating false positives. Sentinel Dynamic offers true continuous assessment, constantly scanning your website as it evolves. Automatic detection and assessment of code changes to web applications, alerts for newly discovered vulnerabilities and the ability to retest a vulnerability without having to test from the beginning offering "always-on" risk assessment.

### 6. Provision of a full featured Software as a Service solution for both DAST and SAST implementations.

WhiteHat Security's Sentinel Product family enables your organization to implement a secure SDLC by detecting security vulnerabilities in your source code, mobile, and web applications and protecting them with continuous and concurrent assessment methodology to mitigate constantly evolving threats. By combining our scalable application scanning platform with the world's largest security team in our Threat Research Center (TRC), we provide you with actionable, credible results with near zero false positives.



WhiteHat is Integrated into the SDLC

Reduce Cost and Increase Productivity

- Reduce remediation cost
- Reduce time to fix vulnerabilities
- Extension of your security team
- Optimize developer time
- Free up developer resources
- Drive innovation

© 2016 WhiteHat Security

### 7. Ability for vendor to offer an easy to use and intuitive executive dashboard that shows top vulnerable applications, trending data, and risk scores.

The WhiteHat Security Index report assesses the risk of each individual application based on the vulnerabilities WhiteHat has identified for each, as well as comparing to global and industry percentiles. WhiteHat also provides executive dashboards to display application-specific information based on real-time data. These dashboards display trending data, information about the criticality and prevalence of vulnerabilities within the application, and offer insight into the overall health of individual applications from a security perspective. The dashboard reports can also be created for user-defined groups of applications, as well as for the entire portfolio of applications within scope of the engagement.

### 8. Ability for vendor to offer tiered management system that allows individual administration rights by single application administrator, application group administrator, and global administrator.

All Sentinel services include unlimited user access to the Sentinel portal. The level of user access is governed by the assigned Sentinel role and applications the user is granted access. Customer can administer the accounts of all the Sentinel users via Administration area of the Sentinel portal. Access control is based on the concept of least privilege. Administrative users can be provisioned with group- or application-specific access, or can be assigned privileges to administer assets and accounts across the entire portfolio.

### 9. Ability for vendor to provide detailed explanation of the vulnerability including proof of concept exploit code, and suggested remediation based on the original code (i.e. rather than generic examples).

WhiteHat will provide proofs of concept directly within the Sentinel user interface. For static source code testing (SAST), WhiteHat will identify the specific lines of code where the vulnerability exists. In addition to providing remediation guidance for all DAST and SAST vulnerabilities, WhiteHat will also provide exact code fixes for certain SAST vulnerability findings. WhiteHat security engineers in the Threat Research Center are also available 24x7 to assist with proofs of concept, remediation, and other vulnerability-specific requests.

### 10. Ability to attach metadata to applications so that applications can be classified by arbitrary labels and categories.

WhiteHat Sentinel allows end users to apply tags on all of their assets, both the dynamic analysis web applications and the applications being scanned with the Sentinel Source. Sentinel also supports the ability for customers to create "Asset groups" where they can group assets from both DAST and SAST. Users may then perform searches, lookups, reporting, etc. based on these asset groups.

### 11. Ability for vendor to provide prompt technical support via phone, chat, or email to application developers using the platform

A unique capability of WhiteHat is its function as an extension of clients' security teams. This is most clearly seen in the ability to interact directly with WhiteHat security engineers at any time. This can be done over the phone, through email, or most readily through the Sentinel interface itself via the "Ask a question" component. This functionality allows any Sentinel user to ask detailed questions about specific vulnerability data ranging from proof of concepts, remediation guidance, steps to reproduce, to discussions about business impact. WhiteHat is also more than willing to demonstrate vulnerabilities live over WebEx or in some cases in person.

### 12. Ability for the application vulnerability scanner to provide workflow automation that enables the automated notification of vulnerabilities and changes in risk posture.

All vulnerabilities are reported to the Sentinel user interface the moment they are verified by a security engineer. These vulnerabilities are then displayed in real time within the UI where you may run reports or set up automated email alerts. The automated alerts can be set up to occur in real time, daily, weekly, or monthly.

## VCU Specific Proposal Requirements

### 2.Proposed Price. Describe in detail the proposed license model for the application vulnerability scanner. Indicate in the Pricing Schedule, Section VIII of the RFP the proposed price to include all costs associated with the license(s), any hardware or appliances, implementation, hosting, maintenance, and training to include all proposed products and services. Additional charges shall not be allowed.

***Pricing Assumptions: 247 Web Applications | DAST Pricing Weighted Average: 15% PE, 50% SE, 35% BE**

| VCU Proposed Solution | Product Code / Description | License Count | List Price / App | Volume Discount | Company Price |
|---|---|---|---|---|---|
| Sentinel Premium Edition | PE | 37 | $20,000.00 | 75% | $185,000.00 |
| Sentinel Standard Edition | SE | 123 | $10,000.00 | 75% | $307,500.00 |
| Sentinel Baseline Edition | BE | 86 | $4,000.00 | 80% | $68,800.00 |
| Sentinel Source Xsmall <100K LoC | <4 MB | 64 | $4,500.00 | 30% | $201,600.00 |

| | | | | | |
|---|---|---|---|---|---|
| Sentinel Source Small <250K LoC | <10 MB | 65 | $6,500.00 | 31% | $291,525.00 |
| Sentinel Source Medium <500K LoC | <20 MB | 26 | $12,000.00 | 33% | $209,040.00 |
| Sentinel Source Large <1.5M LoC | <60 MB | 2 | $26,000.00 | 27% | $37,960.00 |
| Sentinel Source Xlarge <3M LoC | <120 MB | 1 | $46,500.00 | 27% | $33,945.00 |
| Sentinel Source XXLarge <5M LoC | <200 MB | 2 | $77,000.00 | 27% | $112,420.00 |
| Sentinel Source Jumbo >5M LoC | >200 MB | 1 | $85,000.00 | 27% | $62,050.00 |
| Platinum Support | | 1 | $150,000.00 | 60% | $60,000.00 |
| **Total** | | | | | **$1,569,840.00** |

**3. Describe the proposed plans and approach for providing the products and services as specified in the RFP. Consider the technical requirements in Section VI, Statement of Needs, Items A through E in the context of implementation and ongoing support, costs of upgrade and replacement, implementation timeline expectations, and costs of warranty and maintenance. Specifically indicate what is included in the offer to provide the required products and services by responding to all Items in Section VI, Statement of Needs, Items A through F. In addition, provide information for the Items listed below, but do not limit information to these Items:**

One of the greatest luxuries that WhiteHat Security offers us as employees is the ability to truly help companies become more secure. Over the years, we've taken our scalable SaaS model and greatly improved it, constantly refining due to the changing needs of both the security world as well as well as the security policy of the enterprises we work with.

The following is a good example of the experiences commonly shared by large enterprises that leverage WhiteHat:

1. Onboarding Phase – The on-boarding process is a critical juncture to establishing your trust and this process is where the end user gets to meet the support team. WhiteHat's Deployment Engineers are technical professionals with experience in the security industry, who review any open cases during the deployment phase and facilitate quick resolutions to ensure a seamless on-boarding experience. They provide end users with all the details needed to get the Sentinel service up and running. The information that is needed from the end user includes but is not limited to:

    a. Application URLs
    b. Credentials
    c. Assessment Schedule

d. Mock Data
e. Primary contacts / users
f. Special testing instructions
g. etc.

We typically start with either a WebEx or an onsite visit where we also discuss the Sentinel service and answer any questions the users may have.

2. Initial Assessment Phase – This is the initial two weeks after we've obtained the necessary assessment information. This is where all the applications that were set up are fully assessed, configured, and tested based on service line for vulnerabilities.

3. Results Overview Phase – After the initial assessment, we strongly encourage the end user to take some time and meet with us to discuss the vulnerabilities discovered. During this time, we will either present over WebEx or onsite, the issues that were found - often demonstrating them live at the request of the end user. We will go through what they are, how they were discovered, how they might impact the business, and answer any questions you may have about them.

4. Ongoing Maintenance Phase – After the initial assessments have been completed on the applications, the WhiteHat Security Threat Research Center (TRC) will constantly monitor the web applications as they are assessed based on the customer set schedule. Any changes to the application will be detected automatically, configured, assessed, verified, and reported to the Sentinel UI proactively. If anything is required by the end user, we will reach out to them and let them know exactly what is needed to ensure a thorough assessment. For example, if credentials are locked out or an associated hostname is needed.

5. Measuring Success Phase – This typically comes after several months of being under the WhiteHat service and often consists of measuring the success of the security program. We will work with the end users to provide metrics and trending of the overall data accumulated throughout the assessments. Example of this data include:

   a. Remediation Percentage
   b. Time to Fix issues
   c. Most common vulnerabilities
   d. Window of exposure
   e. WhiteHat Security Index (WSI) – WSI is a measure of a site's security posture, calculated from a comprehensive set of data signals including number of vulnerabilities, remediation rate, time-to-fix, window of exposure and many more.

This data can then be compared to the industry averages across each of the major verticals. This begins the foundation of being able to answer questions like:

1. Are we getting better?
2. How do we compare to other people within the Entertainment industry?
3. What is our most common issue?
4. How long does it take to fix a critical issue?

Throughout all of the phases, we maintain a strong information loop with our customers and greatly appreciate any feedback to continue the improvement of the Sentinel service.

**3.a. Utilization of the words "shall" or "must" in Section VI, Statement of Needs, Items A through E indicates mandatory technical requirements: Does / Shall your company comply with the mandatory technical requirements as presented in Section IV, Statement of Needs, Items A through E?**

Yes.

**3.b. The vendor will provide a full list of supported programming languages and frameworks for the SAST product. See Section VI.D.5.**

For static analysis service components, detail which programming languages your SAST offering can analyze (include scripting languages).

Our SAST offering can analyze a number of languages commonly used in the creation of web applications, including Java, JavaScript, ASP.NET, PHP and C#, the primary language used in the .NET framework. Mobile languages support includes Objective-C (iOS) and Android (Java).

**For each language, please answer which specific versions are supported —for example, older versions of .NET, older versions of Visual Basic and so on.**

Java 1.1, 1.2, 1.3, 1.4, 5.0, SE 6 and SE 7 are supported. New language features included in Java SE 8 is currently under analysis.

.NET 1.0, 1.1, 2.0, 3.0, 3.5, 4.0 and 4.5 are supported.

PHP 5.0, 5.1, 5.2, 5.3, 5.4 and 5.5 are supported.

Java (includes Android) 1.4 – 1.8

C#.NET 2.x-4.x

PHP 5.x, 7.x

Objective-C (includes iOS) 1.x - 2.x

| | |
|---|---|
| Javascript (includes Javascript APIs in HTML5) | 5, 5.1, 6 |

**For each language, please highlight specific application programming interfaces (APIs), frameworks and library constructs that you support as standard (for example, Struts and Spring MVC for Java).**

WhiteHat Sentinel Source supports a large number of frameworks for supported languages including the following.

Java:
- Java Core
- Java Enterprise
- Spring MVC
- Spring ORM
- Spring JDBC
- Jasper (Includes JSP support)
- Struts 1.x
- Struts 2.x
- Hibernate
- Jax-RS
- RestExpress
- MongoDB
- Morphia
- GSON
- Apache Axis
- Bouncy Castle
- Apache Commons HttpClient
- Apache Commons Lang
- Jax-WS
- Jersey
- Android
- Apache Commons IO
- Apache Common Net
- Apache Commons FileUpload/CSV/DBCP

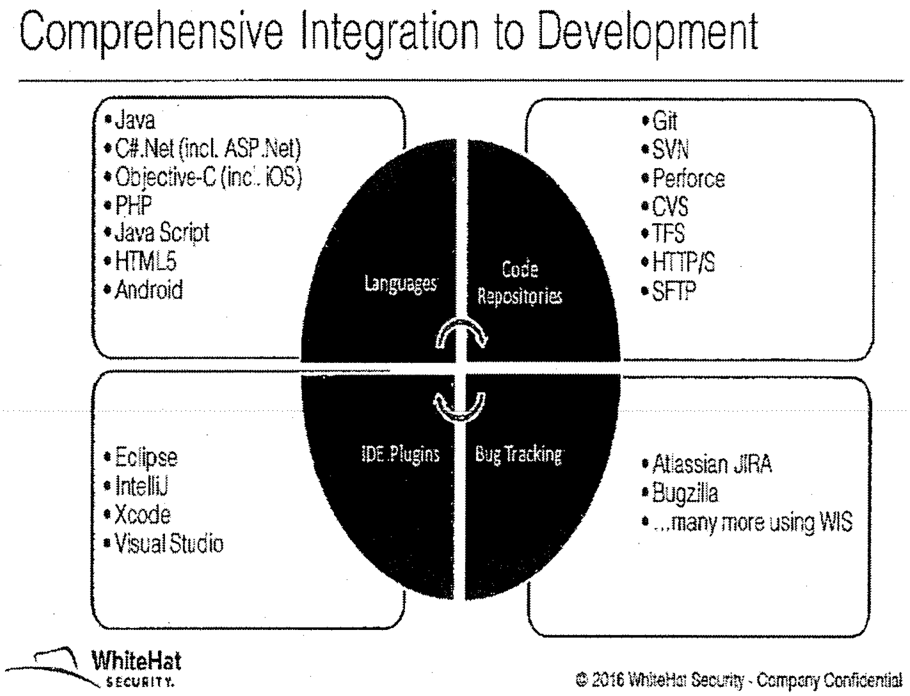
.NET:
- C# Core
- AspNet WebForms
- AspNet Core
- AspNet MVC
- MySql

PHP:
- Zend
- CodeIgnitor
- Yii
- Symfony

Please note that each of these frameworks are not only supported but "rule packs" have been created to customize Sentinel to check for specific framework issues as well as ensure that Sentinel is capable of understanding and analyzing each unique nuance between each framework. These rule packs are created and maintained on a regular basis and any new updates are seamlessly pushed to the Sentinel Source scanner.

WhiteHat continues to write new rule packs for libraries that gain popularity. Customers can purchase WhiteHat professional services to create additional rule packs specific to the libraries that they use.

**3.c. Provide a full list of supported continuous integration platforms, bug trackers, and IDEs. See Section VI.D.9.**



Comprehensive Integration to Development

Languages
- Java
- C#.Net (incl. ASP.Net)
- Objective-C (incl. iOS)
- PHP
- Java Script
- HTML5
- Android

Code Repositories
- Git
- SVN
- Perforce
- CVS
- TFS
- HTTP/S
- SFTP

IDE Plugins
- Eclipse
- IntelliJ
- Xcode
- Visual Studio

Bug Tracking
- Atlassian JIRA
- Bugzilla
- ...many more using WIS

WhiteHat SECURITY.

© 2016 WhiteHat Security - Company Confidential

**3.d. Describe in detail the proposed hiring and training processes. See Section VI.D.12.**

The WhiteHat Threat Research Center University is a completely in-house, custom built training and assessment program that allows WhiteHat to quickly and efficiently train expert security engineers. Utilizing 15 years of real world attack techniques and vulnerabilities, WhiteHat has implemented rigorous training programs and skill assessments to ensure quality, qualified engineers. The program is broken into training modules that consist of both classroom, and hands on real world lab work. This ensures engineers get up to speed much quicker than anyone utilizing dummy practice sites can.

**3.e. Describe in detail the proposed maintenance and support. See Section VI.B.**

Maintenance is not applicable to the WhiteHat Sentinel service, as we are a SaaS based company.

**3.f. Describe in detail the optional on-site training that your company is proposing.**

WhiteHat Security will provide a senior security engineer to spend three days onsite at your facility to help your team develop and execute strategic website risk management plans tailored to your specific business environment. During an annual review, for example, strategies can be developed that enable different business stakeholders – including risk management and compliance, product management and software development teams – to share ideas with WhiteHat experts and strategize on best practices for web security.

**3.g. Submit a copy of the warranty. State the start of the warranty period and the end of the warranty period.**

See above for warranty details. Warranty period is same as contract period.

**3.h. Provide an implementation schedule indicating how long after the award of the contract it shall take your company to allocate the resources and deliver and install the system for use at VCU.**

Implementation is not applicable to the WhiteHat Sentinel Service, as we are a SaaS based company.

**3.i. Describe the process for problem resolution for the proposed products and services.**

WhiteHat provides its clients with several ways of getting support on its products. For questions on vulnerabilities, it is recommended to use the "Ask a Question" feature available within the Sentinel interface. For all other issues, or if another method of contact is preferred, a client may contact support via phone, email, or by accessing the support portal.

### 3.j. Does your company agree with the Procurement Requirements in Section VI.F.? If "NO," identify the specific term and condition(s) and the reason for non-compliance.

(1) Freight terms shall be F.O.B. Destination/Prepaid with inside delivery; additional charges shall not be allowed. (2) The terms and conditions of the RFP govern the resulting contract and not any Contractor terms and conditions or software license agreement. (3) The proposal prices shall include all costs for the equipment and services including all applicable freight and travel and living expenses; extra charges will not be allowed. (4) The initial contract term is from the award and continues for one (1) year after the implementation is complete and the system is accepted with four (4) annual, optional renewal terms.

## 4. Submit information about the qualifications and experience that your company has to provide the Application Vulnerability Scanner products and services.

### a. Describe the firm's qualifications and experience providing the required products and services during the last three (3) years. Information provided should include, but is not limited to, comparable accounts in higher education and the scope of the services. Include information for a minimum of three (3) similar accounts, describing the types of projects and the scope of the services provided. Please include contact information with the name, address, email address and current phone number.

WhiteHat Security was founded in October 2001 and has been operating for 15 years.

**June 2016** - WhiteHat published its eleventh annual Website Security Statistics Report in May. This report provides a one-of-a-kind perspective on the state of website security and the issues that organizations must address in order to conduct business online safely. It is also the only report that focuses exclusively on unknown vulnerabilities in custom web applications, code that is unique to an organization, and found in real-world websites.

**Mid-2015** - WhiteHat introduced the WhiteHat Security Index (WSI), a new feature in WhiteHat Sentinel that provides an immediate way for customers to understand how secure – or not – their websites are. It's the only report of its kind in the industry. An additional Peer Benchmarking dashboard enables users to determine the security of their web sites compared to industry peers.

WhiteHat Sentinel Source, WhiteHat's SAST solution, expanded its capabilities with Directed Remediation and Software Composition Analysis (SCA). The Directed Remediation capability offers targeted and customized code fixes for critical vulnerabilities, while the new SCA capability enables users to detect and remediate any vulnerabilities that are already known to exist in third-party libraries and open source code.

**August 2015** – WhiteHat announced the strategic partnership with Prevoty with product level integration that enables automatic mitigation of applications vulnerabilities via Prevoty's Runtime Application Self Protection (RASP) technology.

**August 2015-** WhiteHat Security was named a leader in the Gartner's Application Security Testing Magic Quadrant for the third year in a row.

**Late 2014** - WhiteHat expanded its Threat Research Center (TRC) team to over 150 security experts total. In late 2014, the company established a research center in Belfast, Northern Ireland, and that team grew to over 50 security engineers by the end of 2015.

**August 2014** – WhiteHat Security was named a leader in the Gartner's Application Security Testing Magic Quadrant for the second year in a row.

**b. Specify the proposed personnel your company intends to assign to the project and provide proof of the expertise for the proposed system. Information needed includes but is not limited to the names, qualifications, and experience of professional IT services technicians to be assigned to the project. Resumes of staff to be assigned to the project may be used.**

See attached Resume. Assumes Platinum Support is selected as part of overall solution.

**c. Does the offer include a single primary point of contact for the VASCUPP institutions for sales, support and problem resolution? If so, please provide the name and contact information.**

Christopher Perkins

Regional Sales Director

1.571.481.0895

chris.perkins@whitehatsec.com

**d. Information demonstrating the Contractor's financial stability to include:**

**1. Full name, address, and telephone number of the organization;**

WhiteHat Security, Inc. | 3970 Freedom Circle, Ste 200, Santa Clara, CA 95054 |
408.343.8300

**2. Date the firm was established;**

2001

**3. Ownership (e.g. public company, partnership, subsidiary, etc.**

Private

**4. If incorporated, provide the state of incorporation**

Delaware

**5. Number of full-time employees on January 1st for the last three (3) years or for the duration the firm has been in business, whichever is less**

300

**e. Provide a list of institutions of higher education with which the firm has a signed term contract.**

12Twenty.com, American University, Apex Learning, Inc., California State University (CSU), Colby College, College Board, CSU Chico, Degreed, Hamdan Bin Mohammed Smart University, Harvard University, iPay Technologies, LLC, NCS Pearson, Inc. (Pearson Assessment and Information), PowerSchool Group, San Jose State University, SAS Institute, Inc. StudySync, The Lampo Group, The Regents of the University of California (UCLA IT Services), Udemy, Inc., University of Indianapolis

**Section XI.L. TESTING AND INSPECTION: VCU reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.**

Rather than a testing and acceptance period, WhiteHat offers a pre-contract evaluation.

**Section XII.F. CANCELLATION OF CONTRACT: The purchasing agency reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon sixty (60) days written notice to the Contractor. In the event the initial contract period is for more than twelve (12) months, the resulting contract may be terminated by either party, without penalty, after the initial twelve (12) months of the contract period upon 60 days' written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.**

Rather than a cancellation right, WhiteHat offers an opt-out of the contract within the first 30 days.

**Section XIII.B. (Source Code Escrow)**

Because WhiteHat offers a hosted solution, no source code escrow will be offered.

**Section XIII.H. (Nonvisual Access to Technology)**

WhiteHat does not offer this at this time.

**Describe any other relevant background information about your organization and your qualification to provide the request product/service.**

Key relevant background information includes:

- WhiteHat Security was first in the industry to deliver a Software as a Service (SaaS) solution for Dynamic Application Security Testing (DAST).
- We have the world's largest army of application security engineers in our Threat Research Center (TRC) of over 150 and growing. These security engineers act as an extension of your security team, by
- always being available to help you with any questions or concerns you may have in regards to the application security vulnerabilities.
- Performs approximately 300,000 assessments per month.
- Surpassed 40,000 websites under management by WhiteHat Sentinel in August 2016
- WhiteHat Security operates 24x7x365

**Describe your after-sales support SLAs.**

All WhiteHat customers receive one-hour SLA response to Sentinel outages. Other support SLA levels vary by contract level and topic, not to exceed one business day for low severity issues reported by Standard support customers. All support issues are handled with a four-hour SLA for Premium Gold support customers, and one-hour SLA for our Platinum support customers. This SLA is matched with round-the-clock staffing and a paging notification system to an on-call senior engineer who can assist with any customer emergencies.

**Describe your approach for investing in technology and research and development to increase operational efficiency while keeping up with the rapidly changing threat environment. What are the highest priority initiatives in your company that affect the requested services? What is your company's vision and direction for currently offered services as well as plans for additional services and support of new technologies? Describe your responsiveness, ability and timeliness to steer product roadmaps based on customer requirements.**

From a development perspective:

WhiteHat Security has a well-defined process and investment in modern tools and technologies to capture customer feedback and feature requests, prioritize in terms of business need and time criticality and track them to delivery through Agile development processes. Agile software development is by definition introspective and takes into account both business needs and development efficiency initiatives as part of each cycle. In addition to regular release cycles (currently every 3 weeks), we have a well-defined schedule for service packs (weekly) and production hot fixes (as needed) to address customer needs.

WhiteHat Sentinel and Source are primary products for WhiteHat with an active roadmap that includes extending our current capabilities to include:

- Site discovery
- Asset management
- Risk management
- Predictive analytics
- Additional Sentinel Source language engines and rule packs based on customer needs

Our rapid iterative software development lifecycle is targeted to enhance and enrich our best-of-class product suite so that customers can get the most comprehensive view of their risks and make intelligent decisions about their security.

We engage in regular customer meetings and reviews, as well as hosting Customer Advisory Board meetings and attending industry conferences to maintain a current view of competitive landscape and customer needs.

From the Threat Research Center:

WhiteHat's Threat Research Center operates with the goal of finding every type of vulnerability, every time, as efficiently as possible. To that end, WhiteHat has developed

Sentinel itself to be much more than an automated scanner. It is a platform that enables a huge variety of tests to be performed. The Engineering team works on the core features of Sentinel, but a separate R&D team within the TRC focuses specifically on creating tests, which are organized into decision trees. Every test has its own custom conditions, and tests can rely on each other as well. All of this flexibility allows the R&D team to create incredibly efficient tests. Over time, we have become much more efficient while simultaneously finding many more type of vulnerabilities. The end result is a scalable solution that is more efficient every day, even as attacks become more complex.

