JAMES MADISON UNIVERSITY

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract No. **UCPJMU4114**

This contract entered into this 10th day of June 2014, by **AccessIT Group, Inc.** hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

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

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

PERIOD OF PERFORMANCE: From June 10, 2014 through June 9, 2017 with seven (7) one-year renewal options.

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposal # MLO-773 dated February 12, 2014:
- (a) The Statement of Needs,
- (b) The General Terms and Conditions,
- (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
- (d) Addendum No. One dated March 6, 2014;
- (e) Addendum No. Two dated March 13, 2014;

(3) The Contractor's Proposal dated March 21, 2014 and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
- (a) Negotiations Summary dated June 10, 2014.

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

CONTRACTOR:	PURCHASING AGENCY:
By: _____ (Signature)	By: _____ (Signature)
David Hark (Printed Name)	NATASHA QUEEN (Printed Name)
Title: President	Title: Buyer Senior

Rev. 10/14/09

RFP # MLO-773, Security Incident and Event Management System Negotiation Summary for AccessIT Group, Inc.

June 10, 2014

1. Contractor's pricing schedule is as follows:

    a. Years 1 – 3: See attached quote for James Madison University dated June 10, 2014.

    b. Support Options: Gold & Platinum. Pricing dependent upon configuration.

    c. McAfee Platinum Support for JMU configuration: $37,500

    d. Hardware & Software: A minimum of 40% off published price list.

    e. SIEM Support Line Items: A minimum of 9% off published price list.

    f. Software Subscription Licenses: A minimum of 25% off published price list.

2. Contractor's proposal is amended to include the following:

    a. Contractor shall waive the cost ($2,600) for one (1) James Madison University employee to attend the 4-day McAfee Security Information and Event Management (SIEM) Administration course. Date to be determined.

    b. Special Term and Condition S. *Renewal of Maintenance* within RFP # MLO-773 is hereby replaced with the following:

    RENEWAL OF MAINTENANCE: Maintenance of the hardware or software specified in the resultant contract may be renewed by the mutual written agreement of both parties for additional one-year periods, under the terms and conditions of the original contract except as noted herein. Price increases shall be negotiated at time of renewal; however, in no case shall the maintenance costs for a succeeding one-year period exceed the prior year's contract price(s) increased by more than three percent (3%).

    c. Special Term and Condition Y. *Warranty Against Shutdown Devices* within RFP # MLO-773 is hereby replaced with the following:

    WARRANTY: Except as otherwise provided herein, Contractor makes no warranty, express or implied, with regard to the Products or any third party hardware or software and expressly disclaims the implied warranties or conditions of merchantability, merchantable quality, or fitness for a particular purpose. The Commonwealth's sole recourse for warranty claims is with the manufacturer of the Product. However, Contractor agrees to pass through any third party warranty that Contractor receives from the manufacturer of the Products to the Commonwealth. The extent of any third party warranty details, terms and conditions, remedies and procedures may be expressly stated on, or packaged with, or otherwise accompany the Products.

    d. Special Term and Condition Q. *Excessive Down Time* within RFP # MLO-773 is hereby replaced with the following:

    EXCESSIVE DOWN TIME: Equipment or software furnished under this contract shall conform to the specifications set forth herein. In the event the equipment or software does not conform, the Contractor shall promptly replace the equipment or software at no charge. Such replacement shall be with new, unused product(s) of comparable quality.

e. Special Term and Condition U. *Source Code* within RFP # MLO-773 is hereby removed in its entirety.

f. All travel expenses shall be in accordance with the Commonwealth of Virginia's per diem allowance for lodging, meals, and incidentals. http://www.jmu.edu/finprocedures/4000/4215mie.shtml.

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

Attn: Matasha Owens
Company: James Madison University
Address: 752 Ott Streeet
City, St, Zip: Harrisonburg, VA 22807
Phone: 540-568-3137
E-mail: owensml@jmu.edu

Date: 6/10/2014
Expires: 6/20/2014
AITG Rep: Mike Korwek
Address: 9256 Bendix Road, Suite 306
City, St, Zip: Columbia, MD 21045
Phone: 410-782-4805
Fax: 410-558-6535
E-mail: mikek@accessitgroup.com

QTY	DESCRIPTION	LIST PRICE	UNIT PRICE	EXT PRICE
	MANUFACTURER - McAfee			
1	**ETM-6000L** *MFE INSTITUTION ELITE MFE ENTERPRISE SECURITY MANAGER 6000 APPL*	$155,993.50	$83,771.00	**$83,771.00**
3	**ETM6000ARMAL** *MFE INSTI ELITE MFE ENT SEC MGR 6000 1YR GL+ARMA 1U+*	$31,198.70	$20,974.00	**$62,922.00**
2	**ERC-2600L** *INSTI ELITE MFE EVENT RECEIVER 2600 APPL 1U+*	$44,992.50	$24,162.00	**$48,324.00**
6	**ERC2600ARMAL** *MFE INSTITUTION ELITE MFE EVENT RECEIVER 2600 1YR GL+ARMA 1U+*	$8,998.50	$6,049.00	**$36,294.00**
1	**ELM-5600L** *MFE INSTITUTION ELITE MFE ENTERPRISE LOG MANAGER 5600 APPL 1U+*	$47,994.00	$25,774.00	**$25,774.00**
3	**ELM5600ARMAL** *MFE INSTITUTION ELITE MFE ENTERPRISE LOG MANAGER 5600 1YR GL+ARMA 1U+*	$9,598.80	$6,453.00	**$19,359.00**
1	**ACE-3450L** *MFE INSTITUTION ELITE MFE ADVANCED CORRELATION ENGINE 3450*	$51,993.50	$27,921.00	**$27,921.00**
3	**ACE3450ARMAL** *MFE INSTITUTION ELITE MFE ADVANCED CORRELATION ENGINE 3450 1YR GL+ARMA 1U+*	$10,398.70	$6,991.00	**$20,973.00**
3	**GTEETM6000GIEAD-AL** *MFE GLOBAL THREAT INTELLIGENCE ENTERPRISE SECURITY MANAGER (ESM) MODULE FOR ETM6000 1:1GL*	$8,640.00	$6,000.00	**$18,000.00**
1	**PENYDM-AT (optional)** *MFE PLATINUM NA ENTERPRISE SUPPORT*	$37,500.00	$37,500.00	**$37,500.00**
1	**TRN-TCL4** *MFE SOLUTION SERVICES PRE-PAID 4 DAY TRAINING*	$2,600.00	$0.00	**$0.00**
	Shipping, Handling, and Insurance Charges (estimated) *Ground Shipping Charges*			**$750.00**
	VA State Sales Tax (6%)			**EXEMPT**
			Solution Total	**$381,588.00**

Pricing provided is all inclusive of applicable sales tax, VAT, and shipping charges. [redacted])
If James Madison University is tax exempt, please include the tax exempt certificate with the order.

PURCHASE ORDERS MAY BE FAXED TO 410-558-6535 OR E-MAILED TO mikek@accessitgroup.com

Signing this quote serves as a binding contract to allow AccessIT Group to provide products and/or services.

Signature: _____

Name: _____

Title: _____

Date: _____

PO #: _____

Terms: **Net 30**

SIEM Proposal for James Madison University

JAMES MADISON UNIVERSITY

Response to RFP #: MLO-773

March 21th, 2014

AccessIT Group, Inc.
Mike Korwek
9256 Bendix Road, Suite 306
Columbia, MD 21045
410-782-4805
mikek@accessitgroup.com
www.accessitgroup.com

McAfee Authorized Partner

AccessIT™ Security Services, Inc.

Table of Contents

I. RFP Cover Sheet

RFP # MLO-773

Issue Date: **February 12, 2014**

Title: **Security Incident and Event Management System**

Issuing Agency: ***Commonwealth of Virginia***

James Madison University

Procurement Services MSC 5720

752 Ott Street, Wine Price Bldg.

First Floor, Suite 1023

Harrisonburg, VA 22807

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

Sealed Proposals Will Be Received Until 2:30 p.m. on March 18, 2014 For Furnishing The Services Described Herein.