**Is your current business (including your channel (reseller) partnerships) regional, national, or international? Describe your approach and your capabilities to provide global support, including, but not limited to, worldwide locations, expertise in international languages, knowledge of national and local laws that affect requested services, and relationships with national and local law enforcement agencies.**

WhiteHat Security is currently international. We currently have offices in Santa Clara California, Houston Texas, and Dublin Ireland with plans of expansion into Germany from both a datacenter and Threat Research Center perspective. We are able to perform assessment on all modern languages and support localization and language support in the product and services (both written and spoken) in English, Japanese, and Spanish. Other languages are planned to be rolled out in 2014.

**Please note that we request that VCU contact WhiteHat prior to personally reaching out to the references outlined below. Thank you.**

Company Name: American University

Contact Title: Director, Information Security

Contact Name: Eric Weakland, CISSP, CISM, CRISC, ITIL

Phone: 202.885.2241

Email: eric@american.edu

Type of Service: DAST

Date of Service: 2009

Company Name: UCLA

Contact Title: Director Information Security

Contact Name: Mike Story

Phone: Upon Request

Email: Upon Request

Type of Service: Upon Request

Date of Service: Upon Request

Company Name: MAXIMUS

Contact Title: CISO

Contact Name: Ed Pagett

Phone: 949.533.0461

Email: edpagett@maximus.com

Type of Service: DAST

Date of Service: 2016

**Request for Proposals RFP #7286528JC**

**Issue Date:** November 29, 2016

**Title:** Application Vulnerability Scanner

**Send all Proposals To:**

Virginia Commonwealth University
RFP #7286528JC
Attention: Jackie Colbert
912 W Grace St, 5th floor
Richmond, Virginia 23284

**Proposals Shall Be Received Until: January 6, 2017 at 11:00 AM**

**Direct ALL inquiries concerning this RFP to:** **Jackie Colbert, Information Technology Category Manager**
**jcolbert@vcu.edu**

**Questions concerning this RFP must be received via email no later than: December 8, 2016 at 2:00 PM EST**

This Request for Proposals & any Addenda are posted on the eVA website at: http://www.eva.virginia.gov

HARD-COPY, ORIGINAL PROPOSALS MUST BE RECEIVED IN VIRGINIA COMMONWEALTH UNIVERSITY'S DEPARTMENT OF PROCUREMENT SERVICES ON OR BEFORE THE DATE AND TIME DESIGNATED ON THIS SOLICITATION. ELECTRONIC SUBMISSIONS AND FACSIMILE SUBMISSIONS WILL NOT BE ACCEPTED IN LIEU OF THE HARD-COPY, ORIGINAL PROPOSAL. VENDORS ARE RESPONSIBLE FOR THE DELIVERY OF THEIR PROPOSAL. PROPOSALS RECEIVED AFTER THE OFFICIAL DATE AND TIME WILL BE REJECTED. THE OFFICIAL DATE AND TIME USED IN RECEIPT OF RESPONSES IS THAT TIME ON THE CLOCK OR AUTOMATIC TIME STAMP IN THE DEPARTMENT OF PROCUREMENT SERVICES.

**IF PROPOSALS ARE HAND DELIVERED OR SENT BY FEDEX, UPS, OR ANY OTHER PRIVATE COURIER, DELIVER TO THE ADDRESS NOTED ABOVE: VIRGINIA COMMONWEALTH UNIVERSITY, RFP #7286528JC, ATTENTION: Jackie Colbert, 912 W. GRACE ST., 5TH FLOOR, RICHMOND, VA 23298-0327.** IF USING US MAIL (NOT RECOMMENDED): IF PROPOSALS ARE MAILED VIA US MAIL ONLY, MAIL TO VIRGINIA COMMONWEALTH UNIVERSITY, RFP#7286528JC, ATTN: Jackie Colbert, PO BOX 980327, RICHMOND, VA 23298-0327. THE RFP NUMBER, DATE AND TIME OF PROPOSAL SUBMISSION DEADLINE, AS REFLECTED ABOVE, MUST CLEARLY APPEAR ON THE FACE OF THE RETURNED PROPOSAL PACKAGE.

In Compliance With This Request for Proposals And To All Conditions Imposed Therein and Hereby Incorporated By Reference, The Undersigned Offers And Agrees To Furnish The Goods/Services Described Herein In Accordance With The Attached Signed Proposal Or As Mutually Agreed Upon By Subsequent Negotiation. Furthermore, The Undersigned Agrees Not To Start Any Work Relative To This Particular Solicitation Until A Resulting Formal Signed Purchase Order Is Received By The Contractor From University's Department of Procurement Services. Any Work Relative To This Request for Proposals Performed By The Contractor Prior To Receiving A Formal Signed Purchase Order Shall Be At The Contractor's Own Risk And Shall Not Be Subject To Reimbursement By The University.
**Signature below constitutes acknowledgement of all information contained through links referenced herein.**

**NAME AND ADDRESS OF** COMPANY:

| | |
|---|---|
| WhiteHat Security, Inc | Date: January 5, 2017 |
| 3970 Freedom Circle, Suite 200 | By *(Signature In Ink)*: |
| Santa Clara, CA Zip Code 95054 | Name Typed: Terry Murphy |
| E-Mail Address: SalesOps@whitehatsec.com | Title: CFO |
| Telephone: ( 408 )343-8300<br>**Toll free, if available** | Fax Number: ( 408 ) 904-7142<br>**Toll free, if available** |
| DUNS NO.: 129-28-0793 | FEI/FIN NO.: 99-0358892 |

| | | | |
|---|---|---|---|
| REGISTERED WITH eVA: | ( ) YES (X) NO | SMALL BUSINESS: | ( ) YES (X) NO |
| VIRGINIA DSBSD CERTIFIED: | ( ) YES (X) NO | MINORITY-OWNED: | ( ) YES (X) NO |
| DSBSD CERTIFICATION #: | ______________ | WOMEN-OWNED: | ( ) YES (X ) NO |

**A Pre-Proposal conference will be held. See Section V herein.**

**THIS SOLICITATION CONTAINS 31 PAGES.**

VIRGINIA COMMONWEALTH UNIVERSITY

# RFP - Addendum

DATE: December 16, 2016

ADDENDUM NO. 01 TO ALL OFFERORS:

Reference - Request for Proposals: RFP #7286528JC

| | |
|---|---|
| Commodity/Title: | Application Vulnerability Scanner |
| Issue Date: | November 29, 2016 |
| Proposal Due: | January 6, 2017 at 11:00 AM |

The above is hereby changed to read: **See Attached.**

NOTE: A signed acknowledgment of this addendum must be received by this office either prior to the proposal due date and hour or attached to your proposal. Signature of this addendum does not constitute your signature on the original proposal document. The original proposal document must also be signed.

Very truly yours,
Jackie Colbert

Jackie Colbert
Procurement Services
Category Manager and Contracting Officer

WhiteHat Security
Name of Firm

, CFO
Signature/Title

1/5/17
Date

# Sentinel User Guide

## Reporting in Sentinel

November 2016

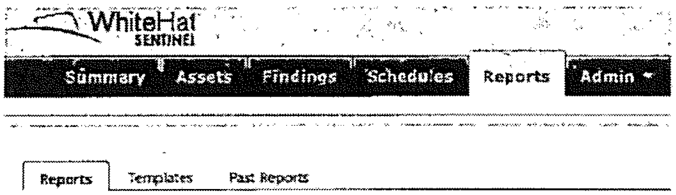
*Current Documentation is available via the Customer Portal at https://whitehatsec.secure.force.com/apex/DocumentDownload.*

# Table of Contents

# Reports in Sentinel

Sentinel offers a variety of reports, from the high-level Executive Summary to the Vulnerability or Attack Vector Details reports. All these reports are available under the Reports tab.

Under the main Reports tab, there are three sub-tabs available: "Reports," "Templates," and "Past Reports."



- The Reports subtab includes
  - report descriptions
  - sample reports
  - links to generate new reports
- The Templates subtab includes
  - Any already-created report templates the user can run
  - Template name, report type, report format, and report frequency
  - Next scheduled run time for the reports
  - Available actions, including editing the template or generating the report immediately
- The Past Reports subtab includes
  - pending reports (which can be canceled)
  - reports generated in the past thirty (30) days (which can be downloaded by clicking on the "View" link)
  - any reporting errors (clicking on "error details" under the "Actions" column will bring up the details)

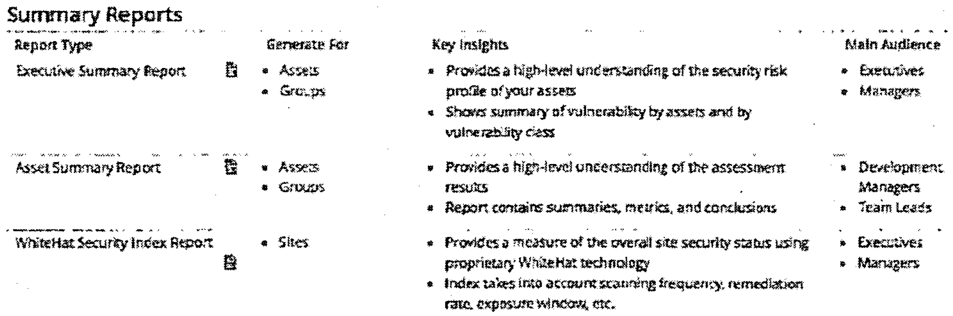
For further information on available report types, please see Sentinel Reports. For information on creating report templates, please see "Creating Report Templates."

## Sentinel Reports

Sentinel reports are divided into four broad types:

- Summary Reports, intended primarily for executives and managers
- Audit and Compliance reports, intended primarily for customer affiliates, executives, and managers
- Vulnerability Detail Reports, intended primarily for security teams and developers
- Sentinel Management Reports, intended primarily for security teams and Sentinel administrators

## Summary Reports

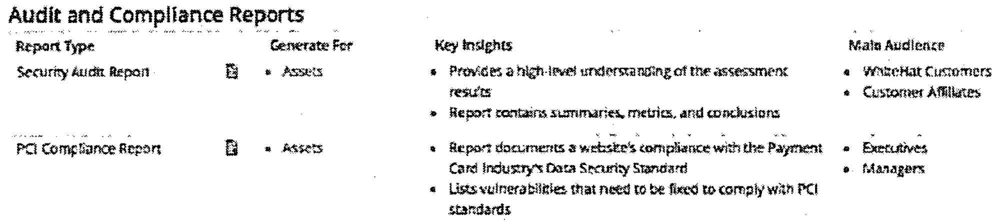


### Summary Reports

| Report Type | Generate For | Key Insights | Main Audience |
|---|---|---|---|
| Executive Summary Report | • Assets<br>• Groups | • Provides a high-level understanding of the security risk profile of your assets<br>• Shows summary of vulnerability by assets and by vulnerability class | • Executives<br>• Managers |
| Asset Summary Report | • Assets<br>• Groups | • Provides a high-level understanding of the assessment results<br>• Report contains summaries, metrics, and conclusions | • Development Managers<br>• Team Leads |
| WhiteHat Security Index Report | • Sites | • Provides a measure of the overall site security status using proprietary WhiteHat technology<br>• Index takes into account scanning frequency, remediation rate, exposure window, etc. | • Executives<br>• Managers |

| Report Name | Description | Utility |
|---|---|---|
| Executive Summary Report: | The Executive Summary report provides a high-level understanding of the security profile of your assets, giving you an overview of vulnerabilities across all the assets you select. This report shows you a summary of vulnerabilities by assets and by vulnerability class, as well as showing your overall security profile. For those customers using both Sentinel and Sentinel Source, this report will cover both dynamic and static test results. | High-level general overview<br>Executive/ C-level review |
| Asset Summary Report: | The Asset Summary report provides a high level understanding of your vulnerability assessment results, including summaries, metrics, and conclusions. Assets without any vulnerability are omitted from this report. For those customers using both Sentinel and Sentinel Source, this report will cover both dynamic and static test results. | Asset-specific overview<br>CSO, CTO, and/ or Security Operations |
| WhiteHat Security Index Report | The Security Index Report provides a measure of the overall site security status, taking into account scanning frequency, remediation rate, exposure window, etc. | Asset-specific status report<br>Executive Staff, managers, CSO, CTO, Security Operations |

## Audit and Compliance Reports

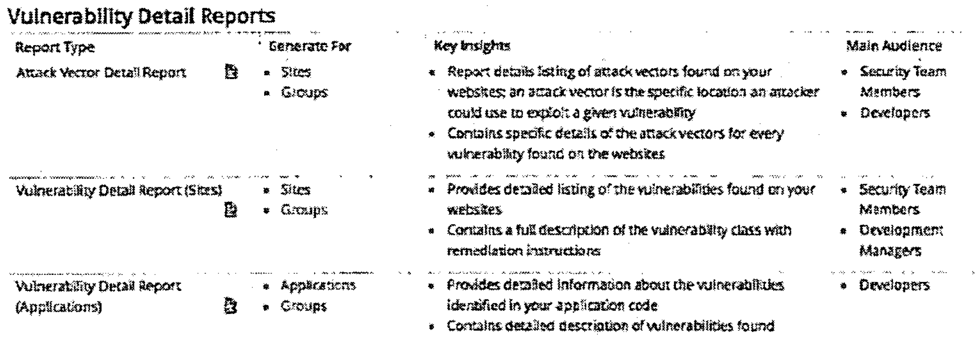


### Audit and Compliance Reports

| Report Type | Generate For | Key Insights | Main Audience |
|---|---|---|---|
| Security Audit Report | Assets | Provides a high-level understanding of the assessment results<br>Report contains summaries, metrics, and conclusions | WhiteHat Customers<br>Customer Affiliates |
| PCI Compliance Report | Assets | Report documents a website's compliance with the Payment Card Industry's Data Security Standard<br>Lists vulnerabilities that need to be fixed to comply with PCI standards | Executives<br>Managers |

| Report Name | Description | Utility |
|---|---|---|
| Security Audit Report: | The Security Audit report provides an overview of open vulnerabilities discovered in the assessment, including summaries, metrics, and conclusions. For those customers using both Sentinel and Sentinel Source, this report will cover both dynamic and static test results. | Executive staff, auditors, and personnel preparing for an audit |
| PCI Compliance Report: | The Sentinel PCI Compliance report documents a website's compliance with the Payment Card Industry's Data Security Standard (PCI-DSS), which includes requirements that web applications be built to secure coding guidelines and that applications be subject to routine vulnerability checks.<br>This report documents compliance with PCI DSS 3.0 Requirements 6.5.1 - 6.5.11. | Executive staff, auditors, and personnel preparing for an audit |

## Vulnerability Detail Reports

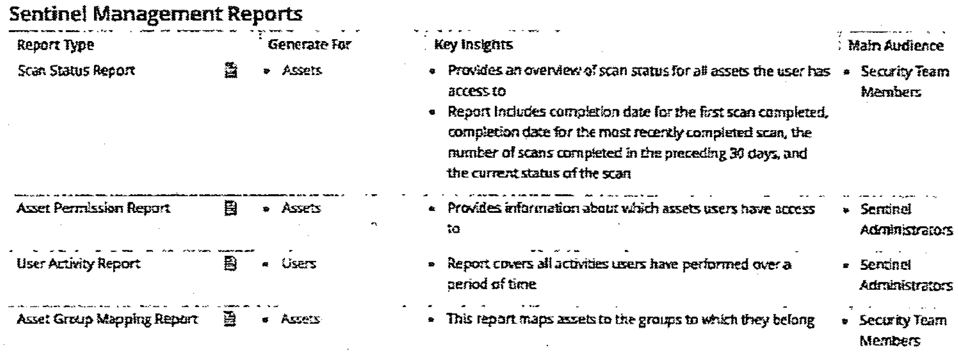


### Vulnerability Detail Reports

| Report Type | Generate For | Key Insights | Main Audience |
|---|---|---|---|
| Attack Vector Detail Report | Sites<br>Groups | Report details listing of attack vectors found on your websites; an attack vector is the specific location an attacker could use to exploit a given vulnerability<br>Contains specific details of the attack vectors for every vulnerability found on the websites | Security Team Members<br>Developers |
| Vulnerability Detail Report (Sites) | Sites<br>Groups | Provides detailed listing of the vulnerabilities found on your websites<br>Contains a full description of the vulnerability class with remediation instructions | Security Team Members<br>Development Managers |
| Vulnerability Detail Report (Applications) | Applications<br>Groups | Provides detailed information about the vulnerabilities identified in your application code<br>Contains detailed description of vulnerabilities found | Developers |

| Report Name | Description | Utility |
|---|---|---|
| Attack Vector Details Report: | The Attack Vector Details report provides of attack vectors found on your websites; an attack vector is the specific location an attacker could use to exploit a given vulnerability found on your sites. In addition to the location and time the vulnerability was discovered, the attack vector details include a breakdown of the exact request and response so that developers can easily address the problem. Note that this report is available for Sentinel (dynamic testing) only, since it is based on an assessment of the production or pre-production site. | Detailed review of specific attack vectors<br>Development and/ or Security Operations |
| Vulnerability Details Report - Sites: | The Vulnerability Detail Report -- Sites provides detailed descriptions of the vulnerabilities found on the sites selected for this report, grouped by vulnerability class. Each report section contains a full description of the vulnerability class, remediation instructions for that class, and a list of specific instances of that vulnerability on each site. Note that this report is available for Sentinel (dynamic testing) only, since it is based on an assessment of the production or pre-production site. | Detailed review of vulnerabilities<br>Development and/ or Security Operations |
| Vulnerability Details Report - Applications: | The Vulnerability Detail Report -- Applications includes detailed description of the vulnerabilities found in each application selected for this report, grouped by category, and includes for reference the code snippets associated with the vulnerabilities. Note that this report is available for Sentinel Source (static testing) only, since it is based on an assessment of the application code. | Detailed review of vulnerabilities<br>Development and/ or Security Operations |

## Sentinel Management Reports



**Sentinel Management Reports**

| Report Type | | Generate For | Key Insights | Main Audience |
|---|---|---|---|---|
| Scan Status Report | 🗎 | • Assets | • Provides an overview of scan status for all assets the user has access to<br>• Report Includes completion date for the first scan completed, completion date for the most recently completed scan, the number of scans completed in the preceding 30 days, and the current status of the scan | • Security Team Members |
| Asset Permission Report | 🗎 | • Assets | • Provides information about which assets users have access to | • Sentinel Administrators |
| User Activity Report | 🗎 | • Users | • Report covers all activities users have performed over a period of time | • Sentinel Administrators |
| Asset Group Mapping Report | 🗎 | • Assets | • This report maps assets to the groups to which they belong | • Security Team Members |

| Report Name | Description | Utility |
|---|---|---|
| Scan Status Report: | The Scan Status Report will generate a .csv report of assets, service levels, asset types, and information about the asset's history and current scan status. | Detailed review of scan state, processes, and history<br>Security Operations |
| Asset Permission Report | The Asset Permissions report will generate a .csv report of assets and the users who have some level of permission to access those sites. | Detailed review of assets and user accesses<br>Security Operations |
| Asset Group Mapping Report | The Asset Group Mapping report will generate a .csv report of assets mapped to the groups to which they belong. | Detailed review of assets and asset groups<br>Security Operations |

You can see a sample of each report from the main Reporting tab; just click on "View Sample" under Actions.

Each report allows you to select specific information you would like to include in or exclude from the report you are generating, such as:

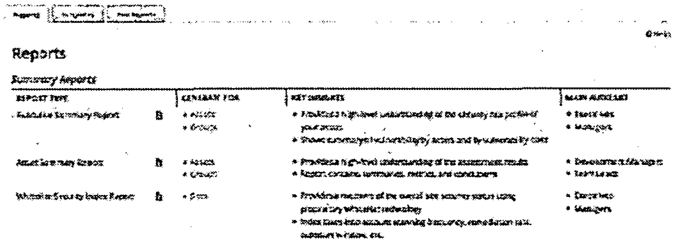
- Assets (Sites or Applications)
- Vulnerabilities (where applicable)
- Status (Open, Closed, or All)

- Date Range
- Details (e.g. Attack Vector, CVSS scores) to include or exdude

# Creating Reports and Templates

You can set up any report to be generated (and an e-mail alert sent to you on completion) using the preferences and schedule you need. Here are the steps to create and schedule a report template.

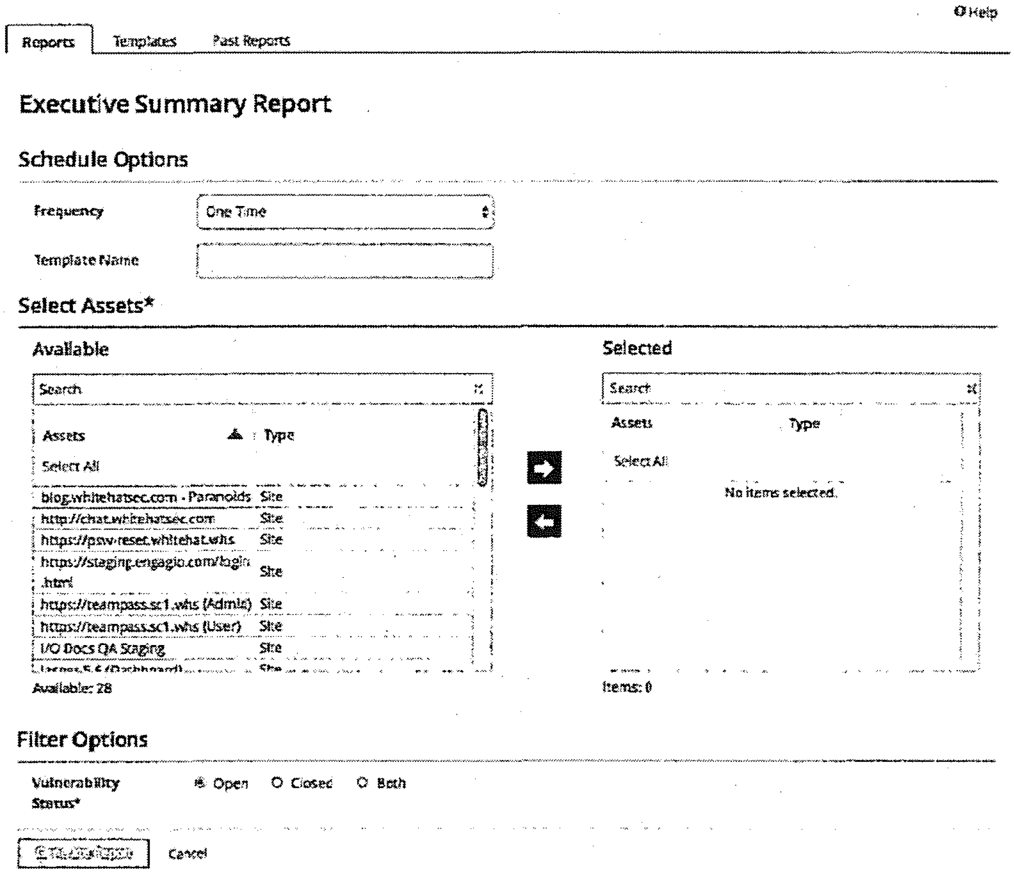
Go to the Reports landing page and click on the link that will take you to the report generation screen:



Reports

*Summary Reports*

| REPORT TYPE | GENERATE FOR | KEY BENEFITS | MAIN AUDIENCE |
|---|---|---|---|
| Executive Summary Report | • Assets<br>• Groups | • Provides a high-level understanding of the security risk profile of your assets<br>• Shows summary of vulnerability by assets and by severity class | • Executives<br>• Managers |
| Asset Summary Report | • Assets<br>• Groups | • Provides a high-level understanding of the assessment results<br>• Report contains summaries, metrics, and conclusions | • Development Managers<br>• Team Leads |
| WhiteHat Security Index Report | • Sites | • Provides a measure of the overall site security status using proprietary WhiteHat technology<br>• Index takes into account scanning frequency, remediation rate, outstanding issues, etc. | • Executives<br>• Managers |



## Executive Summary Report

### Schedule Options

Frequency: One Time

Template Name:

### Select Assets*

Available

| Assets | Type |
|---|---|
| blog.whitehatsec.com - Paranoids | Site |
| http://chat.whitehatsec.com | Site |
| https://psw-reset.whitehat.whs | Site |
| https://staging.engagio.com/login.html | Site |
| https://teampass.sc1.whs (Admin) | Site |
| https://teampass.sc1.whs (User) | Site |
| I/O Docs QA Staging | Site |

Available: 28

Selected

No items selected.

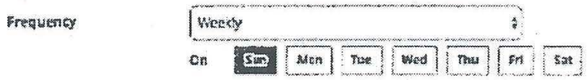
Items: 0

### Filter Options

Vulnerability Status*: ● Open ○ Closed ○ Both

In the Report screen, select your schedule options:

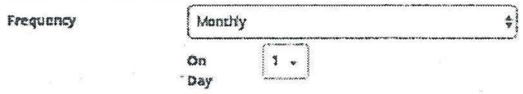
- One Time: This will run the report once, immediately, and notify you when it has been completed. The report will be available to you in the Past Reports tab for thirty days.
- Daily: This will run the report once a day; you will be notified by email when it has been completed and each daily report will be available in the Past Reports tab for thirty days.
- Weekly: This will run the report once every seven days; please select the day on which you want the report to run from the display that will appear:



Frequency Weekly

On Sun Mon Tue Wed Thu Fri Sat

- Monthly: This will run the report once each month on the date selected. Please select a date from the display that will appear:

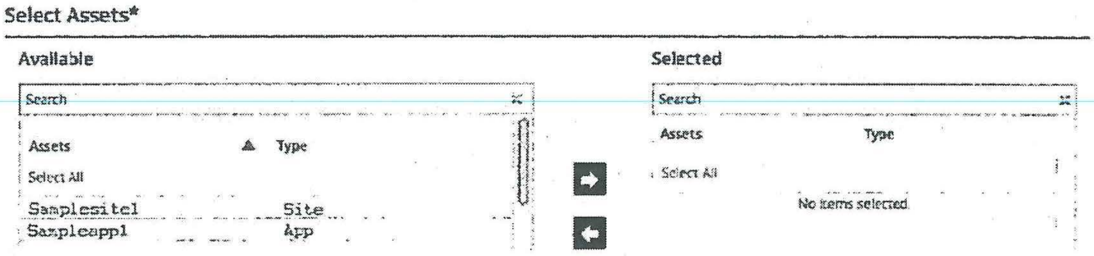


Frequency Monthly

On Day 1

**Note :** Any frequency choice other than "One Time" will require you to name your template; please use a name that is appropriate to the specific report you are running -- for instance "All Assets Monthly Summary Report" -- so that you can distinguish it readily from other possible reports of the same base type you may run.

Once you have selected the Frequency, please select the Assets you want to include in the report; to locate specific assets, use the "Search" bar at the top of the "available" or "selected" columns. You can use the arrows between the "available" and "selected" columns to move assets back and forth, or you can choose "Select All."



Select Assets*

Available

Search

| Assets | Type |
|---|---|
| Select All | |
| Samplesite1 | Site |
| Sampleapp1 | App |

Selected

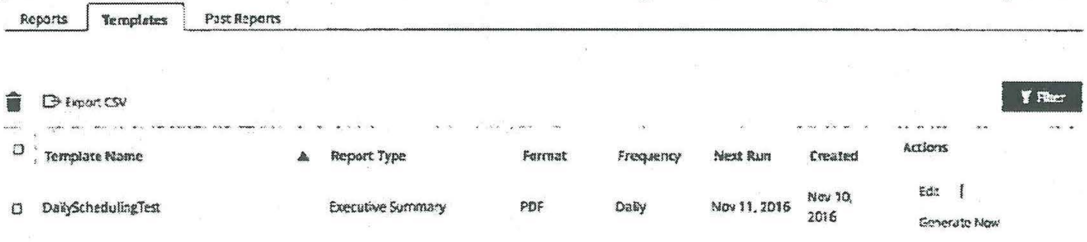
Search

| Assets | Type |
|---|---|
| Select All | |

No items selected

Once you have selected the Frequncy and the Assets you wish to include, please select the Filter Options: filter options will vary by report type.

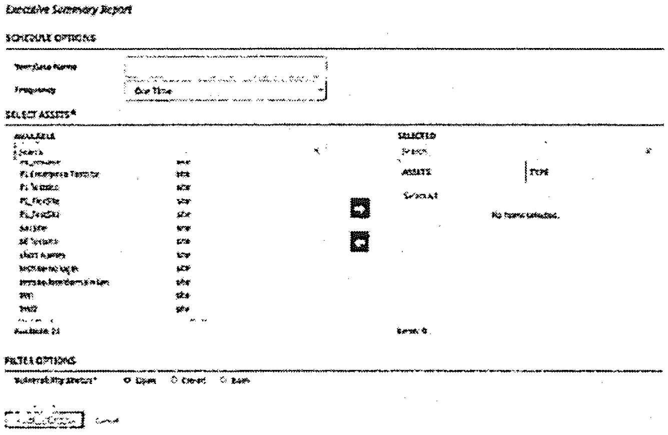
When you are done, click on "Generate Report." If you have selected a one-time report, report generation will begin and you will be notified when it is complete. If you have selected a repeating report, the template you have created will be saved in the "Templates" tab and it will be run at the next scheduled time; in the "Templates" tab you can review and edit that information or generate the report immediately if desired.



Reports Templates Past Reports

Export CSV Filter

| □ | Template Name | Report Type | Format | Frequency | Next Run | Created | Actions |
|---|---|---|---|---|---|---|---|
| □ | DailySchedulingTest | Executive Summary | PDF | Daily | Nov 11, 2016 | Nov 10, 2016 | Edit \|<br>Generate Now |



*Executive Summary Report*

SCHEDULE OPTIONS

Template Name

Frequency: One Time

SELECT ASSETS*

| AVAILABLE | | SELECTED | |
|---|---|---|---|
| Search | | Search | |
| [illegible] | site | ASSETS | TYPE |
| [illegible] | site | Select All | |
| [illegible] | site | | No items selected. |
| Available: 21 | | Selected: 0 | |

FILTER OPTIONS

Vulnerability Status* ● Open ○ Closed ○ Both

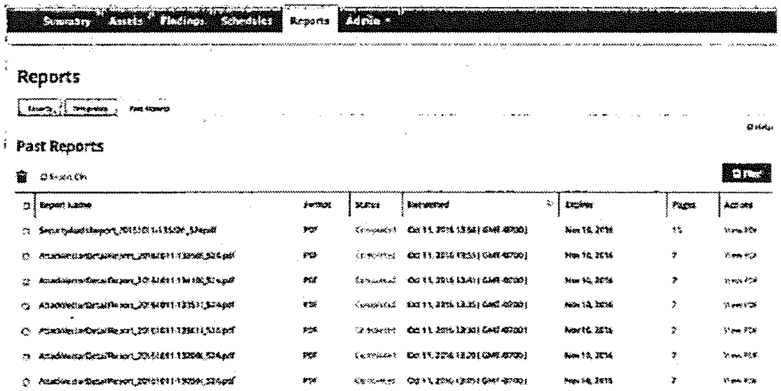
Cancel

## Viewing Completed Reports

Past reports are accessible from the Reports->Past Reports tab for thirty days from the date the report was generated.

You can download any completed report in the Past Reports tab by clicking on the View link (most reports will be PDF, and the link will be "View PDF," but a few may be CSV and the link will indicate that).

30 days after the report was generated, it will be deleted from the past reports tab; if you will need to retain the report for more than 30 days, please download and save the file.



Reports

Past Reports

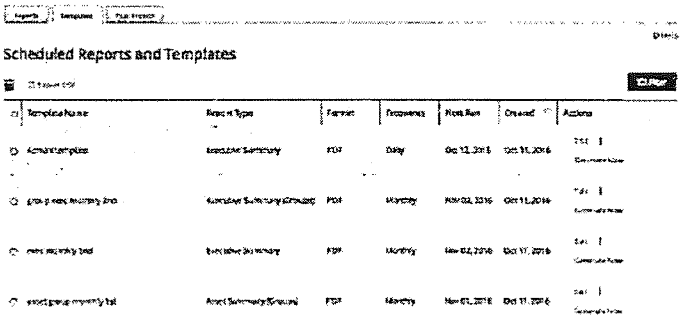
| □ | Report Name | Format | Status | Requested | Expires | Pages | Actions |
|---|---|---|---|---|---|---|---|
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:54 \| GMT-0700 | Nov 10, 2016 | 11 | View PDF |
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:51 \| GMT-0700 | Nov 10, 2016 | 7 | View PDF |
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:41 \| GMT-0700 | Nov 10, 2016 | 7 | View PDF |
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:35 \| GMT-0700 | Nov 10, 2016 | 7 | View PDF |
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:30 \| GMT-0700 | Nov 10, 2016 | 7 | View PDF |
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:20 \| GMT-0700 | Nov 10, 2016 | 7 | View PDF |
| □ | [illegible] | PDF | Completed | Oct 11, 2016 13:05 \| GMT-0700 | Nov 10, 2016 | 7 | View PDF |

## Viewing or Modifying templates

A template is a set of options used to generate a report. Each template has a user-specified name.

You can view or modify templates by going to the Templates tab and clicking on the Edit link for a given template.

Templates are used to generate reports according to a set schedule. You can also generate an on-demand report by clicking on the Generate Now button on the template tab.



## Scheduled Reports and Templates

| | Template Name | Report Type | Format | Frequency | Next Run | Created | Actions |
|---|---|---|---|---|---|---|---|
| ○ | [illegible] | Executive Summary | PDF | Daily | Oct 12, 2016 | Oct 11, 2016 | Edit ⋮<br>Generate Now |
| ○ | group exec monthly 2nd | Executive Summary (Groups) | PDF | Monthly | Nov 02, 2016 | Oct 11, 2016 | Edit ⋮<br>Generate Now |
| ○ | exec monthly test | Executive Summary | PDF | Monthly | Nov 02, 2016 | Oct 11, 2016 | Edit ⋮<br>Generate Now |
| ○ | asset group monthly tst | Asset Summary (Groups) | PDF | Monthly | Nov 01, 2016 | Oct 11, 2016 | Edit ⋮<br>Generate Now |

# The Executive Summary Report

The Executive Summary report shows you a summary of vulnerabilities by assets or by groups and by vulnerability class; as well as showing your overall security profile. For those customers using both Sentinel and Sentinel Source, this report will cover both dynamic and static test results.

For detailed findings, please see "Vulnerability Details Report - Applications" and "Vulnerability Details Report - Sites."

## The Executive Summary Report Options

The Executive Summary Report can be run for Assets or groups; select your preference under "Generate For" in the Reports/Reports tab. This report can be filtered by vulnerability status -- you can select all open vulns, all closed vulns, or both open and closed vulns.

For more information on generating reports, please see Creating Reports and Templates.

# The Asset Summary Report

The Asset Summary Report contains an overview of each asset's vulnerabilities by category, as well as trends of vulnerabilities discovered by month over the past year. In addition, the report lists each asset's vulnerabilities prioritized by their risk and severity level. This report provides an asset-by-asset listing of vulnerabilities, along with an overall graph showing vulnerabilities by class and overall rating.

## The Asset Summary Report - Options

For the Asset Summary Report, you can choose to see Open, Closed, or Both (all) vulnerabilities for any or all severity level(s). For more information on generating reports, please see Creating Reports and Templates.

# WhiteHat Security Index (WSI) Report

Methods

Understanding and Using the WSI Report

Sample WSI Report

The WhiteHat Security Index (WSI) indicates the overall security profile of a given site. This value will change as changes are made to the site, vulnerabilities found or remediated, or other factors the security index is based on change for a given site. (The WSI can be calculated only for dynamic sites, not for static applications.) The WSI provides:

- A single numerical metric that usefully measures a single asset's security
- An overall evaluation of the security of an asset for engineering managers and executives
- Guidance for the security team in determining which vulnerabilities are most critical
- A simple, transparent metric
- An understanding of the asset's security in relation to the relevant industry and to our global set of clients
- Sufficient granularity that moderate changes by the client will be reflected in the index
- Sufficient stability to ensure that small, short-lived changes do not result in large changes in the score
- Easy dimensional modeling and analysis
- Real-time display

The WhiteHat Security Index (WSI) is designed to encourage clients to act in ways that increase security, and to discourage dangerous behaviors and policies, to safeguard the index from deliberate manipulation ("gaming the system"), and to encourage engagement with WhiteHat Security to improve web application security.

## Running the WhiteHat Security Index Report

The WSI Report can be run as a PDF or a CSV report; for more information on generating this report, please see Creating Reports and Templates.

## Methods

The WhiteHat Security Index is based on measuring multiple factors over time. By including the current state and history for each factor, we can evaluate the probability that significant new vulnerabilities will be discovered and remediated appropriately. Additionally, tracking the past performance of an asset helps keep the index value stable when new vulnerabilities are detected - so that major releases may introduce new vulnerabilities without causing a drastic change in the model, but failure to remediate those vulnerabilities over time will be reflected by a decrease in the index.

The WhiteHat Security Index is designed to reward security-conscious behavior; the weight given to a vulnerability is based in part on how long it has been exposed, as well as on its rating, and the Index rewards closing vulnerabilities.

Each factor that contributes to the Security Index is calculated using sophisticated statistical analysis, and measures are included to prevent gaming the system.

Factors considered in the Security Index include:

- Service Duration: How long has a site been under Sentinel service?
- Vulnerability History: What is the site's history of opened and closed vulnerabilities?
- Missing Authentication: Does the site have the necessary authentications?
- Scan Frequency: What is the frequency with which a site is scanned, and what resources are allocated for scanning?
- PCI Compliance: Is the site PCI Compliant?
- Window of Exposure: What is the historical window of exposure for this site?
- Site Complexity: How complex is this site?
- Omitted Vulnerability Classes: What vulnerability classes are not currently being scanned for this site?

## Service Duration

Service Duration reflects the length of time that a site has been under contract as of the date of evaluation. Service Duration is important: the longer we have had the slot under contract the more detail we have collected about it, and the more effective testing is. Service Duration for a slot is compared to the Service Duration across all slots and clients at the same service level (BE, SE, PE, etc.).

## Vulnerability History

Vulnerability History consists of the number of vulnerabilities that are open vs. the number that have been closed as of the date of the evaluation. By including closed vulnerabilities as mitigating factors in this metric, we reward people who are closing vulnerabilities reliably. Closing vulnerabilities is a better indication of security than not having discovered vulnerabilities in the first place because it demonstrates an active security stance that involves seeking out and remediating vulnerabilities.

The longer a vulnerability is open, the negatively it will affect the WSI; the more promptly a vulnerability is closed, the greater the reward is for closing it. Additionally, vulnerabilities are weighted based on how common they are and on the threat and severity associated with the vulnerability.

## Missing Authentication

Slots that need authentication and do not have properly configured login handlers are evaluated as being less secure because sections of that site are not being scanned. If the client has not indicated that login handlers are unnecessary, and the service level for the slot is PE or SE, it is assumed that login handlers are required. (BE slots are presumed not to need login handlers unless they are configured to require one.) The Missing Authentication measure assumes the worst - it defaults to the assumption that the site has a large number of open vulns, because there is no way for WhiteHat to confirm that they do not.

### Scan Frequency

Scan frequency looks at the number of scans completed each week. The more regularly a site is scanned, the more likely vulnerabilities are to be detected before they can be exploited. When scans are performed frequently, even minor changes are reviewed in a timely way. Scan frequency also evaluates whether there are sufficient resources allocated to scanning to allow scans to complete reliably.

### PCI Compliance

PCI compliance is a measure of the historical PCI compliance for a given slot as of the date of evaluation. PCI compliance is largely based on vulnerability category; however, it is also affected by threat and severity values. The service level for a site may limit the nature and type of vulnerabilities that can be detected on a site; a PE site that is non-compliant might be evaluated as being "compliant" if it were evaluated at the BE service level. Therefore, values for slots with lower service levels will be adjusted to account for the vulnerabilities that may not be discovered at this level.

### Window of Exposure

Window of Exposure is a measure of the number of days out of the last 30 days that the site was exposed to a particular vulnerability. Again, a weighting factor is used to adjust for the inconsistencies that may result from differing service levels, and the Window of Exposure is tracked over 180 days - not just the number of days out of 30 count - in order to monitor a pattern of behavior, rather than only the events of the past month.

### Site Complexity

Larger and more complicated sites have a larger surface vulnerable to attack, and are therefore intrinsically less secure; Site Complexity uses the number of form elements and the number of POST/PUT requests on the site as a rough measure of the attack surface. The size of the site can be estimated based on the number of GET requests made during scanning.

### Omitted Vulnerability Classes

Clients can disable the scanning for Predictable Resource Location vulnerabilities; therefore, the index corrects for this by including the effect that could be associated with those vulnerabilities. That is, since scanning for the vulnerability is disabled, the index treats the site as if it were in fact untrustworthy, estimating the number of predictable resource location vulnerabilities to be high.

## Using the WhiteHat Security Index

### Monitoring Your Security Status

The WSI can be used to monitor the security status of assets. Specifically, you can use the WSI to:

- Identify areas of security risk
- Provide guidance on what vulnerabilities to fix
- Compare security status of sites in an organization

- Determine how you are doing relative to global and industry verticals by comparing percentile ratings
- Monitor trends in security status of assets and effectively manage application security program

## Improving your WhiteHat Security Index Score

Your WSI report recommends a set of actions that site owners can take to improve asset security. This includes an ordered list of top vulnerabilities that need to be fixed to improve the score, along with configuration-related recommendations such as increasing scan frequency, providing a scan schedule, or providing missing credentials.

## Prerequisites for a WhiteHat Security Index Score

There are a few prerequisites for the WSI score to be available.

- The site must have had at least three completed scans. This allows the scanner to be fully trained on the site.
- The site must have been being scanned over at least 30 days following the third completed scan, to provide sufficient history to allow the weighting factors to be calculated and to allow some of the model parameters to be primed.
- WSI is available on PE, SE, and BE service levels only.

# Security Audit Report

The Security Audit report provides an overview of open vulnerabilities discovered in the assessment, including summaries, metrics, and conclusions. For those customers using both Sentinel and Sentinel Source, this report will cover both dynamic and static test results. For more detailed findings, please see "Vulnerability Details Report - Applications" and "Vulnerability Details Report - Sites."

Note that you can choose whether to include or refrain from including a count of the vulnerabilities.

For more information on generating reports, please see Creating Reports and Templates.

# PCI Compliance Report

The PCI Compliance Report declares the compliance state of the selected site(s) as defined in PCI DSS 3.0 Requirements 6.5.1 - 6.5.11.

This report is extremely useful for those cases when it is necessary or useful for you to demonstrate that a site is PCI-compliant.

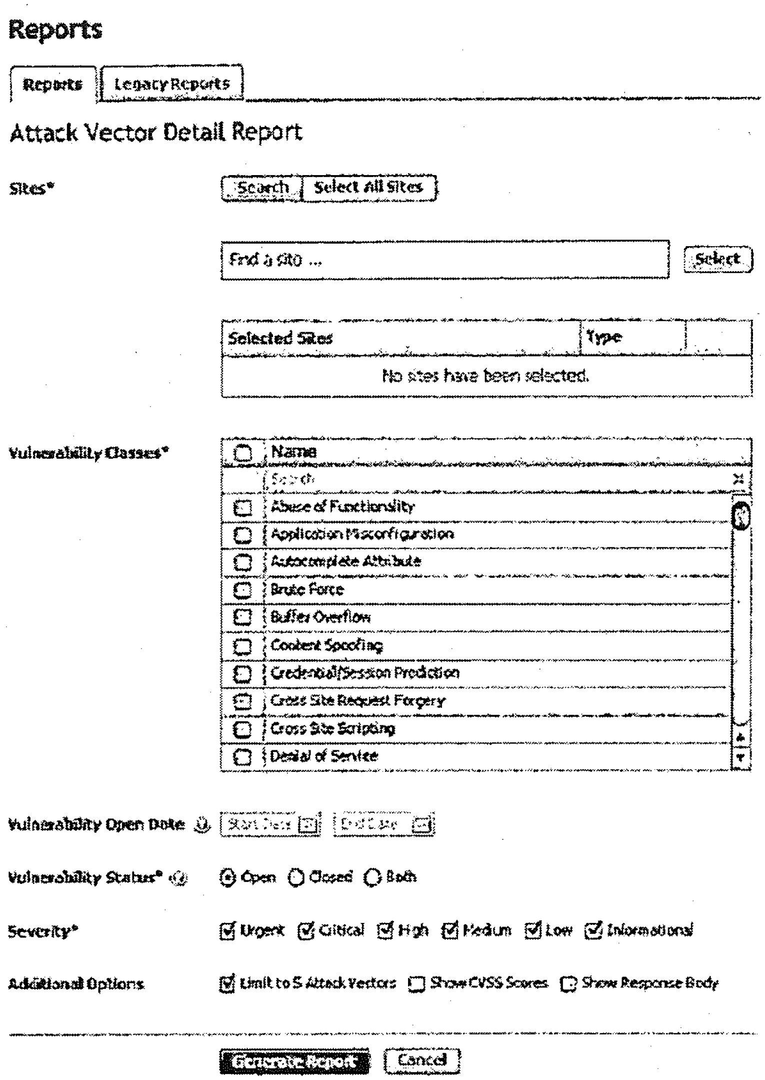
For more information on generating reports, please see Creating Reports and Templates.

# The Attack Vector Detail Report

The Attack Vector Detail Report contains up to five specific attack vectors for every vulnerability instance found on the websites selected for this report. (Note that attack vectors are not reported for code scanned using Sentinel Source (static assessment).) In addition to the location and time the vulnerability was discovered, the attack vector details include a breakdown of the exact request sent so that developers may easily replicate the problem. This report is most likely to be of interest to developers engaged in remediating a specific vulnerability.

## The Attack Vector Detail Report - Options

For the Attack Vector Detail Report, you can select specific assets or groups and vulnerability classes you are interested in, filter by date, specify whether you want to see Open, Closed, or Both (all) vulnerabilities, specify the severity level to include, and determine whether you want to limit the attack vectors, show the CVSS scores, or show the response body in the report; you can also choose to generate the report as a pdf or as a csv file. For more information on generating reports, please see Creating Reports and Templates.



Reports

Attack Vector Detail Report

Sites*

| Selected Sites | Type | |
|---|---|---|
| No sites have been selected. | | |

Vulnerability Classes*

| □ | Name |
|---|---|
| | Search |
| □ | Abuse of Functionality |
| □ | Application Misconfiguration |
| □ | Autocomplete Attribute |
| □ | Brute Force |
| □ | Buffer Overflow |
| □ | Content Spoofing |
| □ | Credential/Session Prediction |
| □ | Cross Site Request Forgery |
| □ | Cross Site Scripting |
| □ | Denial of Service |

Vulnerability Open Date: Start Date / End Date

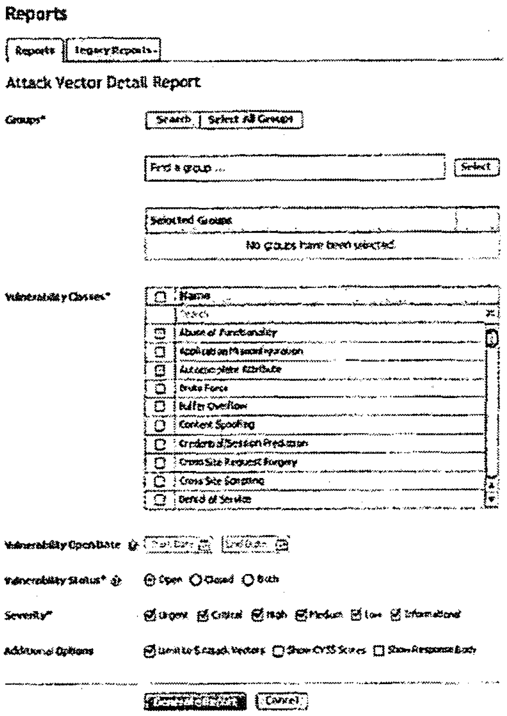
Vulnerability Status*: ● Open ○ Closed ○ Both

Severity*: ☑ Urgent ☑ Critical ☑ High ☑ Medium ☑ Low ☑ Informational

Additional Options: ☑ Limit to 5 Attack Vectors □ Show CVSS Scores □ Show Response Body

## The Attack Vector Detail Report - Selection by Groups

You can also select sites based on groups.