OPTIONAL PRE-PROPOSAL: February 27, 2014 at 2:00 p.m. Offerors are required to register for this pre-proposal conference. See *Special Term and Condition DD. Optional Pre-Proposal Conference* for more information. Offerors are encouraged to attend the optional pre-proposal.

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

All Inquiries For Information and Clarification Should Be Directed To: Matasha Owens, VCO, Buyer Senior Procurement Services, owensml@jmu.edu, 540/568-3137, (Fax) 540/568-7936 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED

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

Name and Address of Firm:

AccessIT Group, Inc.

9256 Bendix Road, Suite 306

Columbia, MD 21045

Date: 3/21/2014

Web Address: www.accessitgroup.com

By: _____
(Signature in Ink)

Name: Mike Korwek
(Please Print)

Title: Account Manager

Phone: 410-782-4805

Fax #: 410-558-6535

Email:_mikek@accessitgroup.com_____

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

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
□ YES; □ NO; ***IF YES*** ⇒⇒ □ SMALL; □ WOMAN; □ MINORITY ***IF MINORITY:*** □ AA; □ HA; □ AsA; □ NW

II. Response to Statement of Needs

A. Application Functionality:

1. Describe the design, detection, and incident response capabilities of the proposed Security Incident and Event Management System to include the ability to detect and report:

   a. Indicators of compromise

   b. Active threats with high probability of success

   c. High risk vulnerabilities

   McAfee Enterprise Security Manager (McAfee ESM) provides the speed and rich context required to identify critical threats, respond quickly, and easily address compliance requirements. Continuous global threat and enterprise risk feeds deliver adaptive and autonomous risk management, allowing remediation of threats and compliance reporting in minutes instead of hours.

   Effective security starts with real-time visibility into all activity on all systems, networks, databases, and applications. McAfee ESM enables your business with true, real-time situational awareness and the speed and scale required to identify critical threats, respond intelligently, and ensure continuous compliance monitoring. Security teams now have access to real-time, risk relevant information to obtain a stronger security posture while shortening response time.

   Advanced risk and threat detection — McAfee ESM connects evolving threat data with a real-time understanding of the risk, asset importance, and security posture throughout the enterprise. This dynamic context, combined with our highly intelligent correlation engine, provides risk scoring and threat prioritization that continually adapts to the enterprise environment. In addition, available integration with McAfee Global Threat Intelligence (GTI) and McAfee ePolicy Orchestrator (McAfee ePO) software help you detect, correlate, and remediate threats in minutes across your entire IT infrastructure.

   Policy-aware compliance management — As compliance requirements evolve, so must your SIEM. McAfee ESM makes compliance management easy with hundreds of pre-built dashboards, complete audit trails, and reports for PCI DSS, HIPAA, NERC-CIP, FISMA, GLBA, SOX, and others. Our support for the Unified Control Framework also allows you to report your policies against more than 240 global regulations and control frameworks.

   Critical facts in minutes, not hours — McAfee's highly tuned appliance can collect, process, and correlate billions of events from multiple years and keep all information available locally for immediate ad hoc queries, forensics, rules validation, and compliance.

   Global Threat Intelligence — An optional live feed of McAfee GTI IP Reputation data provides valuable, real-time information on external threats gathered from hundreds of millions of sensors around the globe, allowing you to pinpoint malicious activity on your network. Enterprise Security Manager can use the GTI IP Reputation data to quickly identify conditions where an internal host has communicated with a known bad actor.

   Decisions Based on Risk and Asset Value — Integration with McAfee Risk Advisor enables real-time risk management. Complementing the McAfee GTI assessment of external risk factors,

McAfee Risk Advisor (MRA) scores internal assets based on assigned value, providing you with an environmental risk assessment. MRA provides accurate risk scores of end points based on asset configuration, vulnerability, and deployed controls along with available countermeasure options.

The McAfee ESM correlation engine associates the external GTI threat feeds with the internal MRA risk scores to surface the events that matter to your organization, saving you time and alerting you faster to potential problems. Visual indicators show trend activity across all dashboards for an "at-a-glance" analysis.

Improved Event Management and Workflows — Automated actions let you use prioritization to manage security as risks change. For example, a watch list can be set to flag dangerous activities, such as contact with a known bad IP address. Or, you might use McAfee ePO to take a range of corrective actions: issue new configurations, implement new policies, or deploy a software update.

To enhance security operations, McAfee Enterprise Security Manager also provides integrated tools for configuration and change management, case management, and centralized management of policy – everything needed to improve workflow and facilitate daily information security operations.

2. Describe the system's intelligence analysis components, design, and capabilities.

   The McAfee ESM is the central point of event data access, administration, configuration, reporting, alerting, and policy management. The ESM is also the final repository for the McAfeeEDB, which is a high-performance embedded relational data storage engine with patented indexing technology that is scalable from small to high-volume, high-access server environments. The McAfeeEDB utilizes patented N-Tree indexing technology stands head and shoulders above any other indexing technology when it comes to satisfying SIEM/Logging requirements. Combining several patented N-Tree and SQL processes along with Circular Tables and a programmatic Internal Interface, the McAfee SIEM enables the highest performing, most responsive SIEM available. McAfeeEDB is tuned to meet the performance requirements of infrastructures that produce large amounts of log information. McAfeeEDB is designed for zero administration deployment as an embedded data manager.

3. Describe the system's incident response workflow and record keeping capabilities.

   The solution provides extensive features for forensic analysis, including: data linking; data drill-down; data pivoting; and dynamic time-correlated baselines. The McAfee SIEM console interface is fully interactive, allowing drill-down from any displayed data point to any other related data point, allowing (for example) an analyst to select a specific user and see all other event information related to that user.

   McAfee SIEM's performance and scalability also support forensic operations: all event and flow data stored locally on the ESM appliance (which typically represents months and years of data) is available for immediate and concurrent analysis, with most queries and reports completing in just seconds. The full granularity of all source data is retained over time.

   McAfee SIEM includes an internal case management feature, and can interface with external systems via standard SMTP email delivery. The McAfee SIEM Correlation Engine includes all required sub-event data to process an incident, and can be added to internal case entries for subsequent updates and tracking.

4. Describe the system's ability to publish situational awareness dashboards to various campus communities.

   The McAfee ESMi is the central point of event data access, administration, configuration, reporting, alerting, policy management. McAfee ESMi's browser-based interface provides users the ability to modify or create custom user-specific (via role based access controls) dashboards using a drag-n-drop wizard allowing users to define query filters, sorting and content. This wizard process is highly interactive and as users craft their view, the data is displayed instantly. Each dashboard template can be modified using custom filtering; Combining tabular & graphical elements; Customer grouping, columns and colors.

5. Describe the system's ability to work in an environment that offloads and/or front-ends the processing, storage, and/or analysis of less critical intelligence on resources other than the SIEM.

   The McAfee SIEM is capable of working with industry standard front-end processors, such as Syslog-NG or OSSIM. Some customers choose to manage the volume of event data by filtering or selectively forwarding only specific events from such a front-end to the SIEM. All standard "syslog" style events can be pre-processed in this manner.

6. Describe log and event data storage accessible in real-time at production speeds. Identify timeframes (*e.g. 60 days, 90 days*).

   McAfeeEDB is capable of performing queries, counts, and analytics on large data stores (1 billion+ records), even under load (50,000 new insertions per second), and still return results in under a second.

   The amount of log and event storage available depends on the sizing of ESM and ELM devices proposed for JMU. The McAfee solution is scalable to meet any needs, from as little as 30 days, to as much as 5 years of online or raw log storage.

7. Describe the ability to configure variable archive times for log and event data of different types or originating from different sources.

   Logs and events can be archived in two ways: Raw logs are retained using McAfee ELM; while parsed and normalized events in McAfee ESM may also be archived for long term retention.

   McAfee ELM retains logs using storage "pools." Pools are logical storage volumes defined to retain logs based on either the total storage volume and/or the length of time the logs need to be retained. A single storage pool can consist of multiple physical storage volumes, including local appliance HDD, CIFS, NFS, and/or SAN storage locations. Each pool can have different retention periods from 1 day to 99 years.

   McAfee ESM appliances include local HDD storage arrays that are used to store parsed and normalized logs and events within a partitioned database. The database may be backed up entirely, or by partition, allowing flexible backup and storage options. In addition, database partitions may be saved directly to external DAS, CIFS, NFS or SAN mount points. This option keeps the data available for analysis from the McAfee SIEM interface without having to move it back to the local McAfee ESM drives.