Reports

Reports | Legacy Reports

Attack Vector Detail Report

Groups* [Search | Select All Groups]

Find a group ... [Select]

Selected Groups: No groups have been selected.

Vulnerability Classes*

| □ | Name |
|---|---|
| | Search |
| □ | Abuse of Functionality |
| □ | Application Misconfiguration |
| □ | Autocomplete Attribute |
| □ | Brute Force |
| □ | Buffer Overflow |
| □ | Content Spoofing |
| □ | Credential/Session Prediction |
| □ | Cross Site Request Forgery |
| □ | Cross Site Scripting |
| □ | Denial of Service |

Vulnerability Open Date: Start Date | End Date

Vulnerability Status*: ● Open ○ Closed ○ Both

Severity*: ☑ Urgent ☑ Critical ☑ High ☑ Medium ☑ Low ☑ Informational

Additional Options: ☑ Limit to 5 Attack Vectors □ Show CVSS Scores □ Show Response Body

When you have made your selections and clicked on "Generate Report," the report will return to you as a pdf file.

For each vulnerability class included in the report, you will first see the description and solution for the vulnerability, and then the details of the attack vectors.

# Vulnerability Details Report - Site

The Vuln Detail Report groups findings by category for each website selected for the report. Each chapter of the report gives a full description of the vulnerability class and the appropriate remediation instructions, followed by a list of the specific instances of that vulnerability on each site. This is an excellent report for helping developers remediate vulnerabilities, or providing an in-depth understanding of the specific vulnerabilities found for a particular asset.

For the Vulnerability Detail Report, you can select specific assets and specify:

- Whether you want to see Open, Closed, or Both (all) vulnerabilities.
- Which vulnerability classes you want to include in the detail report.
- The date range for the report.
- Which severity levels should be included in the report.
- Whether or not Attack Vectors should be shown.
- Whether or not the CVSS Score should be shown.

You can select what is to be included in the report by individual site or by group.

For more information on generating reports, please see Creating Reports and Templates.

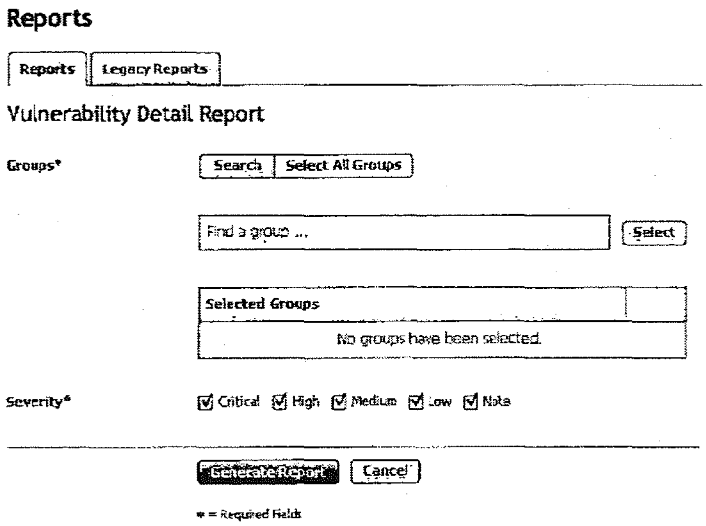
# Vulnerability Details Report - Applications

The Vuln Detail Report groups findings by category for each application selected for the report. Each chapter of the report gives a full description of the vulnerability class and the appropriate remediation instructions, followed by a list of the specific instances of that vulnerability found in the application. This is an excellent report for helping developers remediate vulnerabilities, or providing an in-depth understanding of the specific vulnerabilities found for a particular asset.

For the Vulnerability Detail Report, you can select specific assets and specify:

- Whether you want to see Open, Closed, or Both (all) vulnerabilities
- Which vulnerability classes you want to include in the detail report
- The date range for the report
- Which severity levels should be included in the report

For more information on generating reports, please see Creating Reports and Templates.



Reports

Vulnerability Detail Report

Groups*

Find a group ...

| Selected Groups | |
|---|---|
| No groups have been selected. | |

Severity* ☑ Critical ☑ High ☑ Medium ☑ Low ☑ Note

* = Required Fields

Click on Generate Report, and you will see the pdf of the Vulnerability Detail Report.

# Scan Status Report

The Scan Status Report will generate a csv file showing the scan status of all reports for which you have permissions. This report will include the asset information, service level, and scan status.

For more information, please see Creating Reports and Templates.

## Asset Permission Report

The Asset Permission Report creates a csv report showing the permissions for all the assets for which you have permissions.

Asset permission will include the asset type, url, name, and the email and first and last name of users who have access to that asset.

For more information on creating reports, please see Creating Reports and Templates.

# Asset Group Mapping Report

The Asset Group Mapping Report will include the asset type, url, name, and the names of the group(s) to which that asset belongs for all assets for which you have permissions. The asset's groups will be included in a single cell, separated by the pipe mark ("|").

For more information on generating reports, please see Creating Reports and Templates.

**WhiteHat Security**
3970 Freedom Circle, Santa Clara, CA 95054
https://www.whitehatsec.com
408.343.8300

WhiteHat Security

# WhiteHat Sentinel Onboarding Guide

November 2016

*Current Documentation is available via the Customer Portal at https://whitehatsec.secure.force.com/opex/DocumentDownload.*

WhiteHat Security updates services regularly. For details of recent releases, please see the in-product Release Notes available in the Summary/ Updates tab. The most current documentation available can be located in the WhiteHat Security Customer Portal under the "Documentation and Tools" tab.

**WhiteHat Security**

3970 Freedom Circle
Santa Clara, CA 95054

https://www.whitehatsec.com
T: 408.343.8300

# Table of Contents

# WhiteHat Sentinel Onboarding Processes

WhiteHat's Customer Success unit will work with you to get your Sentinel services up and running as quickly as possible, so that your web assets are being properly scanned and you are receiving accurate security information. The *WhiteHat Sentinel Onboarding Processes* document will outline how the onboarding process will work, and what you can do to expedite it.

Additional information about onboarding and about making the best use of Sentinel and Sentinel Source is available in our Customer Success Center; login information for the Customer Success Center will be sent to you in e-mail on your contract start date. The Customer Success Center provides ready access to the customer success team, to your tickets, to Q&A information, and to downloadable reference and training material (including all user guides).

You will receive several emails from the WhiteHat Service Deployment Team on your contract start date – one providing you with your Sentinel interface login information, one providing your Customer Success Center login information, and one asking to schedule an introductory call. For that call, we will be asking you for the following information:

## For Sentinel Source (SAST) Services

- Source Code Repository and type(s) (e.g. SVN, CVS, Perforce) or Source Code Archive
- URI(s) of the repositories or archives and any associated code bases
- Read-only credentials or certificate information

## For Sentinel (DAST) Services

- Web application hostname(s) and any associated host names
- Web application credentials (two sets; one primary and backup set with the highest available level of access, and one primary and backup set with a standard level of access)
- Weekly assessment schedule(s) (continuous, evenings and weekends, or specified days and times)

## For Sentinel Mobile Services

- All project files for your mobile application(s), both source code and build files
- Two sets of credentials

The better prepared you can be at the beginning of the onboarding process, the more quickly the WhiteHat team can get your scan services running in a continuous mode.

For more detail, please see

- *Onboarding Sentinel Source (Static) Services*
- *Onboarding Sentinel (Dynamic) Services*
- *Onboarding Sentinel Mobile Services*

# Onboarding Sentinel Source (Static) Services

## Required Information

For onboarding your static analysis services, we need to know the type of Source Code Repository you're using (if any), the URIs of the repositories/code bases or binaries we will be assessing, appropriate credentials, and the assessment schedule you want to use.

### Source Code Repository Type(s)

We'll need to know what type of repository houses the application code you want us to assess, so that we can provision the correct connector for that repository within the satellite appliance you'll need to install prior to beginning an assessment. Information on the types of repositories we currently support is available in the Adding a Code Base section of the Managing Your Applications user guide.

### URI(s) of the Repositories and Associated Code Bases

You can add code bases that are part of the application to the scope of the Source scan. Doing this ensures a complete scan of the application's source code.

**NOTE:** Please ask your developers if there are any dependencies not declared within the application source code. If there are, please add these as additional code bases associated to the applic- ation within the Sentinel UI. This will ensure that our scanning engine can thoroughly test all source code related to the application.

### Read-Only Credentials

You'll need to provide us with read-only credentials (if any) to the repositories on which your application resides. This allows our source code scanning engine to automatically log into the repository at the beginning of each schedule scan window.

### Assessment Schedule

You can schedule scans of your source code on an as-needed basis. We recommend scheduling scan windows regularly to ensure a current view of your application's security status.

- Scan Now - Scans source code only once to completion
- Daily - Scans source code once per day to completion
- Weekly - Scans source code once per week to completion
- Never Scan (Default)-- Your source code will not be scanned until you edit the scan schedule to allow scanning
  (**NOTE:** until you set a scan schedule, the assessment schedule will be set to the "Never Scan" default value)

# Service Delivery Timeline and Setup

## Source Appliance Download and Installation (1 Business Day)

The Source VM not only houses our Source scanning engine, but also creates a secure SSH tunnel from our servers to yours that allows us to verify potentially vulnerable code snippets. These snippets are the only pieces of your source code that will be passed via this secure connection to our TRC engineers.

Follow the steps outlined in the Source Appliance guide, attached to your welcome email, to download and set up the VM Appliance within your network. **Note:** We recommend having someone who has experience with ESX servers available for the setup process.

Once you've installed the VM, we will verify the connection to your intended repositories is successful.

## Adding Applications and Code Bases

Since code checkout is done remotely via automation, Sentinel does not support browsing from a repository root, project listing, or web directory. If your application requires multiple repository projects to build, please add each project as a separate codebase. Remember that adding codebases that do not make up a single build may result in build errors that prevent the scan from completing.

If your version control technology is not supported or if your application's build requires dependencies that are not available from a repository accessibl by the satellite appliance, you may use a "mock codebase" to provide additional code to be used in the scan via a gzipped tarball. In addition, you may set an application up to have its binary files scanned, rather than its code.

For more information on adding applications and code bases, please see the user guide Managing Your Applications, found on the Customer Portal under the Documentation and Tools tab.

Contact your customer service agent to discus alternate methods of tarball delivery.

## Vulnerability Verification (Ongoing)

Any time Sentinel finds a vulnerability during a scheduled scan, it sends the potentially vulnerable code snippet to our TRC engineers. Our engineers then verify that the vulnerability is true and actionable before posting it.

# Initial Assessment Complete (1-2 Weeks for initial assessment)

When the first full scan has completed successfully and all verified vulnerabilities have been reported to you, we recommend scheduling a Vulnerability Review call where our TRC engineers can discuss and explain vul-

## Support Levels

### STANDARD

Standard Support is included with all WhiteHat Sentinel subscriptions. It provides multiple contact options, such as access to our secure Customer Success Center, email access, or via a direct phone number.

**Customer support hours are**
**12:00 AM - 7:00 PM PST, Monday through Friday, excluding holidays.**

### GOLD

The Gold Support is designed for enterprise customers who require a highly personalized, proactive support relationship. Aligning people, processes and technology to achieve operational readiness is a key goal of this program. Gold support includes integrating technology with organizational processes, website deployment, change management, and support escalation to reach and remain at a state of operational readiness. To meet these objectives, Gold Support includes:

- An assigned Customer Success Manager (CSM)
- Priority response times and service level agreements (SLAs)
- Regularly scheduled meetings with your CSM to ensure operational efficiency
- Quarterly Business Reviews designed to maximize the value of your purchase
- Custom vulnerability exploit and remediation review

#### Customer Success Manager

Your assigned Customer Success Manager (CSM) is a highly skilled security professional who facilitates support requirements and escalates resolution requests to ensure that your issues are resolved quickly. Based on monthly business reviews, the CSM will manage your service requirements, including the review of open vulnerabilities and the management of each case to ensure proper closure. Each CSM serves as a cross-functional, cross-company advocate, who guides your organization in best practices and enables you to make rapid progress to align your security program with your business goals. The CSM coordinates support services and collaboration between WhiteHat Security, your web application business owners, developers, and security teams.

#### Custom Vulnerability Exploit and Remediation Review

WhiteHat Security will work with your developers to classify and understand the root causes and weaknesses of the discovered website vulnerabilities. Our security engineers are available to talk to your developers, provide a proof of concept, and help them understand the best remediation options available and how other web technology leaders are addressing these issues.

## PLATINUM

Platinum Support is ideal for commercial, government, enterprise, or global organizations utilizing the WhiteHat Sentinel family of products to deploy a comprehensive application security program across the software development lifecycle, and for organizations having stakeholders across multiple divisions or countries.

Platinum Support provides the highest level of a personalized support relationship with WhiteHat Security by providing both a Customer Success Manager (CSM) and giving you direct access to senior Threat Research Center (TRC) security engineers. Platinum level support also includes an annual onsite strategic process review. Platinum Support includes:

- Annual onsite strategic process review
- Quarterly vulnerability review
- Direct access to senior security engineers
- An assigned Customer Success Manager (CSM)
- Priority response times and service level agreements (SLA)
- Custom vulnerability exploit and remediation review
- 24/7/365 access to the Customer Success Center
- WhiteHat Sentinel interface training

### Annual Onsite Strategic Process Review

WhiteHat Security will provide a senior security engineer to spend three days onsite at your facility to help your team develop and execute strategic website risk management plans tailored to your specific business environment. During an annual review, for example, strategies can be developed that enable different business stakeholders – including risk management and compliance, product management and software development teams – to share ideas with WhiteHat experts and strategize on best practices for web security.

Annual Onsite Strategic Process Reviews cover:

- Vulnerability data discovered during the ongoing Sentinel assessments.
- Reports with remediation statistics and metrics.
- Mitigation techniques and security best practices.
- Overview of the current web security landscape and how it affects your organization.

### Direct Access to Senior Security Engineers

WhiteHat provides you direct access by phone and email to senior security engineers. WhiteHat will respond to your requests for assistance within two business hours on Mondays through Fridays from 6:00 AM and 7:00 PM PST, excluding WhiteHat holidays.

Platinum Support includes:

### Quarterly Vulnerability Review

Once per quarter, WhiteHat conducts a detailed review of high risk vulnerabilities discovered. The objective is to help your organization streamline the remediation process. During this review, a WhiteHat security engineer will give live demonstrations of the vulnerabilities, to show how high-risk vulnerabilities can threaten your business. By clearly understanding how each vulnerability can be exploited and understanding the risk associated with each vulnerability, you will be able to prioritize, manage, and mitigate your website risk more effectively.

## Support Features

| SUPPORT FEATURES | STANDARD | GOLD | PLATINUM |
|---|---|---|---|
| Customer Support Web Portal<br>• Case Management<br>• Security Documentation<br>• Knowledgebase & FAQs | • | • | • |
| Sentinel Interface Training<br>• (Onsite training not included in any service level.) | • | • | • |
| Service Request Response Time:<br>(cases submitted during business hours: M-F 12:00 AM – 7:00 PM PST) | Next Business Day | 1 hour - Critical (24x7)<br>4 hours - Serious | 1 hour - Critical (24x7)<br>4 hours - Serious |
| Priority Resolution Service Level Agreements (SLA)<br>• Severity Critical - 1 business day<br>• Severity Serious - 3 business days |  | • | • |
| Quarterly Business Reviews |  | • | • |
| Custom Vulnerability Exploitations and Remediation Reviews (PoC) |  | • | • |
| Annual Onsite Strategic Process Reviews (T&E not included) |  |  | • |
| Quarterly Vulnerability Reviews |  |  | • |
| Direct Line Senior Security Engineers (12AM – 7PM) including holidays |  |  | • |

WhiteHat SECURITY.

nerabilities. This call includes a breakdown of each reported vulnerability class and their threat to your application's security using some of your vulnerabilities as examples.

We encourage you and your security and development teams to request Vulnerability Reviews for specific vulnerabilities any time during your subscription term.

# Onboarding Sentinel (Dynamic) Services

## Required Information

### Web Application Hostname(s) and Associated Host Names

The application hostname establishes the boundaries of the Sentinel assessment. Sentinel will only assess content that is specified by the hostname.

Associated hostnames are those that are considered part of the same application where content is either accessible from a single login entry or without authentication. These hostnames can be added to the assessment scope under the same license, and will allow the assessment to encompass the entirety of the web application. For example:

- Hostname: www.site.com
- Associated hostnames: secure.site.com, www.contact.site.com

**Note:** associated hostnames are critical to ensure full testing of a site that may have multiple site URLs that do not directly link to one another, as in the examples given above. As long as the content is accessible with a single login entry (or with no authentication at all) and using a single session ID, it can be included as part of the same application. If a new login or an additional session ID is required, it is considered to be a separate application for purposes of licensing and assessment.

### Credentials

Though credentials are not required for your application assessments to begin, they're important to ensure we're able to access and test all functionality, specifically for sites that contain authenticated content. Please provide two sets of credentials with access to most or all functionality. One account serves as the primary account for automated testing, while the second account serves as a backup in case the primary account becomes invalid. For PE licenses, two additional test accounts for each user level are needed for business logic testing.

Example:

- Two administrator accounts
- Two expert or special user accounts
- Two standard user accounts

This allows us to perform both horizontal and vertical privilege testing across the various user roles of the application. For example:

- Can Imani see Dar's account profile data?
- Can a non-administrative user escalate their privileges to an administrative account?
- Can Shashi rotate through user accounts and perform transactions as another user?

## Assessment Schedule

The assessment schedule is the recurring weekly date and time range where Sentinel is allowed to actively test your application. Sentinel saves its progress between scheduled windows, so if a scan is unable to complete before the scan window concludes, it can pick up where it left off at the beginning of the next scan window.

You can set your weekly schedule within the Sentinel interface, and there are several scheduling options available.

Continuous (highly recommended): Assessments run 24x7

Nights & Weekends (recommended): Weekdays from 8pm to 6am (based on the time zone you select), and 24 hours a day on weekends

Custom Schedule: You can choose to create a custom assessment schedule based on days of the week and hours of each day. If this option is chosen, please ensure at least 40 hours of scan time per week

**CALENDAR RISK MITIGATION TIP:** IF YOUR SITES ARE HOSTED BY A THIRD PARTY, NOTIFY THEM AHEAD OF TIME REGARDING WHITEHAT IP RANGES AND YOUR PREFERRED SCAN SCHEDULE.

All WhiteHat scans or manual work will come from one of our IP addresses or IP address ranges:

### WhiteHat IP Ranges

| Scanning for Production Sites | Manual Testing |
|---|---|
| • 63.128.163.0/27<br>• 63.128.163.33<br>**Satellite Testing**<br>**US**<br>• 63.128.163.8 - Port 5050<br>• 63.128.163.8 - Port 6511<br>**EU**<br>• 52.28.188.156<br>• 54.93.186.146 | **Santa Clara**<br>• 12.248.108.202<br>• 12.33.220.130<br>• 67.207.113.226<br>**Houston**<br>• 38.122.74.18<br>• 64.244.165.6<br>**Belfast**<br>• 194.46.129.108<br>• 82.68.82.33 |

# Service Delivery Timeline and Setup

## Initial URL Crawl (1-3 Weeks)

Once URLs and site credentials (if applicable) are received and a scan schedule has been entered, our TRC engineers create a customized login sequence that teaches Sentinel to assess authenticated portions of the web application. Sentinel will then begin crawling (also called "spidering") your application. Completion time for the initial crawl varies depending on the number and size of pages within the application. During the initial crawl, only GET requests are tested. For sites under an SE or PE license, all POST request functionality is sent to a TRC engineer for custom test configuration. Sites under a BE license will always be tested using only GET requests.

## Custom Test Configuration (PE and SE only) (1-10 Business Days/Ongoing)

As Sentinel crawls your application, it alerts our Threat Research Center (TRC) of any forms your application contains, so an engineer can make custom test configurations that both allow Sentinel to safely test each form and permit the Sentinel scan to spider pages that lay behind each form. We refer to this step as "form training." If your application contains several layers of forms, it may take several passes by Sentinel and several rounds of form training to reach all pages within the application.

During this step, the TRC engineer may also enable URL rules for any template pages contained in your application. These rules instruct Sentinel to test a sample number of pages for each template used, which allows each Sentinel scan to complete more quickly while remaining thorough. As an example, an auction site that contains millions of products and is constantly adding additional products may use a common template. Instead of attempting to assess each individual product page, we will create a URL rule to assess only a subset of them. This reduces scan completion time without sacrificing quality.

Any time Sentinel discovers new forms or templates during your subscription term, a TRC engineer will recommence this phase. To ensure the safety and quality of the assessment, if anything unexpected is discovered, we will reach out to you before making configurations or implementing changes.

## Review of Site Coverage

Near the end of the custom test configuration phase, TRC engineers will examine all links discovered by Sentinel. If there are pages known to exist that are missing from our scan coverage, an engineer will add them to our testing scope as entry points. Directories or files that are not directly accessible from a link connected to the web application are common examples of pages that may need to be added as entry points .

You can expedite this phase by reviewing the pages found and tested by Sentinel within your Sentinel Interface and notifying us if sections of your application are missing.

## Vulnerability Verification

Any time Sentinel finds a vulnerability, it flags the page and attack vector and sends a notification to our TRC engineers. Our engineers then verify by hand that the vulnerability is true and actionable before posting it.

Vulnerabilities are grouped by the URL on which they are discovered, and then into the various vulnerability classes found within the Web Application Security Consortium V2 (WASC v2). The various methods to exploit discovered vulnerabilities are categorized by vulnerability parameters known as "attack vectors".

# Business Logic Assessment (5 Business Days/Ongoing)

If you've purchased PE Service, our TRC engineers will assess your application for vulnerabilities in its business logic. This testing is done by hand and begins during the Custom Test Configuration phase (see above).

# Initial Assessment Complete

The initial assessment is understood to be complete when the phases detailed above have been completed.

At this point, we recommend scheduling a Vulnerability Review call where our TRC engineers can discuss and explain vulnerabilities. This call includes a detailed breakdown of each vulnerability, as well as a live demonstration of the vulnerabilities discovered, and is a great opportunity to involve other members of your security and development teams.

We encourage you to request a Vulnerability Review any time during your subscription term.

# Onboarding Sentinel Mobile Services

## Required Information

- Project Files for your Mobile Application(s)
    - Source Code
    - Build Files

Our TRC engineers will need your application's project files, including source code and build files. You can upload these files to the SFTP account we create for you.

Our Mobile Assessment Team securely downloads these files to conduct the assessment, and deletes them permanently when the assessment is complete.

## Service Delivery Timeline and Setup

### SFTP Account Setup (1 Business Day)

Our Service Deployment Team will create an account for your team on our SFTP server and provide you with access details. This is where you'll need to upload your application's project files.

### Assessment (10-15 Business Days)

During this time, TRC engineers will be assessing your mobile application for vulnerabilities.

# WhiteHat Sentinel Customer Support

## Optimizing your use of WhiteHat Sentinel with fast, reliable support

WhiteHat empowers you to protect critical data, ensure compliance, reduce risk and accelerate the deployment of secure applications and websites. By providing accurate, comprehensive, and risk-based application security assessments as a software-as-a-service, we deliver the visibility, flexibility, and guidance that organizations need to prevent web attacks.

WhiteHat Support services ensure that you are effectively leveraging all the web application security information that WhiteHat Sentinel delivers. With over 40,000 web applications under management, many in the Fortune 500 companies, WhiteHat's customer support team has superior technical experience in application security, delivering the resources you need to reduce risk, and improve security processes.

WhiteHat Security's highly trained security teams provide enterprise-class software security support. Our engineers know web servers, web applications, and web application software development, including hands-on experience with leading software development frameworks, design patterns, and implementation practices, as they relate to security. There are three levels of support available to Sentinel customers: Standard, Gold, and Platinum.

**HIGHLIGHTS**

Keep your business running in production with quick response times. WhiteHat Sentinel assesses live production applications safely, without impacting performance or your bottom line. Whenever you need expert assistance, we are just a click, email, or phone call away.

Access our Customer Success Center instantly to log, track, and update cases online. The Customer Success Center also offers the latest security information, FAQs, training information, and product documentation.

## APPENDIX A TO CONTRACT
## SERVICE DESCRIPTION

Subject to the terms of the Contract and any Service Order (as defined below), WhiteHat will provide VCU the Services, Support and/or Training pursuant to the terms of this Appendix.

### 1. DEFINITIONS

1.1 "API" means a web service that is accessed via a URL; and is described using the web services description language (WSDL) (limited to simple object access protocol (SOAP) or hypertext transfer protocol (HTTP)) or a representational state transfer (RESTful) API (limited to HTTP).

1.2 "Application" or"Applications" means individually or collectively, a (i) Web Application, (ii) Source Application and (iii) Mobile Application, each as defined in this Section 1.

1.3 "Available" means that WhiteHat customers are able to log on to the WhiteHat Sentinel website as measured at http://stats.pingdom.com/86tj5dh0uwp4/113541 and/or http://stats.pingdom.com/86tj5dh0uwp4/1667403, as applicable.

1.4 "Claim" means any third party claim that the Services or the Training, when used in accordance with this Contract, infringe any United States patent, copyright or trademark of a third party.

1.5 "Customer" means VCU and any (i) public body, (ii) public or private health or educational institution or (iii) lead-issuing institution's affiliated foundations, based in the Commonwealth of Virginia, may access any resulting contract(s) if authorized by the Contractor.

1.6 "Customer Support Web Portal" means WhiteHat's web portal for customer support.

1.7 "Documentation" means any online information, product descriptions, technical specifications, manuals and materials made available to the Customer, relating to the use of the Services.

1.8 "Double-Extra Large Source Application" means a Source Application that is less than (i) 200MB in Uncompressed Source File Size or (ii) five million (5,000,000) Lines of Code.

1.9 "Environment" means the environment (for example, development, staging or production) in which a particular Source Application is housed when scanned by the Services.

1.10 "Extra-Large Source Application" means a Source Application that is less than (i) 120MB in Uncompressed Source File Size or (ii) three million (3,000,000) Lines of Code.

1.11 "Extra-Small Source Application" means a Source Application that is less than (i) 4MB in Uncompressed Source File Size or (ii) one hundred thousand (100,000) Lines of Code.

1.12 "Large Source Application" means a Source Application that is less than (i) 60MB in Uncompressed Source File Size or (ii) one million five hundred thousand (1,500,000) Lines of Code.

1.13 "Lines of Code" means the lines of Customer's source code containing any characters (excluding comments and white spaces), as measured by WhiteHat based on the average of up to the last twenty (20) scans of such Source Application by the Services.

1.14 "Medium Source Application" means a Source Application that is less than (i) 20MB in Uncompressed Source File Size or (ii) five hundred thousand (500,000) Lines of Code.

1.15 "Mobile Application" means an application that can run on one platform, either IOS or Android Platform, and can be written in either Objective-C for IOS, Java for Android, or in HTML/CSS/Javascript.

1.16 "Operation" means a discrete function accessed via a combination of its API's base URL, the Operation's name, and a request payload.

1.17 "Reports" means data reports that contain the results of the tests performed by the Services.

1.18 "Services" means the application and API security testing services (including (i) the associated software and (ii) access to WhiteHat's hosted software application) for the Applications and/or APIs as described on an applicable Service Order.

1.19 "Small Source Application" means a Source Application that is less than (i) 10MB in Uncompressed Source File Size or (ii) two hundred fifty thousand (250,000) Lines of Code.

1.20 "Service Order" means any (i) duly executed service order, (ii) duly executed statement of work, (iii) duly executed order form or (iv) WhiteHat quote with corresponding purchase order incorporating a reference to the WhiteHat quote number, provided for the purpose of acquiring the Services and/or the Training and that incorporates the Contract by reference, and contains a description of the Services and/or Training ordered by Customer and the applicable Fees and term of the Service Order.

1.21 "Services" means the application and API security testing services (including (i) the associated software and (ii) access to WhiteHat's hosted software application) for the Applications and/or APIs as described on an applicable Service Order.

1.22 "Source Application" means the smallest single unit of source code in a single Environment that can run independently on a server or mobile device, the code base of which does not change more than 20% between Service scans.

1.23 "Training" means any computer-based training or onsite training provided by WhiteHat.

1.24 "Training Materials" means any training materials and handouts provided to Customer as part of the Training, including, but not limited to, documents, data, drawings, models, code, applications and reports, and associated software and materials, including any modifications or improvements thereof. Training Materials may include third party materials licensed to WhiteHat.

1.25 "Uncompressed Source File Size" means the size of the source code contained in a Source Application in megabytes (MB) as measured by WhiteHat based on the average of up to the last twenty (20) scans of such Source Application by the Services.

1.26 "Web Application" means an application that consists of a group of related hostnames and one set of user login credentials.

## 2. LICENSE

During the Term and subject to the terms and conditions of this Contract, WhiteHat shall provide to Customer a limited, non-exclusive, non-transferable license to use and access the (i) Services for the number of Applications and/or API Operations set forth in a Service Order, (ii) the Training, and (iii) the associated Documentation and Training Materials, subject to any additional terms and conditions required by any third party providers, as described in a Service Order. Such license grant for any software associated with the Services that must be downloaded by Customer shall include the right to make one copy for internal use in accordance with the Documentation, and such license grant for the Training Materials is provided solely for Customer's internal use to further expand and improve the knowledge base of its employees who have a need to know such information, and expressly prohibits use of the Training Materials for production or commercial purposes. Unless otherwise specified in a Service Order, the terms of this Contract will govern the Service Order. This Contract shall take precedence over any other agreements, contracts or general terms that Customer may have entered into with a Reseller as it relates to the Services and/or Training only. A Service Order is an integral part of this Contract and is fully incorporated herein.

## 3. STANDARD SUPPORT

The following terms describe WhiteHat's standard support offering. Additional support and service level agreements may be procured by Customer as described in a Service Order.

**3.1 Customer Support.** Customer may contact WhiteHat customer support using WhiteHat's Customer Support Web Portal, which will be made available to Customer during the onboarding process. From the Customer Support Web Portal, Customer will have the ability to log and track all of its service support requests. Customer will also be able to review a support portal dedicated to documentation relevant to the Services such as service manuals user guides, and other web security information. After the Effective Date of the customer's initial Service Order, Customer will receive an email from WhiteHat with a URL link to set up Customer's password for the Customer Support Web Portal. Customer may also contact customer support via email to support@whitehatsec.com or by calling (408) 343-8340 (Monday through Friday, 6:00 a.m. - 7:00 p.m. Pacific time, excluding any WhiteHat-observed holidays).

**3.2 System Upgrades.** WhiteHat may periodically schedule a maintenance window to conduct upgrades to the Services, during which the Services will not be Available. WhiteHat will use commercially reasonable efforts to inform Customer of the date, time and duration of such maintenance window at least twenty-four (24) hours in advance of the commencement of such maintenance. WhiteHat shall take into consideration minimizing the disruption to Customer's use of the Services when scheduling regular maintenance windows.

**3.3 Service Availability and Credits**

**(a) Service Uptime.** Subject to the terms of this Contract, including but not limited to Section 3.3(c), during the Term the Services for each Application or API shall be Available to Customer not less than 99.5% of the time each calendar month.

**(b) Credits.** If the Services for an Application or API are Available less than 99.5% of the time in a particular calendar month during the Term as measured by WhiteHat, and WhiteHat is unable to provide such Services via mutually agreeable alternative methods, WhiteHat will issue to Customer a credit equal to 1/(365*24) multiplied by the then-applicable subscription fee for such Application or API for each hour that the Services for such Application or API were not Available during such calendar month. Such credit will be applied against the next invoice (provided by WhiteHat or the applicable Reseller, as appropriate) for such Application or API. In order to obtain a credit under this Section 4.3(b), Customer must provide WhiteHat with written notice of its credit request that identifies the affected Application or API within fourteen (14) days after the date of an availability violation. Credits under this Section 4.3(b) are WhiteHat's sole liability, and Customer's sole and exclusive remedy, for WhiteHat's failure to meet any service uptime levels.

**(c) Exclusions.** Customer shall not receive any credits in connection with any failure or deficiency of Services availability to the extent caused by or associated with: (i) a Force Majeure Event; (ii) regularly scheduled or emergency maintenance and upgrades (including, but not limited to the system upgrades described in Section 3.2 above); (iii) any causes attributable to Customer or its contractors, (iv) software or hardware not provided or controlled by WhiteHat; and (v) outages elsewhere on the Internet, including but not limited to interruptions at any Customer or third party data center or internet service provider, that hinder Customer's access to the Services.

**4. PROPRIETARY RIGHTS**

**4.1 Applications and APIs.** Customer hereby grants WhiteHat the right to access, use, assess and test the Application(s) and/or API(s) in connection with providing Services. Customer acknowledges and agrees that WhiteHat's access and use of the Application(s) and/or API(s) to provide Services, is not subject to any "Terms of Use" or other terms or conditions that may be posted on, linked or otherwise provided with, the Application(s) and/or API(s). Customer represents that it is either the owner of the Application(s) and/or API(s) or has the authority to permit WhiteHat to provide Services. Customer shall provide WhiteHat adequate written evidence thereof upon WhiteHat's request. In the event any of the Applications and/or APIs are subject to third-party rights and any such third party files a claim against Whitehat related to the performance of the Services on such Applications and/or APIs, such action shall be considered a material breach of the Contract and WhiteHat will have the immediate right to terminate this Contract (and any active subscriptions for Services under this Contract) and seek all legal remedies available to it.

**4.2 Restrictions.** Customer shall not: (a) copy or otherwise reproduce, whether in whole or in part, the Services (or software associated therewith), Documentation, Training or Training Materials; (b) modify or create any derivative work of the Services (or software associated therewith), Documentation, Training, or Training Materials; (c) sell, rent, loan, license, sublicense, distribute, assign or otherwise transfer the Services (or software associated therewith), Documentation, Training or Training Materials; (d) cause or permit the disassembly, decompilation or reverse engineering of the Services (or software associated therewith), Documentation, Training or Training Materials, or otherwise attempt to gain access to the source code of the Services or software associated therewith; or (e) cause or permit any third party to do any of the foregoing.

**4.3 Reservation of Rights.** Each party reserves all rights not expressly granted in this Contract and no licenses are granted by either party to the other party under this Contract except as expressly stated in a Service Order, whether by implication, estoppel or otherwise. WhiteHat or its licensors own and retain all right, title and interest (including all intellectual property rights) in and to the Services, Training, Documentation, Training Materials, and associated software, as applicable, including any modifications or improvements thereof. Subject to the terms of this Contract, Customer shall own all right, title and interest to all Reports.

**5. CUSTOMER RESPONSIBILITIES.** Customer further acknowledges and agrees that (i) as between Customer and WhiteHat it is Customer's sole responsibility to update and maintain the Application(s) and/or API(s), including without limitation, fixing any security vulnerabilities; (ii) the Reports are not guaranteed to show all vulnerabilities in the Application(s) and/or API(s); (iii) it is Customer's sole responsibility to test, vet and confirm that any proposed remedial measures referenced in the Reports or otherwise referenced by WhiteHat to Customer are appropriate for Customer's purposes; and (iv) Customer's use of the Services does not render or guarantee that the Application(s)s and/or API(s) will be invulnerable or free from unauthorized access. Customer further acknowledges and agrees that Customer's use of the Services starts on the effective date of the Service Order applicable to such Services and the Customer is responsible for providing to WhiteHat all configuration data (hostnames, user accounts, API documentation, etc.) needed to perform the Services. Failure to provide configuration data does not release Customer from any responsibility in this Contract. Customer acknowledges and agrees that Customer's and its users' use of the Services and Training may be dependent upon access to telecommunications and Internet services. Customer shall be solely responsible for acquiring and maintaining all telecommunications and Internet services and other hardware and software required for its access and use of the Services and/or Training, including, without limitation, any and all costs, fees, expenses, and taxes of any kind related to the foregoing. WhiteHat shall not be responsible for any loss or corruption of data, lost communications, or any other loss or damage of any kind arising from any such telecommunications and Internet services.

[illegible]

# WHITEHAT SECURITY, INC.
# SERVICE ORDER

**Quote Number:** Q00038463

**Contract Number:** 7286528JC

**Customer Name:** Virginia Commonwealth University (VCU)

**Primary Contact Name:** Guy Broome

**Phone:** (804) 827-2072

**Email:** gmbroome@vcu.edu

**Customer Accounting Contact (Required):**

**Bill to Name:** VCU Accounts Payable

**Address:** Box 980327
Richmond, VA 23298-0327

**Phone:** (804) 828-1077

**Email:** jaholcomb@vcu.edu

## A. DESCRIPTION OF SERVICES AND PRICING:

Pursuant to this Service Order, Customer is purchasing a total of 253 Points as set forth in Table A-1 below. Each "**Point**" is equal to $400.00 in value. During the Term of this Service Order, Customer has the right to exchange each of the Points for the Services listed in Table A-2, over the remaining Term, based on the Point Value of each such Service. Customer will notify the WhiteHat on-boarding team in writing (email is acceptable) of each request to exchange the Points for Services. In the event Customer exchanges all 253 of the Points during the Term and wishes to deploy additional Services, Customer agrees to enter into a Service Order to purchase the applicable additional Points at $400 per Point.

**Table A-1**

| Description | Per Point Fee | Quantity | Fees |
|---|---|---|---|
| WhiteHat Sentinel Points (WHS-POINTS) – per Point – annual subscription | $400.00 | 253 | $101,200.00 |
| | | **Total Fees** | **$101,200.00** |

**Table A-2**

| Type of Service | Service Point Value | Service Price Value | Example Quantity | Example Total Point Value | Example Total Price Value |
|---|---|---|---|---|---|
| WhiteHat Sentinel Gold Support – annual subscription (WH-SUP-AU)<br>3 User licenses for WhiteHat Computer Based Training (WH-CBT-250) are included with Gold Support at no additional cost. | 75 | $30,000 | 1 | 75 | $30,000 |
| WhiteHat Sentinel Standard Edition – per Web Application – annual subscription | 6 | $2,400 | 5 | 30 | $12,000 |
| WhiteHat Sentinel Premium Edition – per Web Application – annual subscription | 12 | $4,800 | 4 | 48 | $19,200 |
| WhiteHat Sentinel Source Edition – Small App – per Small Source Application – annual subscription (WHS-SRC-SML) | 12 | $4,800 | 5 | 60 | $24,000 |
| WhiteHat Sentinel Source Edition – Medium App – per Medium Source Application – annual subscription (WHS-SRC-MED) | 20 | $8,000 | 1 | 20 | $8,000 |
| WhiteHat Sentinel Business Logic Assessment – per Web Application – annual subscription (WH-BIZ-LG) | 10 | $4,000 | 2 | 20 | $8,000 |

**In exchange for executing this Service Order no later than June 30, 2017, WhiteHat shall provide the above incentive pricing.**

## B. USAGE RIGHTS

Subject to the terms of the Agreement (defined below), Customer is hereby granted a license to access and use the Services and Training as identified in this Service Order for the Term (defined below), unless otherwise specified in this Service Order.

Hostnames: Customer acknowledges and agrees that (a) Customer is required to provide to WhiteHat in writing the hostnames representing the Web Application(s) to be tested by the Services, and (b) Customer may not change the hostnames that represent a given Web Application during the Term without purchasing an additional Services subscription in connection with such change.

WhiteHat Sentinel Source: At any time during the Term, if Customer is using the Services to perform scans on a Source Application that exceeds the maximum allowable Uncompressed Source File Size and the number of Lines of Code (both as measured by WhiteHat), as applicable, purchased by Customer under this Service Order for such Source Application, WhiteHat has the right to invoice Customer for the Fees applicable to the actual Uncompressed Source File Size or number of Lines of Code of such Source Application used by Customer. On such invoice, Customer will be charged the applicable incremental Fee for the licenses required to bring Customer into compliance with its actual usage for each Source Application, using the prices set forth below prorated over the remaining Term of this Service Order.

Large Source Application Annual Fee – per Source Application (WHS-SRC-LRG): $18,400 (46 Points)
Extra-Large Source Application Annual Fee – per Source Application (WHS-SRC-XLG): $33,600 (84 Points)
Double-Extra Large Source Application Annual Fee – per Source Application (WHS-SRC-XXL): $56,000 (140 Points)

Computer Based Training: Customer acknowledges and agrees that the use of Computer Based Training is subject to third party license terms and conditions ("**CBT Terms**") contained within the online training modules. In the event of a conflict between the terms of the MSSA (including this Service Order) and the CBT Terms, the terms of the MSSA will prevail, to the extent of any conflict.

**Term:** This Service Order shall continue for a period of one (1) year from the Effective Date (as defined below). Any renewal of the subscriptions purchased under this Service Order will be subject to the terms of Section O of the Special Terms and Conditions set forth in the Contract.

Customer acknowledges that for the Services to commence and for ongoing support to be provided the Customer contact information requested below must be accurately provided to WhiteHat.

| **Secondary Contact (Required)** | | **Technical Contact (If Applicable)** | |
|---|---|---|---|
| **Name:** | Dan Han | **Name:** | |
| **Title:** | Chief Information Security Officer | **Title:** | |
| **Telephone:** | (804) 828-1015 | **Telephone:** | |
| **E-mail:** | S2dhan@vcu.edu | **E-mail:** | |

## C. PAYMENT TERMS

Fees are prepaid for the Term, net 30 days after receipt of invoice. All Fees to be paid in U.S. Dollars.

## D. SERVICE TERMS

This Service Order (the "**Service Order**") is entered into as of the date of the last party to sign below ("**Effective Date**") by and between **Customer** and **WhiteHat Security, Inc.,** ("**WhiteHat**") and is subject to the terms and conditions in the contract #7286528JC – Application Vulnerability Scanner between WhiteHat and Customer dated as of the date of the last party to sign below. (the "**Contract**"). If signed below, Customer accepts that this Service Order, the Contract and any other duly executed Service Orders under the Contract constitute the entire agreement between WhiteHat and Customer governing WhiteHat's provision of Services to Customer, to the exclusion of all other terms (the "**Agreement**"). Capitalized terms used, but not defined, in this Service Order are used with the meanings ascribed to such capitalized terms in the Contract.

**This Service Order is accepted and approved as of the Effective Date.**

**WhiteHat Security, Inc.**

Signature:

Name: Garrett McGonigal

Title: Senior Contract Manager

Date: June 23, 2017

**Virginia Commonwealth University (VCU)**

Signature: Karol Kain Gray

Name: Karol Kain Gray

Title: Vice President for Finance and Budget

Date: 6/27/17

to "Step 2". This action will be repeated until the functionality is covered thoroughly and as long as the submitted request is deemed safe.

Also as part of the configuration process, the Threat Research Centre examines every link discovered by Sentinel for overall coverage and streamlines the automated assessment for safe and efficient scanning.

## NON-INVASIVE TESTING METHODOLOGY

WhiteHat Sentinel is best described as a "low and slow" scanner. Sentinel leverages single threaded requests when performing the automated assessment of the web application. Sentinel will send a request to your website and wait for a response back before submitting the next request. In addition, Sentinel is also capped at four requests per second, by default. You have the ability to control this cap within the Sentinel interface. This single threaded method of testing essentially makes Sentinel the equivalent of a single user slowly navigating the website.

Other scanners will bombard your website with hundreds if not thousands of requests simultaneously, running the risk of severely impacting or taking down the website. This is not possible with Sentinel due to this single threaded process. In the event increased response times are detected, we will proactively stop the assessment and contact you to ensure everything is running smoothly.

**WhiteHat Sentinel will not execute live code!**

By leveraging customised testing methodology unique to Sentinel in combination with the vulnerability verification process of our Threat Research Centere, Sentinel is able to detect vulnerabilities in a safe manner without having to execute live code on your web application. This separates Sentinel from other scanners out there that may execute javascript strings to find Cross-Site Scripting or live SQL queries to discover SQL Injection. You can rest assured that Sentinel will never execute real code in an automated fashion on your website. This greatly reduces the chance of negatively impacting the application.

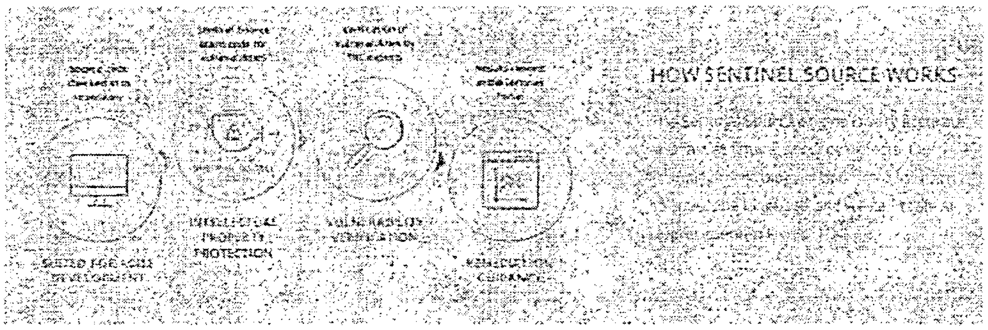
## WHITEHAT SENTINEL SOURCE – STATIC ANALYSIS

WhiteHat Sentinel Source is part of the WhiteHat Sentinel suite of vulnerability management solutions. Sentinel Source is a subscription-based Static Application Security Testing (SAST) solution, directly inspecting source code for vulnerabilities.

WhiteHat Sentinel Source directly assesses source code and gives developers accurate vulnerability data, enabling them to assess and fix code continuously throughout the software development lifecycle (SDLC). Sentinel Source includes verification of all vulnerabilities by the WhiteHat Threat Research Center (TRC).

WhiteHat SECURITY

WhiteHat Sentinel Source, when combined with WhiteHat Sentinel DAST, delivers a proven, scalable and affordable enterprise website security platform across the SDLC, reducing the risk of exposure for websites.


HOW SENTINEL SOURCE WORKS
SUITED FOR AGILE DEVELOPMENT
INTELLECTUAL PROPERTY PROTECTION
VULNERABILITY VERIFICATION
REMEDIATION GUIDANCE

## WHITEHAT SENTINEL SOURCE ADVANTAGES

WhiteHat has designed a solution from the ground up to address the unique characteristics of SAST. Source code assessment permits the discovery of vulnerabilities that are harder to detect in production, and by doing assessments in the development phase, vulnerabilities are remediated earlier.

As a SaaS based service, Sentinel Source enables continuous update of attack vectors via Rule Packs that identify and verify vulnerabilities – this ensures that developers stay up-to-date on the latest attacks.

## INTEGRATION INTO SDLC

Sentinel Source makes it easy to do ongoing assessment of code. Unlimited assessments make it easy to integrate into the normal activities during development. Code may be reviewed before it is built into an executable image. WhiteHat vulnerability data can be easily integrated into existing systems and platforms via fully supported plugins, so that development organizations' view WhiteHat Sentinel Source as an augmentation to the SDLC, rather than an obstacle.

## ACCURATE REPORTING OF VULNERABILITIES

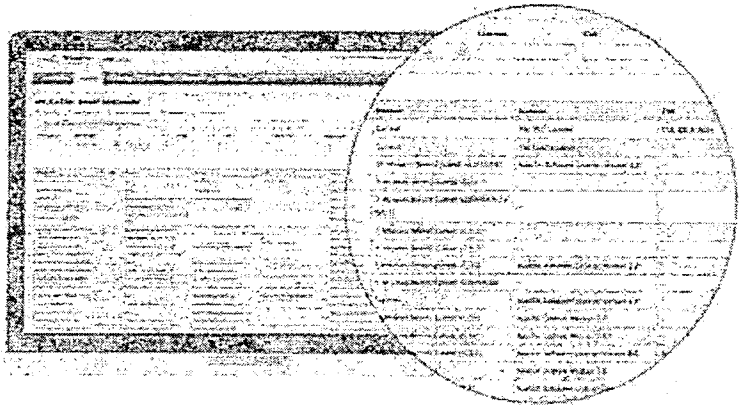
All vulnerabilities are verified and prioritized by the WhiteHat TRC. As a result, Sentinel Source enables developers to focus their efforts on fixing the most critical vulnerabilities.