8. Describe system's capability to use external storage for long term archive with ability to access from and/or re-import into SIEM to be used in data analysis and investigations.

Please reference our response to the previous requirement.

9. Describe the system's ability to monitor and accept intelligence data from:

   a. Logs and events from all IT data center servers (*All layers – e.g. OS, database, web, application*).

      McAfee SIEM supports a wide range of information sources including Antivirus, Application, Authentication, Database, Firewall, Host Server Operating Systems, IDS/IPS, Mainframe, Network switches and routers, Protocols, Security Appliances, UTM, Virtual Private Network, VPN, Vulnerability Systems/VA, Web Content Filters and Proxy Servers.

      Please reference Appendix A – McAfee ESM Integration List Feb 2014 for a full list of supported products/applications and their associated collection methods.

   b. Logs from all firewalls, IDS/IPS devices, data center routers and switches, Internet, core routers, 1000 employee endpoints (*e.g. windows desktop event log information*).

      All are supported. Please reference Appendix A – McAfee ESM Integration List Feb 2014 for a full list of supported products/applications and their associated collection methods.

   c. Logs from a network management system monitoring employee switches indicating CAM table overloads, ARP poisoning, MAC address changes, or DHCP security activation.

      McAfee would need to review the specific log format for these products, and possibly develop parsing rules to accommodate these events. Customers can also create such rules via the built-in Rules Creation wizard, using industry standard Regex commands.

   d. Network traffic intelligence on Internet links, inside IT Data Centers, and on Core Campus routers with depth of knowledge equivalent to layer 4 or higher (*e.g. Netflow or layer 7 deep inspection*).

      The McAfee Event Receiver (ERC) has the ability to accept NetFlow v5, v7, and v9 as well as sFlow and jFlow from platforms that can generate this. In addition, an Event Receiver can, using a SPAN port, perform native flow collection "off the wire" and create/manage flow records that are equivalent to IPFIX. All flow records, whether collected from 3rd party sources and/or natively collected can be correlated/viewed within the ESM management interface.

10. Describe the system's ability to accept, understand, and process all critical intelligence types as identified in Section II, Background. Include OSSEC file/ registry integrity and change reports from windows and linux clients, Oracle Middleware Audit Framework, Application ASCII log files, Nessus vulnerability scanner, DNS (*Bind and Bluecat*) , DHCP (*ISC and Bluecat*), web and application servers (*including Apache, IIS, Tomcat, Oracle, and PeopleSoft*), and Windows event logs (*including those associated with process, Applocker, and SACL auditing on high risk endpoints*).

    McAfee SIEM supports a wide range of information sources including Antivirus, Application, Authentication, Database, Firewall, Host Server Operating Systems, IDS/IPS, Mainframe, Network switches and routers, Protocols, Security Appliances, UTM, Virtual Private Network, VPNA, Vulnerability Systems/VA, Web Content Filters and Proxy Servers.

Please reference Appendix A – McAfee ESM Integration List Feb 2014 for a full list of supported products/applications and their associated collection methods.

11. Describe the system's ability to incorporate and correlate identity and role information in decision making processes allowing emphasis on high risk accounts and assets with information which may be obtained from Active Directory, Oracle Internet Director, Cisco NAC, IPAM, and SCCM.

    Many data sources, such as Windows servers and AD, provide user and/or group information which will be parsed and stored in the event data fields. These fields are fully available to all functions within the product, including filtering, correlation, alarming, and Risk analysis.

12. Describe the system's ability to extract and correlate authentication transaction information through all layers including those that result in IP address changes and proxy accounts. This includes:

    > authentication services (*e.g. Active Directory, Oracle Virtual Directory, Oracle Internet Directory, and Safenet*), middleware and infrastructure (*e.g. Oracle Access Manager, Oracle Adaptive Access Manager, shibboleth, Microsoft federation(possible future), Oracle federation (possible future), SSLVPN, F5, reverse proxies, wireless access points, and NAC)* and applications (*e.g. PeopleSoft app/web/proxy servers, Exchange RPC/OWA/O365, and SharePoint/sharepoint365*).

    As long as the sourcing components provide the SIEM with information regarding authentication (user, host, IP), the solution extracts and store those items, and will provide correlation across all sources.

13. Describe the system's ability to configure and write rules that can query resources outside the SIEM (*e.g. whitelists, databases, and directories*) for information to supplement a detected event and have the SIEM alter response accordingly.

    McAfee SIEM offers a graphical drag-n-drop user interface to quickly and easily create custom correlation rules from scratch or by using one of the 170+ default rules as a template. Correlation rules can be created using any of the 60+ elements McAfee SIEM indexes individually or in combination, as well as utilizing Time, Date, Data Source (specific or Type) and severity. Additional contextual elements such as Event Threshold, Monitored Time Range and Group By are available.

14. Describe the system's ability to consume reputation intelligence from internal and external sources.

    The McAfee Global Threat Intelligence feed is available to customers on a subscription basis. This feed is compiled by McAfee Labs using over 25 Million endpoints worldwide. An API for external threat feeds is available for the GTI integration.

    McAfee SIEM provides direct linkages to many external sources, such as Bugtrak, ICE, CVE, DataStorm, MSDB and others. Vulnerability data is also used from many tools (McAfee/Foundstone, Tenable Nessus, Rapid7, etc.) to link known issues to events.

15. Describe the system's ability to write custom intelligence parsing routines and classify and correlate them (*e.g. custom device log formats, custom data structures, custom events*). Include ability to write custom rules and algorithms with granular whitelist capabilities.

The solution includes both Rules Creation and Correlation Editor functions within the product, and allows the customer to create custom parsing rules or correlation rules in a GUI-driven interface. Custom parsing rules are primarily Regex based, with a complete interface provided to assist in their creation. Correlation rules are logic driven, created with the visual GUI. Complex logic is provided for visual representation of Boolean entries (and/or/not), gates, timing and firing sequences, variables, thresholds, and more.

The system also includes an extensive Watchlist structure for the creation of custom white or black lists, and methodologies for automated updates through hands-off enrichments.

16. Describe the system's ability to cooperatively work with a preprocessing infrastructure providing custom intelligence events.

    As mentioned above in #15, the solution includes a very flexible group of interfaces that allow for the creation of unique rules. The customer may need to develop some of these rules internally, or can optionally ask for McAfee's assistance.

17. Describe system data analysis, search, query, and reporting capabilities.

    The McAfee ESM provides a high speed interactive dashboard with an integrated extensive Boolean based filter panel for ad-hoc log/event/flow searches and the ability to perform custom ad-hoc queries within any of the dashboard views. Various default dashboard views from complex incident views to customizable event analysis views where fields/columns/sorting can be customized are available for filtered searches. Each and every data visualization is constructed from data queried against more than 60+ separate indexes providing the fastest and most relevant subset of data for any given forensic or compliance context based search.

    The McAfee ELM provides a search interface for complex regular expressions.

18. Describe support for flexible automated notifications, dashboards, and reporting as well as incident handling workflow.

    McAfee ESM provides a fully-featured alerting function. Wide ranges of alerting mechanisms are supported out-of-the-box, including:

    - Display a visual alert in the ESM console
    - Play a sound from the ESM console
    - Create a case in the ESM internal case management system
    - Create a case in Remedy
    - Update a watch list with data as needed
    - Generate a custom report
    - Send an email message
    - Send an SMS message, via email-to-SMS gateways
    - Take action on the end point via McAfee ePO
    - Take action on the network via McAfee NSM
    - Execute a custom script

    Reporting and alerting can be automated to complement processes that address workflow automation. This includes identifying and notifying appropriate user groups defined by the administrator.

19. Describe the system's capacity to handle growth in events and network flows. Specify the

percentage growth without an increase in cost.

McAfee SIEM appliances are designed to expand as the log collection needs of the organization evolve. Several ESM, Event Receiver, and ELM appliance models are available; each rated by performance and scale. For smaller networks, combination appliances are also available, which combine ESM, Event Receiver, and/or ELM functions into a single appliance. For larger networks, appliances may be distributed horizontally (adding new appliances to handle increased collection needs), or hierarchically (adding 'tiers' of appliances in a 'manager-of-managers' configuration). This flexibility allows the architecture to grow with the organization's needs, while maintaining a common and familiar user interface.