WhiteHat SECURITY

## SOFTWARE COMPOSITION ANALYSIS

Software Composition Analysis (SCA) allows you to identify third-party and open source components that have been integrated into all your applications. It informs you about the licenses for each of them and identifies out-of-date libraries that should be upgraded or patched. SCA can let you know if any open-source frameworks have open CVEs that must be addressed. Click on a specific CVE and you'll be brought to MITRE page with recommendations on how to upgrade or downgrade out of a common vulnerability. Libraries written internally and used by other apps within your organization can also be tracked by SCA. The SCA report includes:

- Per application breakdown of every component that is used
- License information for each component
- Information on components that are out-of-date
- Component version and whether it's the most current
- Identification of Common Vulnerabilities and Exposures (CVEs)



## DIRECTED REMEDIATION

### How it Works

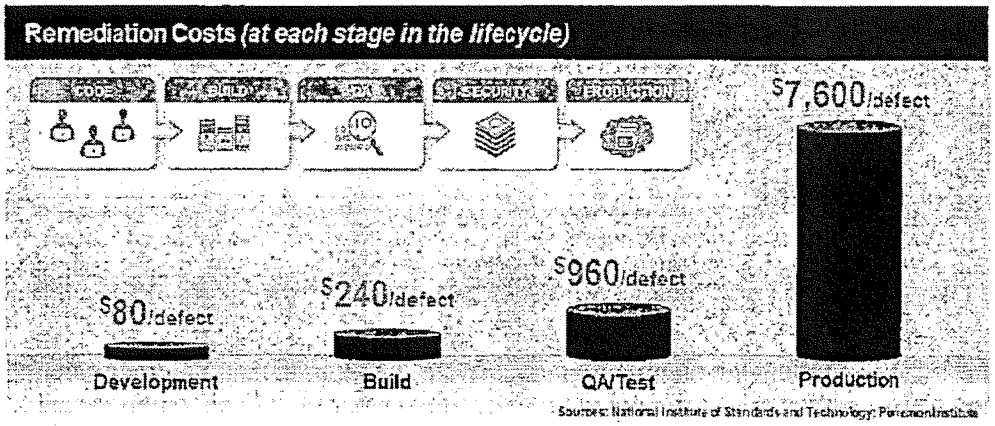
- Sentinel Source scans the entire source code and identifies security vulnerabilities.
- Sentinel Source Remediation Engine expresses a security fix using state-of-the-art algorithms utilizing positional analysis and data flow analysis and each security fix is verified by security experts in WhiteHat Security's Threat Research Center (TRC).
- The end user views the recommended security fix in Sentinel Source and chooses to apply the fix to their source
- code or to adjust the proposed solution according to their environment.
- The end user then runs a new scan and confirms that the vulnerability has been fixed.

WhiteHat
SECURITY

VCU
Virginia Commonwealth University

## LOWER COSTS

Sentinel Source is a SaaS solution, resulting in drastically lowered corporate maintenance costs and up-to-date vulnerability criteria.


Remediation Costs *(at each stage in the lifecycle)*

Sources: National Institute of Standards and Technology; Ponemon Institute

## FLEXIBILITY IN ASSESSMENTS

Sentinel Source allows for flexible assessment schedules. An assessment may be scheduled as frequently as weekly or nightly, in conjunction with a sprint, or on demand as a post-build component in a continuous integration environment.

## PRESERVATION OF INTELLECTUAL PROPERTY

Sentinel Source was designed to fit within the way organizations work. As a result, WhiteHat deploys a H/W or VM appliance at the customer's site. So, no code is removed from the network. Because assessments are done on the premises and only small code snippets are available to WhiteHat TRC engineers for verification, source code will not leave the developer's site – eliminating the possibility of IP loss or theft.

## EARLY RISK REMEDIATION

The WhiteHat Sentinel vulnerability verification process identifies real vulnerabilities, eliminating false positives. Accurate results help developers get their code right before it goes to the staging site, pushing fewer vulnerabilities onto the production website where attacks occur.

### EASE OF USE

Sentinel Source uses the same UI as all other Sentinel solutions. This common user experience significantly reduces the amount of configuration, training and management needed. Also, with a RESTful API, integration with other applications such as bug-tracking systems is simplified.

### ENHANCE DEVELOPERS SKILLS

Sentinel Source works well in agile environments and provides developers with rapid feedback, increasing their skills and productivity.

## MOBILE APPLICATION SECURITY TESTING

WhiteHat Sentinel Mobile, an industry-leading mobile application security assessment platform, has solutions for testing applications in production as well as source code reviews in development. WhiteHat employs state-of-the-art tools and mature review processes, as well as forensic investigation into the business processes and data calls each app makes. Every vulnerability found in your mobile application is verified by the TRC. WhiteHat Security offers two main forms of Mobile security assessments, **Mobile Express**, and **Sentinel Source for Mobile**. In addition to both of these, customers can purchase a Sentinel Business Logic Assessment (BLA), which is a one-time penetration test of a mobile application.

WhiteHat understands that not every organization has developers for web- and mobile-application creation alike. Often, mobile apps are outsourced to third-party vendors. In these instances, or when the source code is simply not available for other or legacy reasons, Mobile Express can scan for vulnerabilities in iOS and Android platforms, and additionally the Swift language, for developer-signed binaries. Mobile Express covers client-side testing, behavioral testing, and network testing.

When the source code is available for the mobile application, WhiteHat recommends the deeper assessment found in Sentinel Source for Mobile, source code checking using our SAST engine and methodology. Sentinel Mobile BLA covers all the testing of Mobile Express, and adds client-server interaction, business logic testing, and source code testing and evaluation with tests done on real mobile devices – not just emulators. This runtime analysis of traffic and testing is available for both Android and iOS platforms.

WhiteHat SECURITY

VCU Virginia Commonwealth University

## WHITEHAT SENTINEL CUSTOMER SUPPORT

### PLATINUM SUPPORT

Platinum support provides the highest level of a personalized support relationship with WhiteHat Security by providing both a Customer Success Manager (CSM) and giving you direct access to senior Threat Research Center (TRC) security engineers. Platinum level support also includes an annual onsite strategic process review. Platinum Support includes:

- Annual onsite strategic process review
- Quarterly vulnerability review
- Direct access to senior security engineers
- An assigned Customer Success Manager (CSM)
- Priority response times and service level agreements (SLA)
- Custom vulnerability exploit and remediation review
- 24/7/365 access to the Customer Success Center
- WhiteHat Sentinel interface training

**Annual Onsite Strategic Process Review**
WhiteHat Security will provide a senior security engineer to spend three days onsite at your facility to help your team develop and execute strategic website risk management plans tailored to your specific business environment. During an annual review, for example, strategies can be developed that enable different business stakeholders – including risk management and compliance, product management and software development teams – to share ideas with WhiteHat experts and strategize on best practices for web security.

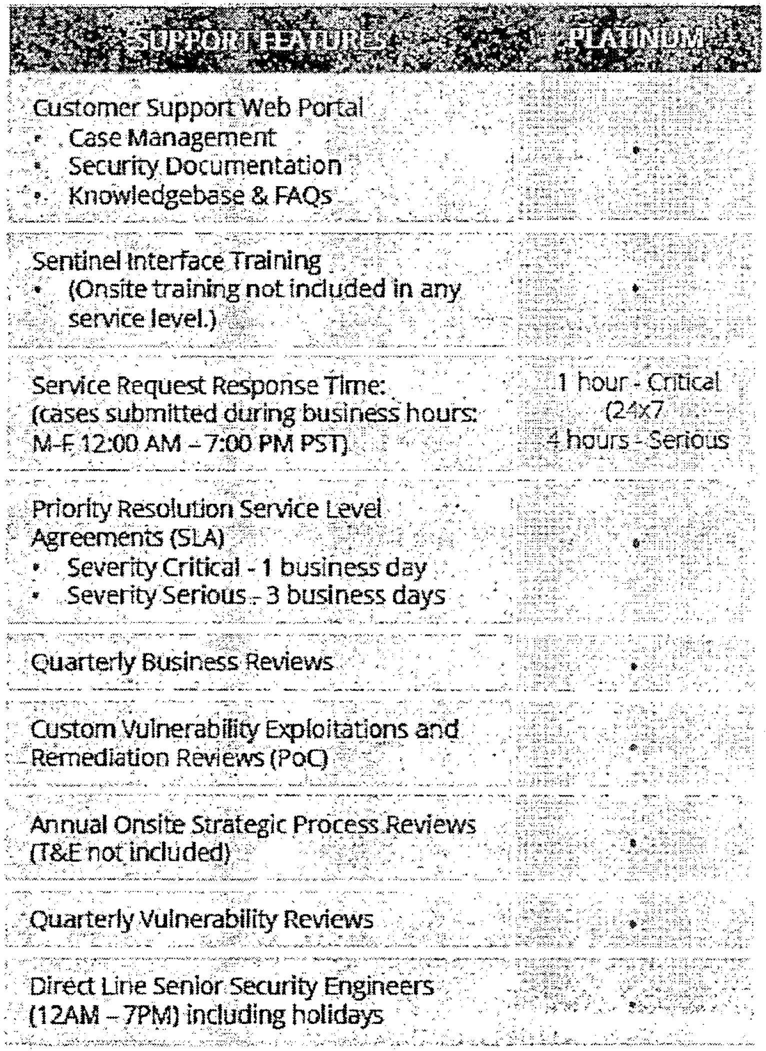
Annual Onsite Strategic Process Reviews cover:

- Vulnerability data discovered during the ongoing Sentinel assessments.
- Reports with remediation statistics and metrics.
- Mitigation techniques and security best practices.

- Overview of the current web security landscape and how it affects your organization.

**Quarterly Vulnerability Review**
Once per quarter, WhiteHat conducts a detailed review of high risk vulnerabilities discovered. The objective is to help your organization streamline the remediation process. During this review, a WhiteHat security engineer will give live demonstrations of the vulnerabilities, to show how high-risk vulnerabilities can threaten your business.

By clearly understanding how each vulnerability can be exploited and understanding the risk associated with each vulnerability, you will be able to prioritize, manage, and mitigate your website risk more effectively.



| SUPPORT FEATURES | PLATINUM |
|---|---|
| Customer Support Web Portal<br>• Case Management<br>• Security Documentation<br>• Knowledgebase & FAQs | • |
| Sentinel Interface Training<br>• (Onsite training not included in any service level.) | • |
| Service Request Response Time:<br>(cases submitted during business hours: M-F 12:00 AM – 7:00 PM PST) | 1 hour - Critical<br>(24x7<br>4 hours - Serious |
| Priority Resolution Service Level Agreements (SLA)<br>• Severity Critical - 1 business day<br>• Severity Serious - 3 business days | • |
| Quarterly Business Reviews | • |
| Custom Vulnerability Exploitations and Remediation Reviews (PoC) | • |
| Annual Onsite Strategic Process Reviews (T&E not included) | • |
| Quarterly Vulnerability Reviews | • |
| Direct Line Senior Security Engineers (12AM – 7PM) including holidays | • |

WhiteHat SECURITY

VCU Virginia Commonwealth University

Our testing process can include testing for both technical and business logic vulnerabilities. WhiteHat's TRC can perform manual custom testing to identify business logic flaws. The WhiteHat Security experts who uncover these types of vulnerabilities are capable of understanding account structures, contextual logic, and similar characteristics of Web applications. Sentinel provides support for the following types of vulnerabilities:

**Technical Vulnerabilities — WASC**

| | | |
|---|---|---|
| Application Misconfiguration | Buffer Overflow | Content Spoofing |
| Cross Site Scripting | Directory Indexing | Path Traversal |
| Fingerprinting | Format String Attack | HTTP Request Smuggling |
| HTTP Request Splitting | HTTP Response Smuggling | HTTP Response Splitting |
| Improper Filesystem Permissions | Improper Input Handling | Improper Output Handling |
| Information Leakage | Insufficient Transport Layer Protection | Integer Overflows |
| LDAP Injection | Mail Command Injection | Null Byte Injection |
| Predictable Resource Location | Remote File Inclusion | Routing Detour |
| OS Commanding | Path Traversal | SOAP Array Abuse |
| SQL Injection | SSI Injection | Server Misconfiguration |
| URL Redirector Abuse | XML Attribute Blowup | XML Entity Expansion |
| XML External Entities | XML Injection | XPath Injection |
| XQuery Injection | | |

**Technical Vulnerabilities – OWASP 10**

| | | |
|---|---|---|
| A1 - Injection | A2 - Cross Site Scripting | A4 - Insecure Direct Object References |
| A6 - Security Misconfiguration | A7 - Insecure Cryptographic Storage | A8 - Failure to Restrict URL Access |
| A9 - Insufficient Transport Layer Protection | A10 – Urvalidated Redirects and Forwards | |

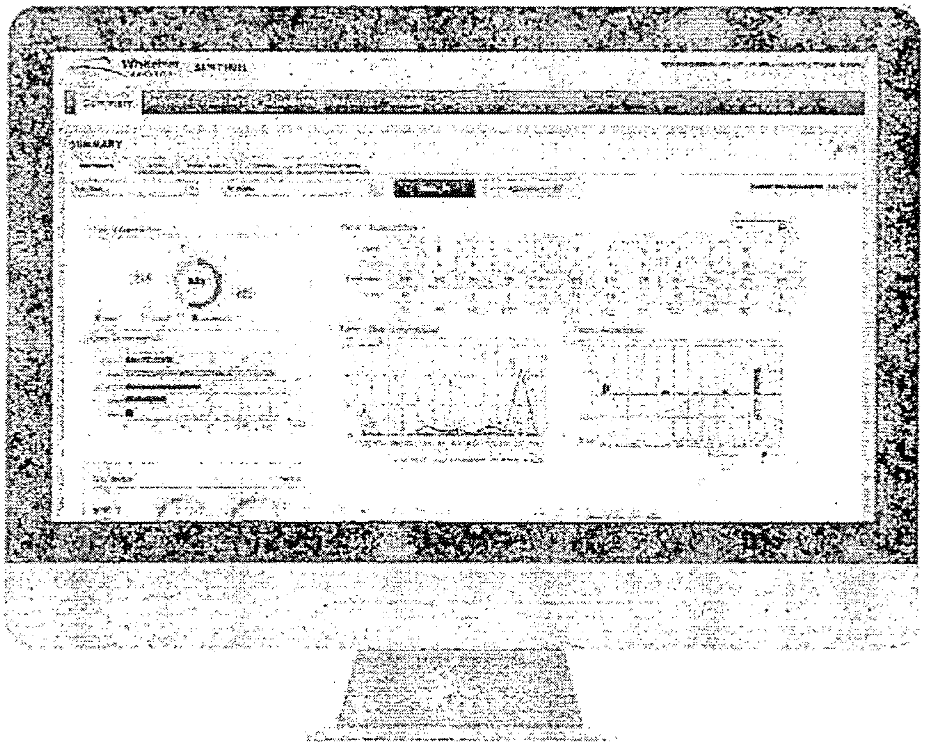
**Business Logic Flaws (including custom, manual testing by WhiteHat Security engineers)**

| | | |
|---|---|---|
| Abuse of Functionality | Brute Force | Credential/Session Prediction |
| Cross Site Request Forgery | Insecure Indexing | Insufficient Anti-automation |
| Insufficient Authentication | Insufficient Authorization | Insufficient Process Validation |
| Insufficient Password Recovery | Insufficient Session Expiration | Session Fixation |

The Sentinel solution combines highly advanced proprietary scanning technology with custom testing by the Threat Research Center (TRC), a team of website security experts who act as a critical and integral component of the WhiteHat Sentinel website vulnerability management service. Sentinel focuses the testing on the web application itself and not the platform that the application is running on. WhiteHat follows the WASC Threat Classification 2.0 for a comprehensive list of design flaws and vulnerabilities enumerated; we also associate CVSS scoring to our vulnerability data within our portal.

## DELIVERABLES & REPORTING

Detailed assessment results are available within the Sentinel platform. Users can generate CSV, PDF and HTML reports via the Sentinel interface or interactively drill into the results via the Sentinel interface. Sentinel also provides Executive Dashboard reporting in the portal, which contains trending data and aggregated vulnerability information to provide an overall view of the security posture of the entire enterprise and/or a specific application (or groups thereof). Dashboards are dynamically updated in real time and are available to users with sufficient access privileges, as provisioned by administrator users.



Sentinel also provides views in the portal and in generated reports that provide information on each vulnerability including details on the location, the exact request sent and response received during the test, a description of the vulnerability, a list of external resources for the vulnerability category and a solution to explain how to remediate the vulnerability. Sentinel can also generate specialized reports such as a PCI Compliance report. Sentinel reporting has extensive data filtering capabilities, allowing users to control which results will be included in the reports.

In addition to reporting within the WhiteHat Sentinel user portal, all WhiteHat data is supported by an open-XML API. This API can be used to extract data directly into various other systems, platforms or programs that may be utilized by clients. WhiteHat also maintains fully supported plugin integration with various IDEs, bug tracking systems, ALM tools, and other software at no additional cost to clients.

## TRAINING

WhiteHat offers both onsite and online training. The training curriculum teaches software developers and security professionals to understand and apply the principles of secure application development. WhiteHat's computer-based training (CBT) is a scalable application security training for your staff, built by application security experts. Give developers and security personnel the tools they need to meet the real-world requirements of building secure code in fast-paced production environments.
WhiteHat Sentinel computer-based training offers several important capabilities:

- A compelling, effective learning environment with high-quality animation.
- Full support for Java and .NET.
- Integration with your SCORM-compliant LMS.
- Embedded quizzes to track participation and comprehension.
- Predictable deployment – without any last minute security headaches
- Unlimited access for each participant.

## DATA COLLECTION & PROTECTION POLICY

WhiteHat Security is Safe Harbor. As a "Software-as-a-Service" vendor for web application security services, WhiteHat recognises the sensitive nature of the data collected and therefore takes every step to secure and maintain the confidentiality, integrity, and availability of our clients' vulnerability information. These include controls at the physical, network, application layer, and business controls including background checks and monitoring.

Sentinel's infrastructure is located at Quality Technology Data Centre's state of the art SAS 70 Type II, PCI DSS Level 1 compliant data center providing physical protection, monitoring, and redundancy:

- Secure building infrastructure with server rooms that are environmentally and physically independent (data center within a data center).
- N+1 Redundant power supplies, chillers, and fire suppression.

- Security guards to manage physical and electronic monitoring. Static and roving teams 24x7 with roving patrols audited by interactive confirmation system.
- Surveillance of all passageways, entrances and exits are captured on videotape and coverage retained for 90 days.
- Security zones provide segmentation for low, medium-low, medium, medium-high, and high security zones used to reduce risk of intrusion.
- Multi-level authentication methods including PIN, badges, and biometric palm scanners for access to various security zones.
- Data center employee access is based on job function and limited based on security zones. Personnel screening includes drug tests and background checks going back 7 years.

All network traffic flows through multi-purpose network appliances that provide:

- High availability data assurance, enabling one network device to take over for another if there is a failure or the device needs to be replaced.
- Network intrusion / detection - network traffic patterns are analyzed to determine if they match known attack patterns, generating a system alert and dynamically blocking network traffic that matches known attack signatures.
- Network Firewalls to allow granular control of network traffic and govern denied protocols, source and destination IPs.
- Web Application Firewalls to analyze web application traffic and dynamically block known attack patterns.

At the application layer, WhiteHat's secure Sentinel portal (over SSL) also includes detailed access control mechanisms and user management options. WhiteHat Sentinel is continually assessed for vulnerabilities. WhiteHat Security removes all assessment & account data from their systems 30 days after a contract has lapsed. All other data is retained based on the following criteria. Retain the last three completed scans for 365 days. Retain all referenced data for 7 years. Retain all data for rolling 90 days. (3 months). Data that has satisfied their required period of retention must be destroyed in an appropriate manner that protects the privacy and confidentiality of all information being destroyed. Data containing confidential and/or proprietary information must be securely maintained, controlled and protected to prevent unauthorized access. The unauthorized destruction, removal or use of any Company record(s) is prohibited and will result in sanctions. No one may falsify or inappropriately alter information in any record or document.

WhiteHat Negotiation Questions for RFP #7286528JC

Application Vulnerability Scanner

1. Please clarify the WhiteHat response to Section VI.F. Procurement Requirements. The Requirements are restated in the response to this section in the WhiteHat proposal. Does your company agree with the Procurement Requirements in Section VI.F.?
   Yes ______ No _______
   If "NO," identify the specific term and condition(s) and the reason for non-compliance.

2. Utilization of the words "should" or "may" in Section VI, Statement of Needs, Items A through E indicates a non-mandatory requirement.
   Does / Shall your company comply with the non-mandatory technical requirements as presented in Section VI, Statement of Needs, Items A through E (i.e. "should" becomes "shall")?

   Yes ______ No _______

   If "NO," identify the specific requirement and the reason for non-compliance.

3. On page 7 of the WhiteHat proposal, the information about the warranty is not clear. Is the information submitted the entire warranty? What is the reference to Section 4.3? Is there warranty/indemnification to protect VCU from any third party infringement claims? Please provide a copy of the complete warranty.

4. Confirm that the offer from WhiteHat to provide the Application Vulnerability Scanner is not expired. Does WhiteHat agree to extend the offer until June 30, 2017?

5. Small, Women-Owned and Minority-Owned Business Commitment:
   Complete and submit Appendix I of the RFP. (Attached) VCU has a 42.0% SWaM expenditure goal.

6. Invoicing and Payment:
   Complete and submit Appendix I of the RFP. (Attached)

7. Please indicate how long after the contract award your firm can commit the proposed resources to the project.

8. While VCU does have 247 Web Applications, the proposed price for the Sentinel Application Vulnerability Scanner solution is significantly over budget. At this time VCU is considering phasing in the number of Web Applications starting with the forward facing applications. Please come prepared to discuss reducing the number of applications, the DAST Pricing Weighted Average, and the size of the Web Applications. Also, it would be helpful to know what actual price differences there are between Platinum Support, Gold Support and other support offerings.

9. Is the pricing offered the most favorable pricing offered to any customer for the same volume at this particular time? What additional discounts or price breaks can be offered?

10. Please elaborate on the coverage.

11. Confirm that the Clarification Response dated March 10, 2017 is incorporated into the Negotiation Response by reference.

WhiteHat Security, Inc. (herinafter "Offeror", "Contractor", 'Prime Contractor", "Vendor" or "WhiteHat") has submitted a proposal dated January 5, 2017 ("Proposal") to VCU's Request for Proposal (RFP) for the provision of application security testing services to VCU.

VCU has engaged WhiteHat to provide the Services and/or Training (each defined in Appendix A) as further described under the Appendix A ("Service Description"), pursuant to the terms and conditions contained herein, inclusive of the Service Description (collectively the "Contract").

## XI. GENERAL TERMS AND CONDITIONS:

A. PURCHASING MANUAL: This Contract is subject to the provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and their Vendors and any revisions thereto, which are hereby incorporated into this Contract in their entirety. A copy of the manual is available for review at the VCU Procurement Services Office. In addition, the manual may be accessed electronically at http://procurement.vcu.edu/ or a copy can be obtained by calling VCU Procurement Services at (804) 828-1077.

B. APPLICABLE LAW AND COURTS: This Contract shall be governed in all respects by the laws of the Commonwealth of Virginia and any litigation with respect thereto shall be brought in the courts of the Commonwealth. The Contractor shall comply with all applicable federal, state and local laws, rules and regulations.

C. ANTI-DISCRIMINATION: By entering into this Contract, Offerors certify to the Commonwealth and to VCU that they will conform to the provisions of the Federal Civil Rights Act of 1964, as amended, as well as the Virginia Fair Employment Contracting Act of 1975, as amended, where applicable, the Virginians With Disabilities Act, the Americans With Disabilities Act and Section 2.2-4311 of the *Virginia Public Procurement Act.* If the Contract is made to a faith-based organization, the organization shall not discriminate against any recipient of goods, services, or disbursements made pursuant to the Contract on the basis of the recipient's religion, religious belief, refusal to participate in a religious practice, or on the basis of race, age, color, gender or national origin and shall be subject to the same rules as other organizations that contract with public bodies to account for the use of the funds provided; however, if the faith-based organization segregates public funds into separate accounts, only the accounts and programs funded with public funds shall be subject to audit by the public body. (*Code of Virginia*, § 2.2-4343.1).

In every Contract over $10,000 the provisions in 1. and 2. below apply:

1. During the performance of this Contract, the Contractor agrees as follows:

a) Virginia Commonwealth University is an equal opportunity/affirmative action institution providing access to education and employment without regard to age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability. As such, the Contractor will not discriminate against any employee or applicant for employment because of age, race, color, national origin, gender, religion, sexual orientation, veteran's status, political affiliation or disability or any other basis prohibited by state law related to discrimination in employment, except where there is a bona fide occupational qualification reasonably necessary to the normal operation of the Contractor. The

Contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices setting forth the provisions of this nondiscrimination clause.

b) The Contractor, in all solicitations or advertisements for employees placed by or on behalf of the Contractor, will state that such Contractor is an equal opportunity employer.

c) Notices, advertisements and solicitations placed in accordance with federal law, rule or regulation shall be deemed sufficient for the purpose of meeting these requirements.

2. The Contractor will include the provisions of 1. above in every subcontract or purchase order over $10,000, so that the provisions will be binding upon each subcontractor or vendor.

D. ETHICS IN PUBLIC CONTRACTING: By entering into this Contract, Offeror certifies that its Proposals are made without collusion or fraud and that they have not offered or received any kickbacks or inducements from any other Offeror, supplier, manufacturer or subcontractor in connection with their Proposal, and that they have not conferred on any public employee having official responsibility for this procurement transaction any payment, loan, subscription, advance, deposit of money, services or anything of more than nominal value, present or promised, unless consideration of substantially equal or greater value was exchanged.

E. IMMIGRATION REFORM AND CONTROL ACT OF 1986: By entering into this Contract, Offeror certifies that it does not and will not during the performance of this Contract employ illegal alien workers or otherwise violate the provisions of the Federal Immigration Reform and Control Act of 1986.

F. DEBARMENT STATUS: By submitting its Proposal, Offeror certifiesy that it is not currently debarred by the Commonwealth of Virginia from submitting proposals on contracts for the type of goods and/or services covered by this solicitation, nor is it an agent of any person or entity that is currently so debarred.

G. ANTITRUST: By entering into this Contract, the Contractor conveys, sells, assigns, and transfers to the Commonwealth of Virginia all rights, title and interest in and to all causes of the action it may now have or hereafter acquire under the antitrust laws of the United States and the Commonwealth of Virginia, relating to the particular goods or services purchased or acquired by the Commonwealth of Virginia under said contract.

H. CONFIDENTIALITY:

1. Definition of Confidential Information. By virtue of this Contract, the parties may have access to each other's Confidential Information. "Confidential Information" shall mean any written, machine-reproducible and/or visual materials that are clearly labeled as proprietary, confidential, or with words of similar meaning, and all information that is orally or visually disclosed, if not so marked, if it is identified as proprietary or confidential at the time of its disclosure or in a writing provided to the receiving party within thirty (30) days after disclosure. Confidential Information does not include

information that: (a) is now, or hereafter becomes, through no act or failure to act on the part of the receiving party, generally known or available to the public; (b) was acquired by the receiving party before receiving such information from the disclosing party and without restriction as to use or disclosure; (c) is hereafter rightfully furnished to the receiving party by a third party, without restriction as to use or disclosure; or (d) is information which the receiving party can document was independently developed by the receiving party without use of the disclosing party's Confidential Information.

2. Use of Confidential Information. Neither party shall disclose any of the other party's Confidential Information to any third party or use such Confidential Information for any purpose other than to (i) perform its obligations or exercise its rights under this Contract; or (ii) as otherwise required by law. Each party shall use the same measures to protect the Confidential Information of the other party as it uses with respect to its own confidential information of like importance, but in no event shall it use less than reasonable care, including, instructing its employees, vendors, agents, consultants and independent contractors of the foregoing and requiring them to be bound by appropriate confidentiality agreements. If a party is required to disclose by law the Confidential Information of the other party, such party shall use best efforts to give the other party reasonable advance notice of such required disclosure. WhiteHat reserves the right to disclose the terms and conditions of this Contract, in confidence, (a) to accountants, banks and financing sources and their advisors for the purpose of securing financing; and (b) in connection with an actual or proposed merger or acquisition or similar transaction. Upon termination or expiration of this Contract the receiving party will promptly return to the disclosing party or destroy, at the disclosing party's option, all tangible items containing or consisting of the disclosing party's Confidential Information.

## I. PAYMENT:

1. To Prime Contractor:

a) Invoices for items ordered, delivered and accepted shall be submitted by the Contractor directly to the payment address shown on the purchase order/Contract. All invoices shall show the VCU Contract number and/or purchase order number; social security number (for individual Contractors) or the federal employer identification number (for proprietorships, partnerships, and corporations).

b) Any payment terms requiring payment in less than thirty (30) days will be regarded as requiring payment thirty (30) days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than thirty (30) days, however.

c) All goods or services provided under this Contract or purchase order, that are to be paid for with public funds, shall be billed by the Contractor at the contract price, regardless of which public institution is being billed.

d) The following shall be deemed to be the date of payment: the date of postmark in all cases where payment is made by mail, or the date of offset when offset proceedings have been instituted as authorized under the Virginia Debt Collection Act.

e) Unreasonable Charges. Under certain emergency procurements and for most time and material purchases, final job costs cannot be accurately determined at the time orders are placed. In such cases, contractors should be put on notice that final payment in full is contingent on a determination of reasonableness with respect to all invoiced charges. Charges which appear to be unreasonable will be researched and challenged, and that portion of the invoice held in abeyance until a settlement can be reached. Upon determining that invoiced charges are not reasonable, VCU shall promptly notify the Contractor, in writing, as to those charges which it considers unreasonable and the basis for the determination. A Contractor may not institute legal action unless a settlement cannot be reached within thirty (30) days of notification. The provisions of this Section do not relieve VCU of its prompt payment obligations with respect to those charges that are not in dispute (Code of Virginia, § 2.2-4363).

2. To Subcontractors:

a) Contractor awarded a contract under this RFP is hereby obligated:

i. To pay the Subcontractor(s) within seven (7) days of the Contractor's receipt of payment from VCU for the proportionate share of the payment received for work performed by the Subcontractor(s) under the contract; or

ii. To notify VCU and the Subcontractor(s), in writing, of the Contractor's intention to withhold payment and the reason.

b) The Contractor is obligated to pay the Subcontractor(s) interest at the rate of one percent per month (unless otherwise provided under the terms of the contract) on all amounts owed by the Contractor that remain unpaid seven (7) days following receipt of payment from VCU, except for amounts withheld as stated in 2. above. The date of mailing of any payment by U.S. Mail is deemed to be payment to the addressee. These provisions apply to each sub-tier Contractor performing under the primary contract. A Contractor's obligation to pay an interest charge to a Subcontractor may not be construed to be an obligation of VCU.

J. <u>PRECEDENCE OF TERMS</u>: Paragraphs A-J of these General Terms and Conditions shall apply in all instances. In the event there is a conflict between any of the other General Terms and Conditions and any Special Terms and Conditions in this solicitation, the Special Terms and Conditions shall apply.

K. <u>QUALIFICATIONS OF OFFERORS</u>: VCU may make such reasonable investigations as deemed proper and necessary to determine the ability of the Offeror to perform the services/furnish the goods and the Offeror shall furnish to VCU all such information and data for this purpose as may be requested. VCU reserves the right to inspect Offeror's physical facilities prior to award to satisfy questions regarding the Offeror's capabilities. VCU further reserves the right to reject any Proposal if the evidence submitted by, or investigations of, such Offeror fails to satisfy VCU that such Offeror is properly qualified to carry out the obligations of the Contract and to provide the services and/or furnish the goods contemplated therein.

L. TESTING AND INSPECTION: VCU reserves the right to conduct any test/inspection it may deem advisable to assure goods and services conform to the specifications.

M. ASSIGNMENT OF CONTRACT: A Contract shall not be assignable by the Contractor in whole or in part without the written consent of the VCU Director of Procurement Services, except that Contractor may assign this Contract to any successor to substantially all of its business or assets to which this Contract relates, upon written notice to VCU. This Contract shall inure to the benefit of and be binding on the respective successors and assigns of the parties.

N. CHANGES TO THE CONTRACT: Changes can be made to the Contract in any one of the following ways:

1. The parties may agree in writing to modify the scope of the Contract. An increase or decrease in the price of the Contract resulting from such modification shall be agreed to by the parties as a part of their written agreement to modify the scope of the Contract.

2. The VCU Procurement Services Department may order changes within the general scope of the Contract at any time by written notice to the Contractor. Changes within the scope of the contract include, but are not limited to, things such as services to be performed, the method of packing or shipment, and the place of delivery or installation. The Contractor shall comply with the notice upon receipt. The Contractor shall be compensated for any additional costs incurred as the result of such order and shall give VCU a credit for any savings. Said compensation shall be determined by one of the following methods:

   a) By mutual agreement between the parties in writing; or

   b) By agreeing upon a unit price or using a unit price set forth in the Contract, if the work to be done can be expressed in units, and the Contractor accounts for the number of units of work performed, subject to the VCU's right to audit the Contractor's records and/or to determine the correct number of units independently; or

   c) By ordering the Contractor to proceed with the work and keep a record of all costs incurred and savings realized. A markup for overhead and profit may be allowed if provided by the Contract. The same markup shall be used for determining a decrease in price as the result of savings realized. The Contractor shall present VCU with all vouchers and records of expenses incurred and savings realized. VCU shall have the right to audit the records of the Contractor as it deems necessary to determine costs or savings. Any claim for an adjustment in price under this provision must be asserted by written notice to VCU within thirty (30) days from the date of receipt of the written order from VCU. If the parties fail to agree on an amount of adjustment, the question of an increase or decrease in the Contract price or time for performance shall be resolved in accordance with the procedures for resolving disputes provided by the Disputes Clause of this

Contract or, if there is none, in accordance with the disputes provisions of the Commonwealth of Virginia's Purchasing Manual for Institutions of Higher Education and Their Vendors. Neither the existence of a claim or a dispute resolution process, litigation or any other provision of this Contract shall excuse the Contractor from promptly complying with the changes ordered by the VCU Procurement Service Office or with the performance of the Contract generally.

O. DEFAULT: In case of failure to deliver goods or services in accordance with the Contract terms and conditions, VCU after due oral or written notice, may procure them from other sources and hold the Contractor responsible for any resulting additional purchase and administrative costs. This remedy shall be in addition to any other remedies which VCU may have in law or equity.

P. USE OF BRAND NAMES: Unless otherwise provided in this Contract, the name of a certain brand, make or manufacturer does not restrict Offerors to the specific brand, make or manufacturer named, but conveys the general style, type, character, and quality of the article desired. Any article, which the public body, in its sole discretion, determines to be the equal of that specified, considering quality, workmanship, economy of operation, and suitability for the purpose intended, shall be accepted. The Offeror is responsible to clearly and specifically identify the product being offered and to provide sufficient descriptive literature, catalog cuts and technical detail to enable VCU to determine if the product offered meets the requirements of the solicitation. This is required even if offering the exact brand, make or manufacturer specified. Unless the Offeror clearly indicates in its proposal that the product offered is an "equal" product, such proposal will be considered to offer the brand name product referenced in the RFP.

Q. TRANSPORTATION AND PACKAGING: By submitting their Proposals, all Offerors certify and warrant that the price offered for FOB Destination includes only the actual freight rate costs at the lowest and best rate and is based upon the actual weight of the goods to be shipped. Except as otherwise specified herein, standard commercial packaging, packing and shipping containers shall be used. All shipping containers shall be legibly marked or labeled on the outside with purchase order number, commodity description, and quantity. Further, Offeror shall bear the risk of loss until the goods and equipment until VCU accepts Delivery of them.

R. INSURANCE: By signing and submitting a Proposal under the RFP, the Offeror certifies that if awarded the Contract, it will have the following insurance coverages at the time the Contract is awarded. For construction contracts, if any Subcontractors are involved, the subcontractor will have workers' compensation insurance in accordance with §§ 2.2-4332 and 65.2-800 et seq. of the *Code of Virginia.* The Offeror further certifies that the Contractor and any Subcontractors will maintain these insurance coverages during the entire term of the Contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.

Minimum Insurance Coverages and Limits Required for Most Contracts:

1. Worker's Compensation - Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify VCU of increases in the number of employees that change their workers'

compensation requirements under the *Code of Virginia* during the course of the Contract shall be in noncompliance with the Contract.

2. Employers Liability - $100,000.

3. Commercial General Liability - $1,000,000 per occurrence. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. VCU must be named as an additional insured and so endorsed on the policy.

4. Automobile Liability - $1,000,000 per occurrence. (Only used if motor vehicle is to be used in the contract.)

S. Reserved.

T. DRUG-FREE WORKPLACE: During the performance of this Contract, the Contractor agrees to (i) provide a drug-free workplace for the Contractor's employees; (ii) post in conspicuous places, available to employees and applicants for employment, a statement notifying employees that the unlawful manufacture, sale, distribution, dispensation, possession, or use of a controlled substance or marijuana is prohibited in the Contractor's workplace and specifying the actions that will be taken against employees for violation of such prohibition: (iii) state in all solicitations or advertisements for employees placed by or on behalf of the Contractor that the Contractor maintains a drug-free workplace: and (iv) include the provisions of the foregoing clauses in every Subcontract or purchase order of over $10,000, so that the provisions will be binding upon each Subcontractor and/ or Vendor.

For the purposes of this section, *"drug-free workplace"* means a site for the performance of work done in connection with a specific Contract awarded to a Contractor, the employees of whom are prohibited from engaging in the unlawful manufacture, sale, distribution, dispensation, possession or use of any controlled substance or marijuana during the performance of the Contract.

U. NONDISCRIMINATION OF CONTRACTORS: A Bidder, Offeror, or Contractor shall not be discriminated against in the solicitation or award of this Contract because of race, religion, color, sex, national origin, age, disability, or against faith-based organizations or any other basis prohibited by state law relating to discrimination in employment. If the award of this Contract is made to a faith-based organization and an individual, who applies for or receives goods, services, or disbursements provided pursuant to this Contract objects to the religious character of the faith-based organization from which the individual receives or would receive the goods, services, or disbursements, the public body shall offer the individual, within a reasonable period of time after the date of his objection, access to equivalent goods, services, or disbursements from an alternative provider.

V. eVA BUSINESS-TO-GOVERNMENT VENDOR REGISTRATION, CONTRACTS, AND ORDERS: The eVA Internet electronic procurement solution, website portal www.eVA.virginia.gov, streamlines and automates government purchasing activities in VCU. The eVA portal is the gateway for vendors to conduct business with VCU Institution and other public bodies. All Vendors desiring to provide goods and/or services to VCU shall participate in the eVA Internet e-procurement solution by completing the free eVA Vendor Registration. All

Bidders or Offerors must register in eVA and pay the Vendor Transaction Fees specified below; failure to register will result in the bid/proposal being rejected.

Vendor Transaction Fees are determined by the date the original purchase order is issued and are as follows:

1. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:

   a) DSBSD-certified Small Businesses: 1%, capped at $500 per order.
   b) Businesses that are not DSBSD-certified Small Businesses: 1%, capped at $1,500 per order.

2. For orders issued July 1, 2014 the vendor transaction fees can be found at www.eVA.virginia.gov

The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Department of General Services, approximately thirty (30) days after the corresponding purchase order is issued and payable thirty (30) days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

W. FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA). The Selected Offeror/Vendor acknowledges that for the purposes of this Contract it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this Contract for University's and its students' benefit, and will not share such data with or disclose it to any third party except as provided for in this Contract, required by law, or authorized in writing by the University.

## XII. SPECIAL TERMS AND CONDITIONS:

A. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this proposal, no indication of such sales or services to Virginia Commonwealth University will be used in product literature or advertising. The Contractor shall not state in any of the advertising or product literature that the Commonwealth of Virginia or any agency or institution of the Commonwealth has purchased or uses its products or services.

B. AUDIT: The Contractor shall retain all books, records, and other documents relative to this contract for five (5) years after final payment, or until audited by the Commonwealth of Virginia, whichever is sooner. The agency, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.

C. AVAILABILITY OF FUNDS: It is understood and agreed between the parties herein that the agency shall be bound hereunder only to the extent of the funds available or which may hereafter become available for the purpose of this agreement.

D. PROPOSAL ACCEPTANCE PERIOD: Any proposal in response to this solicitation shall be valid for sixty (60) days. At the end of the sixty (60) days, the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.

E. PROPOSAL PRICES: Proposal prices shall be in the form of a firm unit price or service offering for each item during the contract period.

F. CANCELLATION OF CONTRACT: The purchasing agency reserves the right to cancel and terminate any resulting Contract, in part or in whole, without penalty, upon sixty (60) days written notice to the Contractor. In the event the initial contract period for the Services is for more than twelve (12) months, the resulting Contract may be terminated by either party, without penalty, after the initial twelve (12) months of the contract period upon 60 days written notice to the other party. Either party will have the right to terminate the resulting Contract for a material breach of the terms and conditions of such Contract by the other party ("Material Breach") that is not cured within thirty (30) days of receipt by the breaching party of a notice of such breach. Any Contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation. For clarity, Service fees are non-refundable for cancellation of the Contract during an active service subcription period, other than in connection with a termination by VCU as a result of a Material Breach. In the event VCU terminates the Contract as a result of a Material Breach, VCU may request a refund of the remaining prorated, prepaid and unused fees associated with any of VCU's then active subscriptions for Contractor Services.

G. SPECIAL EDUCATIONAL OR PROMOTIONAL DISCOUNTS: The Contractor shall extend any special educational or promotional sale prices or discounts immediately to the Commonwealth during the term of the contract. Such notice shall also advise the duration of the specific sale or discount price.

H. DRUG FREE WORKPLACE: The Contractor acknowledges and certifies that it understands that the following acts by the Contractor, its employees and/or agents performing services on state property are prohibited:

1. The unlawful manufacture, distribution, dispensing, possession or use of alcohol or other drugs; and

2. Any impairment or incapacitation from the use of alcohol or other drugs (except the use of drugs for legitimate medical purposes).

3. The Contractor further acknowledges and certifies that it understands that a violation of these prohibitions constitutes a breach of contract and may result in default action being taken by the Commonwealth in addition to any criminal penalties that may result from such conduct.

I. EXTRA CHARGES NOT ALLOWED: The proposal price shall be for complete installation ready for Commonwealth's use, and shall include all applicable freight and installation charges; extra charges will not be allowed.

J. FINAL INSPECTION: At the conclusion of the work, the Contractor shall demonstrate to the authorized owners representative that the work is fully operational and in compliance with contract specifications and codes. Any deficiencies shall be promptly and permanently corrected by the Contractor at the Contractor's sole expense prior to final acceptance of the work. For clarity, the foregoing inspection and acceptance will only apply where Contractor is providing professional services, and not to software as a service offerings provided on a subscription basis.

K. Reserved.

L. INDEMNIFICATION: Contractor agrees to indemnify, defend and hold harmless the Commonwealth of Virginia, its officers, agents, and employees from any claims, damages and actions of any kind or nature, whether at law or in equity, arising from or caused by the use of any materials, goods, or equipment of any kind or nature furnished by the Contractor/any services of any kind or nature furnished by the Contractor, provided that such liability is not attributable to the sole negligence of the using agency or to failure of the using agency to use the materials, goods, or equipment in the manner already and permanently described by the Contractor on the materials, goods, or equipment delivered, and that any intellectual property infringement indemnification is limited to third party claims and is subject to the terms below under Intellectual Property Indemnification.

**INTELLECTUAL PROPERTY INDEMNIFICATION [limit IP claims to third party only]**

Subject to the terms of this Section, WhiteHat shall, at its sole cost and expense, defend (or at its sole option settle), indemnify and hold harmless VCU and the VCUIndemnitees from and against any Claims (as defined in Appendix A).

WhiteHat's obligations of indemnification shall be subject to the following: (a) VCU shall notify WhiteHat of any such Claim promptly after it obtains knowledge of such Claim, (b) VCU shall provide WhiteHat with reasonable assistance, information, and cooperation in defending the lawsuit or proceeding, at WhiteHat's sole cost and expense, (c) VCU shall give WhiteHat full control and sole authority over the defense and settlement of such Claim, provided settlement fully releases the VCU Indemnitees and is solely for monetary damages and does not admit any liability on behalf of the VCU. Notwithstanding the foregoing, VCU may join in defense and settlement discussions directly or through counsel of VCU's choice at VCU's own cost and expense.

Following notice of a Claim or upon any facts which in WhiteHat's sole opinion are likely to give rise to such Claim, WhiteHat shall in its sole discretion and at its sole option elect to (a) procure for VCU the right to continue to use the Services or Training, at no additional cost to VCU or VCU Indemnitees, (b) replace the Services or Training so that it becomes non-infringing but functionally equivalent, (c) modify the Services or Training to avoid the alleged infringement but in a manner so that it remains functionally equivalent, or (d) terminate this Contract and provide a refund to VCU of all amounts prepaid by VCU to WhiteHat for Services or Training that have not yet been provided.

Notwithstanding anything contrary contained herein, WhiteHat shall have no obligation to indemnify, defend or hold harmless the VCU hereunder to the extent a Claim is caused by or results from: (a) VCU's combination or use of the Services or Training with software, services or products developed by VCU or other third parties, unless specifically contemplated by this Contract, (b) modification of the Services or Training by anyone other than WhiteHat or its agents without WhiteHat's express approval, (c) VCU's continued allegedly infringing activity after being notified thereof or after being provided modifications that would have avoided the alleged infringement, (d) VCU's use of the Services or Training in a manner not contemplated by this Contract, the Documentation or the Training Materials, or (e) VCU's negligence, recklessness or intentional misconduct or its failure to abide by all laws, rules, regulations or orders applicable to the Services and/or the Training.

The foregoing states the sole and exclusive liability and sole remedy of WhiteHat for any infringement of intellectual property rights.

M. LIMITATION OF LIABILITY: To the maximum extent permitted by applicable law, the Contractor will not be liable under this contract to VCU or any third party for any indirect, incidental, special or consequential damages, or damages from lost profits, revenue, data or use of the supplies, equipment and/or services delivered under this Contract or any ording document for the Services governed by this Contract. The above stated limitation of liability will not apply, however, to liability arising from: (a) personal injury or death; (b) defect or deficiency caused by willful misconduct or negligence on the part of the Contractor; or (c) circumstances where the Contract expressly provides a right to damages, indemnification or reimbursement. EXCEPT WITH RESPECT TO LIABILITY ARISING FROM (1) A PARTY'S NEGLIGENCE OR WILLFUL MISCONDUCT, (2) PROPERTY DAMAGE, OR (3) PERSONAL INJURY, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY'S AGGREGATE LIABILITY HEREUNDER FOR ANY CAUSE OF ACTION OR THEORY OF LIABILITY EXCEED THE AMOUNTS PAID BY VCU TO WHITEHAT HEREUNDER DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE DATE THE CAUSE OF ACTION AROSE. THESE LIMITATIONS ARE AN ESSENTIAL BASIS OF THE BARGAIN AND SHALL APPLY NOTWITHSTANDING ANY FAILURE OF THE ESSENTIAL PURPOSE OF ANY REMEDY.

N. PRIME CONTRACTOR RESPONSIBILITIES: The Contractor shall be responsible for completely supervising and directing the work under this contract and all subcontractors that he may utilize, using his best skill and attention. Subcontractors who perform work under this contract shall be responsible to the prime Contractor. The Contractor agrees that he is as fully responsible for the acts and omissions of his subcontractors and of persons employed by them as he is for the acts and omissions of his own employees.

O. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for four (4) successive one (1) year periods under the terms and conditions of the original contract except as stated in 1. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew should be provided approximately 60 days prior to the expiration date of each contract period:

1. If the Commonwealth elects to exercise the option to renew the contract for an additional one (1) - year period, the contract price(s) for the additional one (1) year shall not exceed the contract price(s) of the previous contract period increased/decreased by more than the percentage increase/decrease of the All Items category of the CPI-W section of the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

P. SUBCONTRACTS: No portion of the work shall be subcontracted without prior written consent of the purchasing agency. In the event that the Contractor desires to subcontract some part of the work specified herein, the Contractor shall furnish the purchasing agency the names, qualifications and experience of their proposed subcontractors. The Contractor shall, however, remain fully liable and responsible for the work to be done by its subcontractor(s) and shall assure compliance with all requirements of the contract. For clarity, VCU acknowledges that Contractor engages data centers, and consents to such engagement, as a part of Contractor's provision of Services.

Q. WARRANTY (COMMERCIAL): The Contractor agrees that the supplies or services furnished under any award resulting from this solicitation shall be covered by the warranties, as described below, and that the rights and remedies provided therein are in addition to and do not limit those available to the Commonwealth by any other clause of this solicitation.

**LIMITED SERVICE WARRANTIES.**

**Conformance with Documentation.** Contractor warrants that the Services will substantially conform in all material respects in accordance with the Documentation. VCU will provide prompt written notice of any non-conformity and provide Contractor a reasonable opportunity, not to exceed thirty (30) days, to remedy such non-conformity. Contractor may modify the Documentation in its sole discretion, provided the functionality of the Services is not materially decreased during the Term (as defined in Appendix A).