Please note: McAfee SIEM licensing is by appliance, Events Per Second (EPS), and is not restricted to or licensed by number of users, end-systems, log sources or device types. Therefore, each proposed configuration is sized based upon a customer's individual requirements and anticipated EPS rates of the log sources initially integrated today, as well as future growth expectations.

20. Describe the system's capability for 100% growth in three (3) years with modular component additions.

    The McAfee SIEM can be expanded substantially with the addition of Event Receivers and ELM components to handle more than 100% growth in three years. Sizing of the primary manager, the ESM device, should be carefully planned to provide growth of this level without requiring a replacement or upgrade. Modular downstream devices, such as Event Receivers or ELM log managers, can be added at any time in the future to accommodate rapid growth.

21. Describe the system's ability to utilize and/or import stored activity and event logs from Oracle databases. Describe ability to work with the Oracle Middleware Audit Framework.

    McAfee SIEM supports Oracle through the acquisition of audit logs or through the optionally available McAfee DEM. Quoting this optional appliance would require additional scoping of JMU's requirement for interfacing with external databases, and therefore is not included in the Section VIII (Proposed Cost).

    The McAfee DEM passively monitors database activity by tracking, analyzing and logging all database activity on the network (or directly on a database server via an optional agent). McAfee DEM can detect data access violations, anomalies, and other risk behavior in addition to providing a full audit trail of all database sessions.

22. Describe the system's ability to interface with external threat intelligence sources (*e.g. dns blacklists, spam blacklists, web site reputation systems*) provided by your firm or others and any associated costs. Indicate how your firm's product would make use of such information.

    McAfee Global Threat Intelligence for Enterprise Security Manager puts the power of McAfee Labs directly into the security monitoring flow through the high-speed, highly intelligent McAfee SIEM, which is built for Big Security Data. This optional subscription service continually delivers and adjusts source reputations for more than 140 million IP addresses, bringing the context of external system reputations directly into the security event stream and quickly identifying current and past interactions with known bad actors. McAfee Global Threat Intelligence (McAfee GTI™) IP reputation is derived from the correlation of threat intelligence from all major threat vectors, leveraging more than 100 million global sensors and more than 350 researchers. Annual subscription pricing has been provided for GTI in Section VIII (Proposed

Cost).

McAfee SIEM also provides direct linkages to many external sources, such as Bugtrak, ICE, CVE, DataStorm, MSDB and others. Vulnerability data is also used from many tools (McAfee/Foundstone, Tenable Nessus, Rapid7, etc.) to link known issues to events.

23. Describe any network connections between provided components, agents, or connectors that are not authenticated and encrypted.

    There are none. McAfee SIEM encrypts communications between all components. AES-256 bit is used between appliances and SSL/TLS is used between the browser based interface and the ESM.

24. Describe any network communications between provided components and outside vendors. State their purpose, content of data transferred, connection direction, and protocols involved.

    The McAfee SIEM ESM manager device will communicate to our centralized Rules Update Server, at the customers selected time interval, to receive parsing rule updates. This process uses port 80. An alternative, manual update method is also available.

    Optionally, the customer may elect to connect the ESM to our service technicians with a remote VPN tunnel on Port 443. This is a secure, controlled support capability that can be enabled or disabled at the customer's discretion.

25. Describe storage capacity for log, event, and network traffic data. Differentiate between storage of raw, unaltered data as received from sources and modified formats as applicable.

    Storage capacity for parsed event data:

Appliance Hardware	Qty	Collection Rate	Analytic Performance	Local Storage
ETM-5600	1	60,000 EPS	Less than 3 minutes	8TB

    Storage capacity for raw logs:

Appliance Hardware	Qty	Collection Rate	Analytic Performance	Local Storage
ELM-5600	1	50,000 EPS	N/A	8TB

26. Describe the proposed solution's ability to archive historical log, event, and network traffic data both within the proposed solution storage and external storage. Describe ability to use the proposed solution's reporting and analysis tools to access on-board and off-board archived event and traffic data.

    Events collected by McAfee ESM are parsed, indexed, normalized and stored on the appliance for fast access and analytics.

    For McAfee ESM, archives saved via a properly configured network mount point do not need to be restored to local appliance storage, as they may be directly searched or analyzed by the McAfee SIEM over the network. Archives may also be restored to local appliance storage if desired, via a restoration process performed within the McAfee ESM console.

    Logs collected by McAfee ELM are stored in the original raw log format, as received from the data source.

For McAfee ELM, log storage is maintained as the final repository and does not require restoration. The McAfee ELM stores event logs in a secure, compressed (user definable) and digitally-signed manner to ensure chain of custody and non-repudiation. To check the integrity of these logs, there is an Integrity Check option within the ELM that allows administrators to check an individual event or the entire system, and anything in between, to ensure the logs are in their original state.

27. Describe the ability to query your data storage with external tools for log entries, events, network traffic, and/or incident records.

    The McAfee ESM, which stores the parsed event data, uses a filter dialog which allows users to type, copy-n-paste, or pick from a list, search criteria from any of the 60+ elements that McAfee SIEM tracks for each event. McAfee ESM does not require regular expression or query language to search for event data.

    With the use of McAfee ELM, users can search the ELM database via the McAfee SIEM console using regex or string matches. The ESM indexes where the ELM files are located and can retrieve raw logs when needed versus having to go through a separate ELM query engine.

28. Based on storage capacity and the JMU environment, provide estimated log, event, and network traffic storage lifetime of the proposed solution.

    Based on anticipated volumes, the ESM will provide approximately 260 days of storage, while the ELM is anticipated to provide approximately 330+ days of storage.

29. Describe in detail licensing and pricing model. Include price boundaries for number of event sources, traffic flows, event volume, accounts, users, identities, roles, API connections, CPUs, cores, collectors, and/or any other parameter affecting price. State whether figures for events and flows are peak or average and if the latter, over what time period. Specify any costs in *Section X, Pricing Schedule* of this solicitation.

    McAfee SIEM licensing is by appliance, Event Per Second (EPS), and is not restricted to or licensed by number of users, end-systems, log sources or device types. Therefore, each proposed configuration is sized based upon a customer's individual requirements and anticipated EPS rates of the log sources initially integrated today, as well as future growth expectations.

    All costs have been provided in Section VIII (Proposed Cost).

30. Provide definitions for an event, an event source, a flow, and a flow source.

    An event: An event record is the database entry consisting of fields parsed from the raw data. We store all aggregated event records in the McAfeeEDB data store for rapid searching, filtering and reporting.

    We also provide optional raw data storage when using the ELM Enterprise Log Manager devices. These devices store the un-aggregated event data source record in its original format (or as close as possible) for more granular forensics research.

    An event source: The device or application from which you are collecting an event. Event source examples include, but are not limited to, Antivirus, Application, Authentication, Database, Firewall, Host Server Operating Systems, IDS/IPS, Mainframe, Network switches and routers, Protocols, Security Appliances, UTM, Virtual Private Network, VPN, Vulnerability Systems/VA,

Web Content Filters and Proxy Servers.

A flow: A flow record is the database entry derived from parsing Netflow/Jflow/Sflow data as it arrives from flow sources. Flow records include source and destination addresses, ports, time duration, byte counts, and more, depending on version.

A flow source: Flow sources typically include switches and routers, but other network devices may also be capable of creating them.

Specify the impact, if any, on pricing, licensing, or resource limits of accepting events, logs, or other data from the following sources:

a. A Symantec management server forwarding client malware detection activity.

   No impact other than required inclusion in the Events Per Second calculations.

b. An Identity Finder management server forwarding client sensitive data scan results.

   No impact other than required inclusion in the Events Per Second calculations. Custom rules may be needed.

c. An SCCM desktop management server forwarding client patching and configuration activity.

   No impact other than required inclusion in the Events Per Second calculations.

d. An OSSEC management server forwarding file integrity information about monitored servers.

   No impact other than required inclusion in the Events Per Second calculations.

e. Nessus server forwarding client and server vulnerability information

   No impact, and does not factor in to the EPS calculation.

f. A database query tool running on an external system performing database queries across related databases (*e.g. on multiple Oracle Identity Management components*) and forwarding consolidated results to SIEM as a custom event.

   No impact other than required inclusion in the Events Per Second calculations. Custom rules may be needed.

g. A Windows event collector forwarding selected audit events from high risk endpoints.

   No impact other than required inclusion in the Events Per Second calculations.

31. Describe the ability to interface with external ticketing systems explaining the methods of integration and any product specific integration capabilities.

    McAfee ESM is capable of interacting with external case and workflow systems. McAfee ESM uses SMTP to interact with these systems and has integrated with BMC's Remedy, FrontRange Heat, Service Now, and several others.

32. Describe the ability to support LDAPS authentication and LDAP group authorization for accounts used to access the SIEM by security staff, administrators, support staff, management, etc.

    McAfee SIEM supports Active Directory and RADIUS for authentication. McAfee SIEM also supports Active Directory Users and Group filtering for Views, Reports and Correlation Rules.

33. Specify the primary user interface for security staff, administrators, support staff, management, etc. (*e.g. HTML web browser, web browser with Flash, web browser with java, web browser with ActiveX control, standalone java client, standalone windows client, X session*). Provide interface requirements (*e.g. browsers supported, OS supported, requirements for Java, Flash, or other add-on software*).

    McAfee SIEM uses a browser-based, Flash enabled interface that allows administrators to access the system from anywhere in the world. The following are the minimum system requirements for McAfee SIEM when managing the McAfee ESM via the web client:

    - OS Windows 2000 SP4/XP SP2/2003 Server SP1/Vista SP1/2008 Server/Version 7 Linux (SuSe 10, Mandrake 10.2, or Fedora Core 5 recommended) Mac (limited testing on OS 9.2.2 and OS X 10.4.10)
    - CPU: P4, 2Ghz
    - RAM: 1.5 GB
    - Resolution: 1024 x 768
    - Browser:
        - IE 7.x or later
        - Firefox 3.0 or later
        - Chrome 12.0.742.91 or later
    - Flash Player: 11.2.x.x or later

34. Provide line item pricing in *Section X, Pricing Schedule* of this solicitation for all hardware, software, licenses, and other solution components. Indicate which can be purchased independently of others (*e.g. layer 7 deep packet inspection components, interfaces with external ticketing systems, interfaces with external reputation systems*). Specify what data and calculations were used to arrive at the proposed solution size and licensing.

    The core of the proposed McAfee SIEM solution is the McAfee Enterprise Security Manager (ETM-5600). The ETM browser-based user interface provides complete configuration and management for all McAfee SIEM components. This includes all device configurations, policy configuration and tuning, event management, reporting, analysis, and other relevant functions. The log management function will be covered by a single McAfee Enterprise Log Manager (ELM-5600) appliance to support raw log storage and retention requirements. The collection of logs from data sources is provided by the McAfee Event Receiver (2xERC-2600). The McAfee Advanced Correlation Engine (ACE-3450) will provide dedicated correlation logic to support real time or historic correlation.

    McAfee utilized the data provided in the RFP documents (i.e., *RFP # MLO-773.doc*, *Summary of IT infrastructure.pdf*, and *Addendum No. One - 773.pdf*) to arrive at the proposed solution.

    All costs have been provided in Section VIII (Proposed Cost).

35. Provide line item pricing for additional hardware, software, license, and other necessary components to increase capacity 100% should JMU determine, in its sole discretion, to do so. Specify what data and calculations were used to arrive at the proposed solution size and licensing.

No additional line item pricing is needed for 100% growth. McAfee has already scoped the bill of materials contained in the Proposed Cost section (Section VIII) with 100% growth in mind.

McAfee utilized the data provided in the RFP documents (i.e., *RFP # MLO-773.doc*, *Summary of IT infrastructure.pdf*, and *Addendum No. One - 773.pdf*) to arrive at the proposed solution.

All costs have been provided in Section VIII (Proposed Cost).

The core of the proposed McAfee SIEM solution is the McAfee Enterprise Security Manager (ETM-5600). The ETM browser-based user interface provides complete configuration and management for all McAfee SIEM components. This includes all device configurations, policy configuration and tuning, event management, reporting, analysis, and other relevant functions. The log management function will be covered by a single McAfee Enterprise Log Manager (ELM-5600) appliance to support raw log storage and retention requirements. The collection of logs from data sources is provided by the McAfee Event Receiver (2 x ERC-2600). The McAfee Advanced Correlation Engine (ACE-3450) will provide dedicate correlation logic to support real time or historic correlation.

36. Describe your firm's ability to provide an online demonstration environment for the proposed products to aid in assessment. Provide access information and describe the environment and the data feeding it.

    McAfee is willing to negotiate a proof of concept/evaluation agreement period in order for JMU to fully and thoroughly test the McAfee SIEM solution. A POC scoping session will determine the type/model number of hardware required. McAfee will provide the hardware for the POC.

37. Provide electronic copies of available product documentation including installation guides, user guides, administrator guides, APIs, integration guides, tuning guides, release notes, etc. or web site account and link where they can be downloaded.

    McAfee will provide access to solution documentation during the product trial period. The McAfee ESM GUI provides access to on-line help for the User Guide. This is augmented by electronic versions of the McAfee ESM User Guide, Device Install Guide, and Quick Start Guide being available via the customer support portal.

38. Provide access to vendor and product knowledgebase. If unavailable, knowledgebase articles, whitepapers, support data and similar resources describing performance tuning and limitations, performance, integration methods, most common support calls, and most commonly requested event sources that are not supported.

    McAfee will provide access to support and product knowledgebase documentation during the product demonstration period.

39. Describe the training options and include a catalog of training offerings and their associated costs. Response should include differentiation between technical staff and end-user training.

    Although it is not a formal requirement in JMU's RFP document, AccessIT Group and McAfee strongly recommend a professional services package to assist with the initial installation, implementation, and knowledge transfer for the proposed McAfee SIEM solution. McAfee Professional Services provides a combined team of certified project managers, architects and security experts that deliver comprehensive shared best practices, expert insight, streamlined operations, and tools focused on comprehensive protection while maximizing return on

investment. The proposed professional services package would include the following:

Part Number	Part Description	List Price ($ USD)
MD-SMALL-DEPLOY	McAfee Solution Services Small Deployment Consulting	$17,000.00

The McAfee Professional Services methodology includes alignment in a six-step lifecycle:

- Strategize – Identify strategic objectives, set priorities, and build an approach for implementation
- Plan – Create an efficient and feasible roadmap for successfully meeting your company's business objectives
- Design – Architect your security business process, infrastructure, and operational requirements
- Implement – Install, configure, and deploy your McAfee proven security solution
- Operate – Execute your security operations and remediation plan
- Optimize – Streamline and enhance your systems through tuning and deployment of additional functionality

Also, the McAfee Security Information and Event Management (SIEM) Administration course from McAfee University provides attendees (technical staff and end-user) with formal hands-on training on the setup, configuration, communication flow, and data source management of McAfee SIEM (McAfee SIEM/NitroSecurity appliances). In addition, attendees will understand how to effectively implement the appliances in a complex Enterprise environment. This is a 4-day course that covers the following:

Course Outline	
Day One	
Module 1	SIEM Overview
Module 2	ESM & Receiver Overview
Module 3	ESMI Views
Module 4	Receiver Data Source Configuration
Day Two	
Module 5	Aggregation
Module 6	Policy Editor
Module 7	Correlation
Day Three	

Module 8	Alarms and Watchlists
Module 9	SIEM Workflow
Module 10	Reporting
Day Four	
Module 11	Working with ELM
Module 12	Troubleshooting and System Management.

The cost of the above outlined 4-day course is $2600.00 per attendee at a McAfee designated location, plus any additional Time & Expense charges that the student may incur if the course is not local to James Madison University.

The McAfee Training department also now offers an independent self-guided "eLearning course" on Security Information and Event Management Essentials.

All costs have been provided in Section VIII (Proposed Cost).

40. Describe the support options available through your company including on-going support of the application. Describe what portions of support to be performed by IT, the customer versus the vendor.

All support will be provided directly by the manufacturer and not through AccessIT Group.

The McAfee Gold Support option provides for the following core capabilities:

- 24x7x365 Support
- Product updates & upgrades
- Analysis on latest malware trends
- Support Notification Service (SNS)
- Service Portal
- Remote Assistance
- Knowledge Base
- Online Tutorials
- Online Product Evaluation (Global Solutions Lab)
- Major Languages Support
- Support with tiered escalations per Gold Response Charter

McAfee Platinum Support option expands on their Gold Support program by offering:

- Direct access to specialists for all your products
- Enhanced escalation strategy
- Enhanced SMS alerting services
- Authorized contacts (10)
- Named Support Account Manager
- Product planning and protection analysis
- Regular case and business reviews

- Risk assessments
- Technical onsite visits
- Emergency on-site assistance (up to 2)

Each support plan is an annual contract and is inclusive of the features and services listed above.

41. JMU is interested in developing a strategic relationship with the successful vendor. Provide information regarding ideas on how such a relationship can prove mutually beneficial.

    AccessIT Group (AITG) is mutually committed to an ongoing, strategic relationship with James Madison University. AITG has years of experience working with various universities and colleges of all sizes from New York to Southern Virginia, and can serve as a highly resourceful sounding board in numerous facets of information security as JMU develops and defines strategic IT security plans, projects, and roadmaps in future years. In turn, a relationship with an organization as large and prestigious as James Madison University would be welcomed into our higher education customer portfolio, and would only help to strengthen our position as a highly specialized and even further diversified security provider & reseller in the mid-Atlantic region.

    McAfee is also committed to JMU for a long term partnership. This partnership would include the following: a dedicated Sales Account Executive, a dedicated SIEM Specialist, a dedicated SIEM Sales Engineer, along with world-class Global McAfee ESM Support and their Professional Service team. McAfee's dedicated team is committed to providing you the best solution to address your current SIEM requirements as well as future needs and growth. The McAfee team will demonstrate a partnership approach throughout your vendor selection process along with setting up numerous calls with the team to further understand your sizing and architecture along with offering additional onsite meetings/discussions. McAfee also offers JMU the opportunity to participate in their Advisory Council that will enable JMU to provide input to McAfee's engineering teams for future product enhancements.

42. Describe active user groups and how they function.

    McAfee's annual FOCUS Security Conference offers their customers and partners a one-of-a-kind opportunity to exchange ideas with other members of the McAfee community and gain valuable knowledge to implement their security initiatives. More information can be found at http://www.mcafeefocus.com/.

    Also, the McAfee Community enables you to connect with other customers to learn and share solutions about McAfee products. Community members can post discussions, form user groups, share documents, and write blog posts.

    Visit the McAfee Community at http://community.mcafee.com.

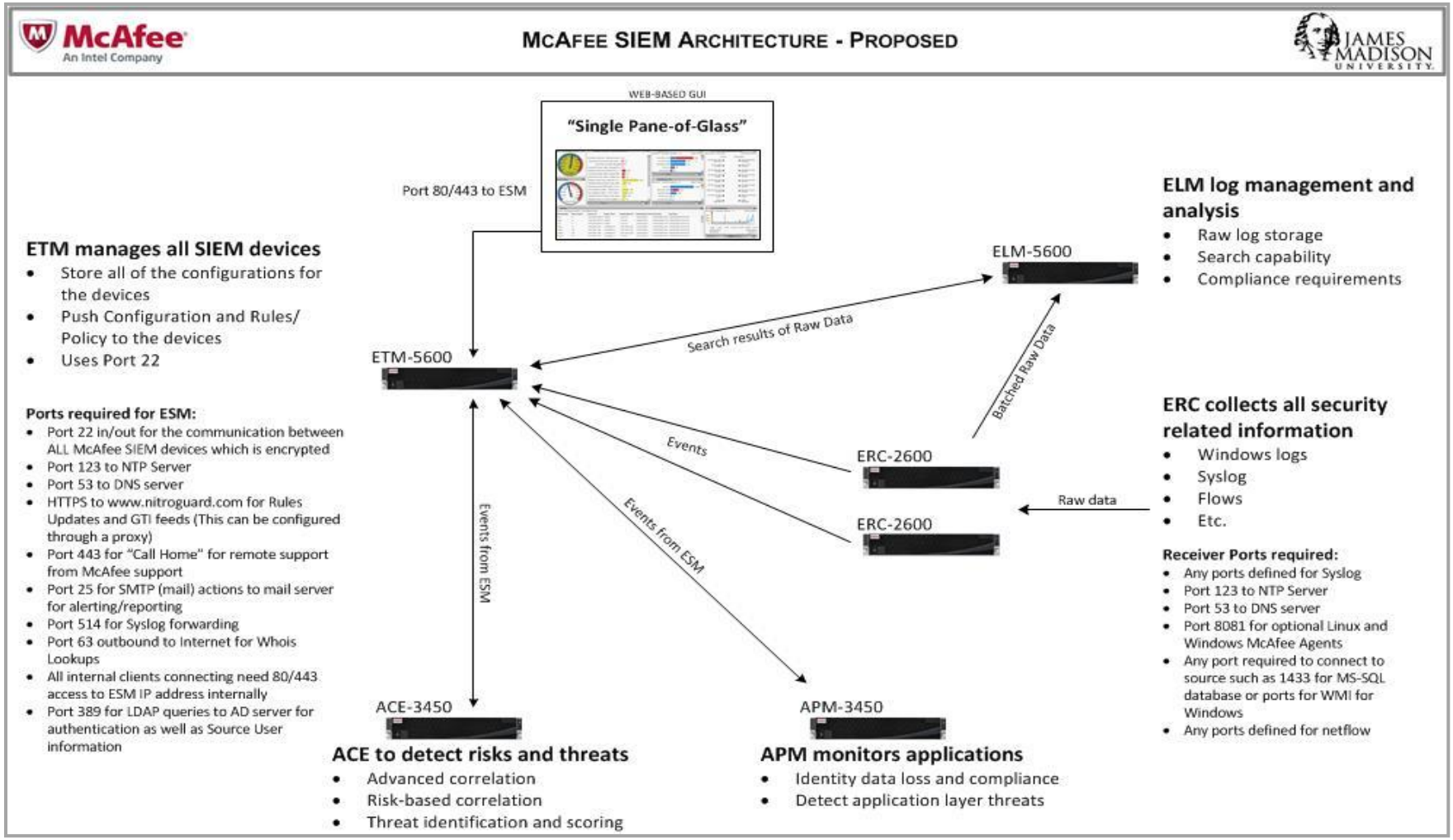
    Finally, the McAfee Global Customer Advocacy program provides our top customers with assistance in certain circumstances that focus on critical situation management, risk avoidance as well as consulting within McAfee to improve the overall customer experience by providing additional opportunities for direct access to some of McAfee's top resources and management.

43. Provide your privacy statement.

    The McAfee Privacy Policy (Appendix C) outlines how McAfee collects, uses, and discloses your personal information. You will also find information on how you can update your account and preferences, as well as details on how we protect your personal information.

B. Technical:

1. Provide a detailed diagram of the typical architecture/technical environment required for the system. List all protocols and ports used for communications and indicate which components are clients and which are servers and whether the communications are fully, partially, or not encrypted. Specify any communications paths where unencrypted authentication or other sensitive data are passed. List all third party dependent integration points and data paths including any web content included from or sent to outside parties.



2. Describe the toolset from which your application is derived.

   McAfee SIEM system appliances are built using a custom security hardened Linux distribution, on purpose built hardware.

3. Describe hardware and software requirements for the proposed system(s) along with any sizing assumptions made to arrive at those requirements.

   The core of the proposed McAfee SIEM solution is the McAfee Enterprise Security Manager (ETM-5600). The ETM browser-based user interface provides complete configuration and management for all McAfee SIEM components. This includes all device configurations, policy configuration and tuning, event management, reporting, analysis, and other relevant functions. The log management function will be covered by a single McAfee Enterprise Log Manager (ELM-5600) to support raw log storage and retention requirements. The collection of logs from data sources is provided by the McAfee Event Receiver (2x ERC-2600). The McAfee Advanced Correlation Engine (ACE-3450) will provide dedicated correlation logic to support real time or historic correlation.

   Optionally available is the McAfee Application Data Monitor (APM-3450) for application session analysis/monitoring.

   The collection tier will support up to 24K EPS allowing for growth beyond the stated events rate. The ETM-5600 will support up to 60K EPS which will allow for growth and data from the ERC appliances. With this proposed solution, if the collection tier needs to expand there is still capacity on the ETM-5600 to accommodate future growth.

   Below is our recommended solution:

Appliance Hardware	Qty	Collection Rate	Analytic Performance	Local Storage
ETM-5600	1	60,000 EPS	Less than 3 minutes	8TB
ERC-2600	2	12,000 EPS	N/A	1.8TB
ELM-5600	1	50,000 EPS	N/A	8TB
ACE-3450 (optional)		100,000 EPS	N/A	1.8TB
APM-3450 (optional)		1 Gbps	N/A	1TB

4. Describe supported server hardware and/or virtualized platforms. Describe support for the following operating systems: Linux and Windows. If virtualization is supported, what virtualization technologies are supported including what components can be virtualized?

   The McAfee solution is provided on two platforms: Appliance-based on varied sized Intel secure servers, or as ESX/ESXi compatible VMs in various sizes. All components of the solution are VM ready.

   The proposed McAfee SIEM appliance solution is built using a self-contained, hardened Linux distribution on purpose built hardware. JMU does not need to provide an open operating system for either of the McAfee SIEM deployment options.

5. Describe support for load balancing and system failover including any and all vendor specific preferences. Also include any vendor specific configuration guides.

The current solution requires the allocation of sources to specific Event Receivers, or to Event Receiver HA pairs. Migration utilities are provided to shift sources as required to balance collection loading. The current solution does not provide load balancing today, but this feature is planned for a future release.

The system provides multiple levels of redundancy and high availability. The McAfee ESM can be deployed in a redundant geo diverse pair with continuous data sync between the devices. At the collector level, the McAfee Event Receiver can be deployed in an HA pair. The McAfee ELM can write the raw log data to multiple geo-diverse locations (mirrored pools).

In addition, McAfee Event Receivers cache event and flow data locally to ensure uninterrupted data collection in the event that there is a network failure between the Event Receiver and one or more ESM appliances.

Finally, the appliances themselves are built for reliability, using redundant power, as well as dedicated drive arrays for data collection and for operating system files.

6. Describe how scalability is accomplished as the criticality of the system(s) and number of users increase.

   McAfee SIEM appliances are designed to expand as the log collection needs of the organization evolve. Several ESM, Event Receiver, and ELM appliance models are available; each rated by performance and scale. McAfee SIEM appliances may be distributed horizontally (adding new appliances to handle increased collection needs), or hierarchically (adding 'tiers' of appliances in a 'manager-of-managers' configuration). This flexibility allows the architecture to grow with the organization's needs, while maintaining a common and familiar user interface.

7. Describe the system capabilities and options for the backup and restoration of the system components (*example: database*)

   McAfee ESM can perform scheduled backups and store the backups locally or on CIFS, NFS or SAN installation. The backups are full and incremental and can be defined by the administrator. These backups can be the log data and/or the system configuration. If a restore is ever required, the process is simply to upload an existing backup to that appliance through the ESM UI and then simply click on the restore button.

   For backup of raw logs retained using McAfee ELM, any network-attached third-party storage architecture is supported, including automated storage backups.

8. Describe any standard and proprietary APIs, integration/connection resources, and development languages and tools that extend your toolset.

   McAfee is working on an API, planned for a future release, which will cover the following:

   - Queries
   - Watchlists
   - Users
   - Notifications
   - Data sources

- Importing

9. Describe requirements for application servers. Describe specific platform recommendations or requirements for certified configuration *(e.g. WebLogic, and Apache Tomcat);* include either specific application server version or required J2EE version.

   Not required with the proposed McAfee SIEM solution.

10. Describe support for web servers *(i.e. Apache, Weblogic and IIS).*

    Not required with the proposed McAfee SIEM solution.

11. Describe the supported database platforms including versions and include any information on additional features required of the DBMS needed to support the functionality of your system as proposed.

    Not applicable. McAfee ESM is a self-contained appliance which stores all event data in its McAfeeEDB. The McAfeeEDB is a purpose built, multi-partition, multi-threaded, simultaneous query database. It is self-maintaining and uses a patented indexing system. Customers do not have to create custom indexes to access any data from any event across any time period.

12. Describe your SLA to stay current with versions of software utilized by your product.

    McAfee maintains active support for the current shipping version of its code as well as one prior release to ensure broad-spectrum coverage of all support-eligible appliance products and to provide multiple avenues for resolving any identified support or security requirements using a viable code upgrade. Enhancements or bug fixes tied to meeting or maintaining advertised functionality purchased by our customers is back-ported into each of the three release versions supported at any given time to minimize the requirement for major release version changes on the part of the customer if an issue cannot be addressed with simple reconfiguration, tuning, or a targeted local patch. In all cases, McAfee will endeavor to provide minimally-invasive workarounds or resolution for support and security purposes; in all cases, we will collaborate with supported customers to assist with balancing change management program requirements against the need to maintain and/or restore system functionality in the event of a problem.

13. Describe support for real-time access to data through some other method (*e.g. on-the-fly access to database through ODBC, ADO, JDBC, LDAP, etc. allowing dynamic web content and applications).*

    McAfee has a planned release for an API interface that utilizes SOAP to provide query access for internally stored event data.

14. Describe storage including file formats.

    The McAfeeEDB (Embedded DataBase) and its internal file formats and table definitions are considered proprietary information.

C. Maintenance and Support:

Because consistency and stability of the operating environment and rapid correction of system failures are critical to James Madison University, major consideration will be given to the amount and extent of hardware and software maintenance coverage and to the quality of maintenance.

1. Describe services that may be required in the normal course of operating the system that are not covered under the maintenance contract.

   Typical routine maintenance items would include:

   - The addition/change/deletion of data sources as the customers environment changes
   - Creation or modifications of alarms, reports, watchlists, or other customer specific entries
   - Periodic checks of SIEM system logs
   - Other corrective processes if needed

2. Describe the maintenance costs for the first year, and, on the basis of an annually renewable contract, the maintenance costs for each of the following five (5) years.

Part Number	Year 1 Cost ($ USD)	Year 2 Cost ($ USD)	Year 3 Cost ($ USD)	Year 4 Cost ($ USD)	Year 5 Cost ($ USD)	Year 6 Cost ($ USD)
ETM5600ARMAL	$13109.00	$13109.00	$13109.00	$13109.00	$13109.00	$13109.00
ERC2600ARMAL	$8193.00	$8193.00	$8193.00	$8193.00	$8193.00	$8193.00
ELM5600ARMAL	$8739.00	$8739.00	$8739.00	$8739.00	$8739.00	$8739.00
ACE3450ARMAL (optional)	$9467.00	$9467.00	$9467.00	$9467.00	$9467.00	$9467.00
APM3450ARMAL (optional)	$4697.00	$4697.00	$4697.00	$4697.00	$4697.00	$4697.00
GTEETM5600GIEAD (optional)	$3345.00	$3345.00	$3345.00	$3345.00	$3345.00	$3345.00
TOTAL Required Components	**$30041.00**	**$30041.00**	**$30041.00**	**$30041.00**	**$30041.00**	**$30041.00**
TOTAL All Components (includes optional items)	**$47550.00**	**$47550.00**	**$47550.00**	**$47550.00**	**$47550.00**	**$47550.00**

*Please Note that Year 1 maintenance costs are listed as actual costs, whereas outyear annual costs are shown the same as Year 1 costs. JMU should assume that outyear maintenance costs may increase, on average, between 1-5% per annum.

All applicable Year 1 costs have been provided in Section VIII (Proposed Cost).

3. Describe the procedures for obtaining services for all types of maintenance *(e.g.*

installation of corrective code, enhancements, applicable "escalation" procedures for providing additional assistance in diagnosing a failure that is not resolved in a timely manner to include notification procedures and timing as well as what higher levels of assistance will be made available.)

Please reference Appendix B – McAfee Gold Support Handbook for detailed information on support plan coverage and escalation procedures.

4. Describe procedure for handling upgrades. Specify how often upgrades are made to the application software and how "patches" and "fixes" to the systems are handled. Describe if and how your product impacts our ability to apply security updates in a timely manner to underlying or supporting products *(e.g. Windows, Linux, Java, Oracle, MS Office, Web server).* Timely is defined as no later than 30 days from the time of vendor release.

   McAfee Support has an automated rules update server, as well as well-established procedures for providing patches and updates to closed networks, referencing our extensive work with federal agencies as well as with critical energy facilities. McAfee SIEM incorporates a "single .tar file for all OS and software upgrades" so that upgrades can be completed once and tested once. All upgrades are downloaded and handled through the McAfee ESM GUI by JMU technical staff.

   On average, there have been 1-2 major releases per year with 2-4 maintenance releases per year for the McAfee SIEM solution.

   The McAfee SIEM solution does not impact your ability to apply security updates in a timely manner to underlying or supporting products.

5. Describe the nature of system enhancements in development that are scheduled for release in the next twelve months.

   McAfee product roadmap information is considered highly confidential technical information. Under a Non-Disclosure Agreement or should McAfee be selected for award, we would welcome the opportunity to provide an interactive, in-depth presentation regarding McAfee's long and short-term plans for the solution(s) proposed in this response.

6. Describe all responsibilities of both the contractor and James Madison University in the isolation and diagnosis of system failures.

   Please reference Appendix B – McAfee Gold Support Handbook for detailed information on support plan coverage and escalation procedures.

7. Describe your "escalation" procedure.

   Please reference Appendix B – McAfee Gold Support Handbook for detailed information on support plan coverage and escalation procedures.

D. <u>Trialing:</u>

1. JMU may perform a thirty (30) or sixty (60) day production evaluation on proposed products selected at the sole discretion of the University. Notified Offerors shall provide the proposed products and solutions to JMU for evaluation and testing. JMU will install

the proposed products and direct full production data streams to it. JMU will attempt to implement test scenarios to assess ability of the solution to meet JMU needs. Test scenarios may be conducted on the following: event detection and noise reduction, behavior detection, correlation, analysis, reporting/dashboard, and other miscellaneous items. Specify all components that will be needed by JMU for implementation of a complete evaluation and production solution and provide delivery timeframes. Time is of the essence. Specify any components not provided in your proposal (*e.g. hardware, operating systems, licenses*) that are needed for full evaluation and implementation.

McAfee is willing to negotiate a proof of concept/evaluation agreement period in order for JMU to fully and thoroughly test the McAfee SIEM solution. A POC scoping session will determine the type/model number of hardware required. McAfee will provide the hardware for the POC.

2. Describe in detail how JMU can explore the performance and proper sizing of the solution during trialing of selected products at the sole discretion of the University. Describe system statistics, counters, logs, and/or other system tools that can be used to measure resource utilization, event rates, flow rates, dropped events and flows, license limits, headroom, etc.

   McAfee is willing to negotiate a proof of concept/evaluation agreement period in order for JMU to fully and thoroughly test the McAfee SIEM solution. A POC scoping session will determine the type/model number of hardware required. McAfee will provide the hardware for the POC.

III. Offeror Expertise and Qualifications

AccessIT Group is a highly specialized and focused IT security and infrastructure technologies provider in the mid-Atlantic region. Our organization has been in business for over 13 years, and we specialize in services ranging from security policy and solution design, to security solution installation and implementation. We provide enterprise level products and services for both regional and global companies, and our engineers maintain the highest level of certification for the products and services we provide.

At AccessIT Group, our mission is to enable our clients to have full confidence that their IT security infrastructure will provide them with uninterrupted business continuity and productivity. From design and implementation to IT security compliance and training, we provide our clients with a single point of contact for all their security needs.

AccessIT Group is recommending McAfee's Enterprise Security Manager (ESM) SIEM for James Madison University's Security Incident and Event Management System RFP. McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

On November 30th, 2011, McAfee completed the acquisition of privately-owned NitroSecurity, a leading provider of security information and event management (SIEM) solutions that provide complete visibility and situational awareness to protect critical information and infrastructure. NitroSecurity has been providing SIEM solutions since 2006. The McAfee SIEM (formerly NitroSecurity) is ranked as a leader in the 2013 Gartner Magic Quadrant for SIEM, and develops and utilizes the industry's fastest analytical tools to identify, correlate, and remediate information security threats in minutes instead of hours.

This acquisition has brought together best-in-class technologies:

- NitroSecurity's leadership position in the SIEM market helps McAfee significantly expand our Risk and Compliance and Global Threat Intelligence capabilities.
- NitroSecurity's SIEM management, which has already passed integration testing with McAfee ePolicy Orchestrator (ePO), gives customers a single security platform for event analysis and management across the environment. The integration expands the capability of the McAfee ePO platform to view events, activity and logs created by networks, databases and applications.
- The McAfee ePO platform can leverage the extended SIEM capabilities to more rapidly institute a range of monitoring and mitigation actions, such as issuing new configurations, implementing new policies and deploying more recent software updates.

AccessIT Group and McAfee generally do not assign or release resumes during the RFP process. The primary reason is that technical resources cannot be scheduled/allocated until JMU decides to move

forward with the trialing period, or if professional services are purchased in tandem with the hardware and respective support. As such, here is a sample resume of a typical McAfee SIEM pre and post-sales support engineer that support the McAfee SIEM solution:

- Experience in implementation of security products with an emphasis on security network information event management (SIEM), log management, IDS/IPS, and database activity monitoring
- Strong background in networking, especially architecture design and analysis
- Firewalling, secure networking, hardware appliance management, and related technology experience
- Experience supporting regulated industries with compliance drivers such as GLBA, HIPAA, PCI DSS, NERC/FERC requirements, Sarbanes-Oxley, etc.
- Vendor certifications often include: CCNA, CCIE, CCNP, CCDE, HP ExpertONE, etc.
- Other certifications often include: CISSP, GIAC, GSEC, CISA and/or equivalent.

IV. References

All of the following account references below are using McAfee's Enterprise Security Manager (ESM) SIEM in an enterprise-wide deployment. AccessIT Group and McAfee would be happy to supply customer introductions to our customer references should McAfee be considered a finalist in the selection process. We are adamant on protecting our reference customers from inquires as we are respectful of their privacy and available time and resources. In the event that a reference call is needed in the near future, we would be happy to reach out to our customer base to establish an introduction.

Account Name	Contact Name	Contact Title	Contact Phone	Contact E-mail
Johns Hopkins University (Enterprise)	Contact information available upon request			
Laureate Education	Contact information available upon request			
Virginia Community College System	Contact information available upon request			
Virginia State Lottery	Contact information available upon request			

V. Attachment A (Offeror Data Sheet)

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years 13 Months 2

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #
CoStar Group	9 months	1331 L Street NW, Washington, DC 20006	Andrew Ugwuh, 202-336-6908
NRUCFC	1 year, 4 months	20701 Cooperative Way, Dulles, VA 20166	Duc Lai, 703-467-1803
Maersk Line Limited	2 years, 8 months	1 Commercial Place, Floor 20, Norfolk, VA 23510	Kenneth Buchanan, 757-589-1913
CareFirst Blue Cross Blue Shield	4 years, 6 months	10455 Mill Run Circle, Owings Mills, MD 21117	Dave Ferguson, 410-998-4323
Transaction Network Services	1 year, 0 months	10740 Parkridge Boulevard, Reston, VA 20191	Kent Kling, 703-453-8449

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

Mike Korwek / AccessIT Group, Inc. / 9256 Bendix Road, Suite 306, Columbia, MD 21045

Julie Wallace / AccessIT Group, Inc. / 20106 Valley Forge Circle, King of Prussia, PA 19406

June Chung / AccessIT Group, Inc. / 20106 Valley Forge Circle, King of Prussia, PA 19406

Valerie Galderi / AccessIT Group, Inc. / 115 Route 46 W, Building E, Suite 35, Mountain Lakes, NJ 07046

3. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
[ ] YES [X] NO

IF YES, EXPLAIN:_____

_____

_____

_____

VI. Attachment B (Small Business Subcontracting Plan)

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

Offeror Name: AccessIT Group, Inc.

Preparer Name: Mike Korwek

Date: 