**Service Availability.** Contractor warrants that the Services will meet the requirements set forth below (Service Availability). In the event of a breach of the foregoing warranty, as VCU's sole and exclusive remedy, Contractor will provide the remedy set forth under the Service Availability and Credits section in Appendix A.

**No Viruses.** Contractor warrants that the Services and the Training do not contain any computer code that is intended to (i) disrupt, disable, harm, or otherwise impede in any manner, the operation of VCU's software, firmware, hardware, computer systems or network (sometimes referred to as "viruses" or "worms"), (ii) permit unauthorized access to VCU's network and computer systems (sometimes referred to as "traps", "access codes" or "trap door" devices), or any other similar harmful, malicious or hidden procedures, routines or mechanisms which could cause such programs to cease functioning or to damage or corrupt data, storage media, programs, equipment or communications, or otherwise interfere with VCU's operations.

**Warranty Disclaimer.** EXCEPT AS PROVIDED HEREIN, WHITEHAT PROVIDES THE SERVICES AND TRAINING "AS IS" AND MAKES NO WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, WITH RESPECT TO THE SERVICES, TRAINING, REPORTS, DOCUMENTATION, TRAINING MATERIALS OR ANY OTHER RELATED DATA, AND SPECIFICALLY DISCLAIMS ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, USEFULNESS, ANY IMPLIED WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, TITLE OR FITNESS FOR A PARTICULAR PURPOSE AND ANY CONDITION OR WARRANTY ARISING FROM COURSE OF PERFORMANCE, DEALING OR USAGE OF TRADE. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF CERTAIN WARRANTIES IN CERTAIN CIRCUMSTANCES. ACCORDINGLY, SOME OF THE LIMITATIONS SET FORTH ABOVE MAY NOT APPLY. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THE TRAINING OR TRAINING MATERIALS AS A CITATION AND/OR AS A POTENTIAL SOURCE FOR FURTHER INFORMATION DOES NOT MEAN THAT WHITEHAT ENDORSES THE INFORMATION SUCH ORGANIZATION OR WEBSITE MAY PROVIDE OR THE RECOMMENDATIONS IT MAY MAKE.

R. POLICY OF EQUAL EMPLOYMENT: Virginia Commonwealth University is an equal opportunity/affirmative action employer. Women, Minorities, persons with disabilities are encouraged to apply. The University encourages all vendors to establish and maintain a policy to insure equal opportunity employment. To that end, Offerors should submit along with their proposals, their policy of equal employment.

S. eVA BUSINESS-TO-GOVERNMENT CONTRACTS AND ORDERS: The solicitation/contract will result in purchase order(s) with the eVA transaction fee specified below assessed for each order.

1. For orders issued July 1, 2011 thru June 30, 2013, the Vendor Transaction Fee is:
   a) DSBSD-certified Small Businesses: 0.75%, Capped at $500 per order.
   b) Businesses that are not DSBSD-certified Small Businesses: 0.75%, Capped at $1,500 per order.
2. For orders issued July 1, 2013, and after, the Vendor Transaction Fee is:
   a) DSBSD-certified Small Businesses: 1%, Capped at $500 per order.
   b) Businesses that are not DSBSD-certified Small Businesses: 1%, Capped at $1,500 per order.

   The specified vendor transaction fee will be invoiced, by the Commonwealth of Virginia Department of General Services, approximately 30 days after the corresponding purchase order is issued and payable 30 days after the invoice date. Any adjustments (increases/decreases) will be handled through purchase order changes.

   The eVA Internet electronic procurement solution, website portal www.eva.virginia.gov, streamlines and automates government purchasing activities in the Commonwealth. The portal is the gateway for vendors to conduct business with state agencies and public bodies.

   Vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet e-procurement solution and agree to comply with the following: If this solicitation is for a term contract, may provide an electronic catalog (price list) or index page catalog for items awarded. The format of this electronic catalog shall conform to the eVA Catalog Interchange Format (CIF) Specification that can be accessed and downloaded from www.eVA.virginia.gov. Contractors should email Catalog or Index Page information to eVA-catalog-manager@dgs.virginia.gov.

T. GRAMM-LEACH-BLILEY ACT: The Contractor shall comply with the Act by implementing and maintaining appropriate safeguards to protect and prevent unauthorized release of student, faculty and staff nonpublic information. Nonpublic information is defined as social security numbers, or financial transactions, bank, credit and tax information.

U. DETERMINATION OF RESPONSIBILITY: The Contract will be awarded to the responsive and responsible Offeror with a Proposal, conforming to the RFP, will be most advantageous to VCU, technical and financial factors considered. A responsible Offeror is one who affirmatively demonstrates to VCU that it has adequate financial resources and the requisite capacity, capability, and facilities to perform the Contract, has a satisfactory record of performance on other comparable projects, has a satisfactory record of integrity and business ethics, and is otherwise qualified and eligible to receive award under the solicitation and laws and regulations applicable to the procurement. VCU reserves the right to investigate the capabilities of Offeror, confirm any part of the information furnished by an Offeror, and require other evidence to determine that the Offeror is responsible.

V. Reserved.

W. Reserved.

## XIII. SPECIAL TERMS AND CONDITIONS INFORMATION TECHNOLOGY:

X. QUALIFIED REPAIR PERSONNEL: All warranty or maintenance services to be performed on the items specified in this solicitation as well as any associated hardware or software shall be performed by qualified technicians properly authorized by the manufacturer to perform such services. The Commonwealth reserves the right to require proof of certification prior to award and at any time during the term of the contract.

Y. SOURCE CODE: In the event the Contractor ceases to maintain experienced staff and the resources needed to provide required software maintenance, the Commonwealth shall be entitled to have use, and duplicate for its own use, a copy of the source code and associated documentation for the software products covered by the contract. Until such time as a complete copy of such material is provided, the Commonwealth shall have exclusive right to possess all physical embodiments of such Contractor owned materials. The rights of the Commonwealth in this respect shall survive for a period of twenty years after the expiration or termination of the contract. All lease and royalty fees necessary to support this right are included in the initial license fee as contained in the pricing schedule. For clarification, the foregoing provision shall not apply to the Services provided by Contractor.

Z. SOFTWARE UPGRADES: The Commonwealth shall be entitled to any and all upgraded versions of the software covered in the contract that becomes available from the Contractor. The maximum charge for upgrade shall not exceed the total difference between the cost of the Commonwealth's current version and the price the Contractor sells or licenses the upgraded software under similar circumstances. For clarification, the foregoing provision shall not apply to the Services provided by Contractor.

AA. THIRD PARTY ACQUISITION OF SOFTWARE: The Contractor shall notify the procuring agency in writing should the intellectual property, associated business, or all of its assets be acquired by a third party. The Contractor further agrees that the Contract's terms and conditions, including any and all license rights and related services, shall not be affected by the acquisition. Prior to completion of the acquisition, the Contractor shall obtain, for the Commonwealth's benefit and deliver thereto, the assignee's agreement to fully honor the terms of the contract.

BB. TITLE OF SOFTWARE: By submitting a bid, the bidder represents and warrants that it is the sole owner of the software or, it not the owner, that it has received all legally required authorizations from the owner to license the software, has the full power to grant the rights required by this solicitation, and that neither the software nor its use in accordance with the contract will violate or infringe upon any patent, copyright, trade secret, or any other property rights of another person or organization.

CC. WARRANTY AGAINST SHUTDOWN DEVICES: The Contractor warrants that the equipment and software provided under the Contract shall not contain any lock, counter, CPU references, virus, worm, or other device capable of halting operations or erasing or altering data or programs. Contractor further warrants that neither it, nor its agents, employees, or subcontractors shall insert any shutdown device following delivery of the equipment and software.

DD. SECTION 508 COMPLIANCE: All information technology which, pursuant to this Contract, is purchased or upgraded by or for the use of any Commonwealth agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794d, the "Act"), as amended. If the Technology provided under this Contract is not in compliance with the requirements of the Act and VCU requests such compliance by Contractor in writing, Contractor agrees to make reasonable commercial efforts to modify the Technology to bring the Technology into material compliance with the Act. If requested, the Contractor must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. The requirements of this Paragraph along with the Non-Visual Access to Technology Clause shall be construed to achieve full compliance with the Information Technology Access Act, §§ 2.2-3500 through 2.2-3504 of the *Code of Virginia*.

EE. NONVISUAL ACCESS TO TECHNOLOGY: All information technology which, pursuant to this Agreement, is purchased or upgraded by or for the use of any State agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with the following nonvisual access standards from the date of purchase or upgrade until the expiration of this Agreement:

1. effective, interactive control and use of the Technology shall be readily achievable by nonvisual means;
2. the Technology equipped for nonvisual access shall be compatible with information technology used by other individuals with whom any blind or visually impaired user of the Technology interacts;
3. nonvisual access technology shall be integrated into any networks used to share communications among employees, program participants or the public; and
4. the technology for nonvisual access shall have the capability of providing equivalent access by nonvisual means to telecommunications or other interconnected network services used by persons who are not blind or visually impaired.

Compliance with the foregoing nonvisual access standards shall not be required if the head of the using agency, institution or political subdivision determines that (i) the Technology is not available with nonvisual access because the essential elements of the Technology are visual and (ii) nonvisual equivalence is not available. As of the effective date of this Contract, non-visual access to the Services (defined in Appendix A below) is not available and the essential elements of such Services are not visual; therefore, the parties agree that compliance with the standards in this Section EE is not required related to the performance of the Services.

Installation of hardware, software, or peripheral devices used for nonvisual access is not required when the Technology is being used exclusively by individuals who are not blind or visually impaired, but applications programs and underlying operating systems (including the format of the data) used for the manipulation and presentation of information shall permit the installation and effective use of nonvisual access software and peripheral devices.

If requested, the Contractor must provide a detailed explanation of how compliance with the foregoing nonvisual access standards is achieved and a validation of concept demonstration.

The requirements of this Paragraph shall be construed to achieve full compliance with the Information Technology Access Act, §§ 2.1-807 through 2.1-811 of the Code of Virginia.

FF. DATA AND INTELLECTUAL PROPERTY PROTECTION:

1. Definitions

   a. "End User" means the individuals authorized by the University to access and use the Services provided by the Selected Firm/Vendor under this agreement.

   b. "Personally Identifiable Information" includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "personal information" as defined in Virginia Code section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; "medical information" as defined in Virginia Code Section 32.1-127.1:05; "protected health information" as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.

c. "Securely Destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.

d. "Security Breach" means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store or dispose of data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.

e. "Services" means any goods or services acquired by the University of Virginia from the Selected Firm/Vendor.

f. "University Data" includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student and personnel data.

2. Rights and License in and to the University Data

The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Selected Firm/Vendor has a limited, nonexclusive license to use these data as provided in this agreement solely for the purpose of performing its obligations hereunder. This agreement does not give a party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the agreement.

3. Intellectual Property Disclosure/Rights

a. Unless expressly agreed to the contrary in writing, all goods, products, materials, documents, reports, writings, video images, photographs or papers of any nature including software or computer images prepared by Selected Firm/Vendor (or its subcontractors) for the University will not be disclosed to any other person or entity without the written permission of the University.

b. Selected Firm/Vendor warrants to the University that the University will own all rights, title and interest in any intellectual property created for the University as part of the performance of this agreement and will have full ownership and beneficial use thereof, free and clear of claims of any nature by any third party including, without limitation, copyright or patent infringement claims. Selected Firm/Vendor agrees to assign and hereby assigns all rights, title, and interest in any and all intellectual property created for the University as part of the performance of this agreement to the University, and will execute any future assignments or other documents needed for the University to document, register, or otherwise perfect such rights. Nothing in this section is, however, intended to or shall be construed to apply to existing intellectual property created or owned by the vendor that the University is licensing under this agreement. For avoidance of doubt, the University asserts no intellectual property ownership under this clause to any pre-existing intellectual property of the vendor, and seeks ownership rights only to the extent Vendor is being engaged to develop certain intellectual property as part of its services for the University.

c. Notwithstanding the foregoing, for research collaboration pursuant to subcontracts under sponsored research agreements administered by the University's Office of Sponsored Programs, intellectual property rights will be governed by the terms of the grant or contract to the University to the extent such grant or contract requires intellectual property terms to apply to subcontractors.

4. Data Privacy

a. Selected Firm/Vendor will use University Data only for the purpose of fulfilling its duties under this agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by this agreement or as otherwise required by law.

b. University Data will not be stored outside the United States without prior written consent from the University.

c. Selected Firm/Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill Selected Firm/Vendor obligations under this agreement. Selected Firm/Vendor will ensure that employees who perform work under this agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this agreement.

d. The following provision applies only if Selected Firm/Vendor will have access to the University's education records as defined under the Family Educational Rights and Privacy Act (FERPA): The Selected Firm/Vendor acknowledges that for the purposes of this agreement it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this agreement for University's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this agreement, required by law, or authorized in writing by the University.

5. Data Security

a. Selected Firm/Vendor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Selected Firm/Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Selected Firm/Vendor warrants that all electronic University Data will be encrypted in transmission (including via web interface) in accordance with industry best practices commensurate to the sensitivity of the information; such as controls outlined in the Moderate or High control baselines in the latest version of National Institute of Standards and Technology Special Publication 800-53.

b. If the Selected Firm/Vendor stores Personally Identifiable Information as part of this agreement, the Selected Firm/Vendor warrants that the information will be stored in accordance with industry best practices commensurate to the sensitivity of the information; such as controls outlined in the Moderate or High control baselines in the latest version of National Institute of Standards and Technology Special Publication 800-53.

c. Selected Firm/Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this agreement.

6. Employee Background Checks and Qualifications

Selected Firm/Vendor shall ensure that its employees who will have potential access to University Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of this agreement.

7. Data Authenticity and Integrity

Selected Firm/Vendor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. The Selected Firm will be responsible during the terms of this agreement, unless otherwise specified elsewhere in this agreement, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

8. Security Breach

a. Response. Upon becoming aware of a Security Breach, Selected Firm/Vendor will timely notify the University consistent with applicable state or federal laws, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Selected Firm/Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.

b. Liability.

1) If Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security

Breach caused by Selected Firm/vendor, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.

2) If Selected Firm/Vendor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor.

9. Response to Legal Orders, Demands or Requests for Data

a. Except as otherwise expressly prohibited by law, Selected Firm/Vendor will:

- immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Selected Firm/Vendor seeking University Data;
- consult with the University regarding its response;
- cooperate with the University's reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
- upon the University's request, provide the University with a copy of its response.

b. If the University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act) or request seeking University Data maintained by Selected Firm/Vendor, the University will promptly provide a copy to Selected Firm/Vendor. Selected Firm/Vendor will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response.

10. Data Transfer Upon Termination or Expiration

a. Upon termination or expiration of this agreement, Selected Firm/Vendor will ensure that all University Data are securely returned or destroyed as directed by the University in its sole discretion. Transfer to the University or a third party designated by the University shall occur within a reasonable period of time, and without significant interruption in service. Selected Firm/Vendor shall ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition. In the event that the University requests destruction of its data, Selected Firm/Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which the Selected Firm/Vendor might have transferred University data. The Selected Firm/Vendor agrees to provide certification of the destruction of such data to the University within a reasonable time following receipt by Selected Firm/Vendor of the request for such destruction.

b. Selected Firm/Vendor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Selected Firm/Vendor's facilities to remove and destroy University-owned assets and data. Selected Firm/Vendor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. Selected Firm/Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

11. Audits

a. The University reserves the right in its sole discretion to perform audits of Selected Firm/Vendor at the University's expense to ensure compliance with the terms of this agreement. The Selected Firm/Vendor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which the Selected Firm/Vendor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If the Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data which has been identified to the Selected Firm/Vendor as having the potential to affect the accuracy of the University's financial statements, Selected Firm/Vendor will at its expense conduct or have conducted once each calendar year a:

- American Institute of CPAs Service Organization Controls (SOC 2) Type II audit, or other security audit with audit objectives deemed sufficient by the University, which attests the Selected Firm/Vendor's data centers' security policies, procedures and controls;
- vulnerability scan of Selected Firm/Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement; and
- formal penetration test of Selected Firm/Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this agreement.

Additionally, the Selected Firm/Vendor will provide the University upon request the results, that will not compromise the security of the Selected Firm/Vendor, of the above audits and applicable high level overview of the scans and tests, and will modify its security measures within a reasonable period of time as needed based on those results in order to meet its obligations under this agreement. The University may require, at University expense, the Selected Firm/Vendor to perform additional audits and tests (not to exceed one such audit each calendar year), the results of which, that will not compromise the security of the Selected Firm/Vendor, will be provided promptly following the completion of such audits to the University.

12. Compliance

    a. Selected Firm/Vendor will comply with all applicable laws and industry standards in performing services under this agreement. Any Selected Firm/Vendor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Selected Firm/Vendor upon request.

    b. Selected Firm/Vendor warrants that the service it will provide to the University is fully compliant with relevant laws, regulations, and guidance that may be applicable to the service, such as: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.

    c. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to the Selected Firm/Vendor service provided to the University, the Selected Firm/Vendor will, upon written request, furnish proof of compliance with PCI-DSS within 10 business days of the request. For clarity, Vendor Services are not required to be PCI-DSS compliant.

13. No End User agreements

    This agreement is the entire agreement between the University (including University employees and other End Users) and the Selected Firm/Vendor. In the event that the Selected Firm/Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing, with University employees or other End Users, such agreements shall be null, void and without effect, and the terms of this agreement shall apply.

14. Survival

    The Selected Firm/Vendor's obligations under Section XIII (DATA AND INTELLECTUAL PROPERTY PROTECTION) shall survive termination of this agreement until all University Data has been returned or securely destroyed.

# APPENDIX I

## PARTICIPATION IN STATE PROCUREMENT TRANSACTIONS SMALL BUSINESSES AND BUSINESSES OWNED BY WOMEN AND MINORITIES

The following definitions will be used in completing the information contained in this Appendix.

## Definitions

- **Small business** is an independently owned and operated business 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. Nothing in this definition prevents a program, agency, institution or subdivision from complying with the qualification criteria of a specific state program or federal guideline to be in compliance with a federal grant or program.
- **Women-owned business** is 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.
- **Minority-owned business** is 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.
- **Minority Individual**: "Minority" means a person who is a citizen of the United States or a legal resident alien and who satisfies one or more of the following definitions:
    - "Asian Americans" means all persons having origins in any of the original peoples of the Far East, Southeast Asia, the Indian subcontinent, or the Pacific Islands, including but not limited to Japan, China, Vietnam, Samoa, Laos, Cambodia, Taiwan, Northern Marinas, the Philippines, U. S. territory of the Pacific, India, Pakistan, Bangladesh and Sri Lanka and who are regarded as such by the community of which these persons claim to be a part.
    - "African Americans" means all persons having origins in any of the original peoples of Africa and who are regarded as such by the community of which these persons claim to be a part.
    - "Hispanic Americans" means all persons having origins in any of the Spanish speaking peoples of Mexico, South or Central America, or the Caribbean Islands or other Spanish or Portuguese cultures and who are regarded as such by the community of which these persons claim to be a part.
    - "Native Americans" means all persons having origins in any of the original peoples of North America and who are regarded as such by the community of which these persons claim to be a part or who are recognized by a tribal organization.
    - "Eskimos and Aleuts" means all persons having origins in any of the peoples of Northern Canada, Greenland, Alaska, and Eastern Siberia and who are regarded as such in the community of which these persons claim to be a part.

## PARTICIPATION BY SMALL BUSINESSES, BUSINESSES OWNED BY WOMEN BUSINESSES OWNED BY MINORITIES

This appendix should only be completed by firms that are not Virginia Department of Small Business and Supplier Diversity (DSBSD) certified small businesses.

Offeror certifies that it will involve Small Businesses, Women-Owned Businesses, and/or Minority-Owned Businesses (SWaM) in the performance of this contract either as part of a joint venture, as a partnership, as Subcontractors or as suppliers.

VCU has an overall goal of 42% SWaM participation for all annual purchases and seeks the maximum level of participation possible from all its contractors.

List the names of the SWaM Businesses your firm intends to use and identify the direct role of these firms in the performance of the contract. State whether the firm is a Small Business (SB), Women-Owned (WO), or Minority-Owned (MO).

Name of Businesses: SB, WO, MO: Role in contract:

None

**Commitment for utilization of DSBSD SWaM Businesses:**

0 % of total contract amount that will be performed by DSBSD certified SWaM businesses.

**Identify the individual responsible for submitting SWaM reporting information to VCU:**

Name Printed: Terry Murphy

Email: terry.murphy@whitehatsec.com

Phone: 408-343-8300

Firm: White Hat Security, Inc.

Offeror understands and acknowledge that the percentages stated above represent a contractual commitment by the Offeror. Failure to achieve the percentage commitment will be considered a breach of contract and may result in contract default.

Acknowledged:
By *(Signature)*:
Name Printed: Terry Murphy
Title: CFO
Email: terry.murphy@whitehatsec.com

Note: Small, Minority and/or Women-owned business sub-contractors are required to become certified and maintain certification through the Virginia Department of Small Business and Supplier Diversity (DSBSD; http://www.sbsd.virginia.gov/swamcert.html ) to fulfill the Offeror's commitment for utilization.

## APPENDIX II
## INVOICING AND PAYMENT

Invoicing:

The Contractor shall submit a fully itemized invoice to Virginia Commonwealth University, Accounts Payable and Support Services, P. O. Box 980327, Richmond, VA 23298-0327, that, at minimum, includes the following information: the Virginia Commonwealth University purchase order number; a description of the goods or services provided; quantities; unit prices; extended prices; and total prices. Payment will be issued in accordance with the payment method selected below and with the Commonwealth of Virginia Prompt Payment Legislation.

Upon request by VCU, the Contractor shall submit invoices electronically using the Ariba Network or other e-commerce channel utilized by VCU; and agrees to comply, within reason, with any future e-commerce initiatives including, but not limited to: procurement, procurement content, sourcing or any other electronic procurement and sourcing solutions.

Questions regarding this method of invoicing should be sent to: ecommerce@vcu.edu.

Payment:

VCU Procurement Services is automating the payment process to the greatest extent possible. Contractors are encouraged to accept payment electronically through the commercial card program. Please review the payment methods described below and select one for your firm. By selecting the payment method below, Contractor acknowledges that the selected payment method is **not specific to the contract resulting from this solicitation and will apply to all payments made to the Contractor** by Virginia Commonwealth University. For example, if the Contractor has an existing contract(s) and is currently receiving payment by paper check, and the Contractor is now electing to receive payment by the commercial card, **all payments** will be made using the commercial card once the commercial card payment process is implemented for the firm.

### Payment Methods

1. **Electronically through a Wells Fargo Visa commercial card:** Payment will be made ten days (10) after receipt of a proper invoice for the amount of payment due, or ten (10) days after receipt of the goods or services, whichever is later.

It is the Contractor's responsibility to contact its banking institutions to determine any credit limit that may restrict the payment of invoices. It is the Contractor's responsibility to have its credit limit raised as necessary to facilitate the timely payment of all invoices. Invoices exceeding the Contractor's credit limit will be returned unpaid.

Failure to accept the commercial card after award of contract will be considered a contract compliance issue and will be addressed accordingly. In addition, invoices will be returned without payment until the Contractor can accept the payment through the commercial card.

Questions regarding this method of payment should be sent to commcard@vcu.edu.

2. **ACH:** Electronic payment via automated clearing house (ACH) to the vendor provided bank account of record. Payment is processed thirty (30) days after receipt of a proper invoice for the amount of payment due, or thirty (30) days after receipt of the goods or services, whichever is later. Additional information about ACH payments is available at: http://www.vcu.edu/treasury/VendorACH.htm.

**Contractor must indicate the method of payment selected:**

________ Commercial Card Payment (Wells Fargo VISA)

X Automated Clearing House (ACH)

**Invoicing and Payment Method Acknowledgement:**

Signature: Robert Stenz
Name Printed: Robert Stenz
Title: Controller
Name of Firm: WhiteHat Security
Date: May 3, 2017

Please identify the following contact information for the individual who will serve as the appropriate point of contact within your company to be contacted by VCU Accounts Payable to implement the electronic invoicing and payment processes:

Name of the individual: Mario Gonzalez
Title: Senior Accountant
Mailing address: 3970 Freedom Circle
Santa Clara, CA 95054-1204
Email address: ar@whitehatsec.com
Phone number: 408-343-8326
Fax number: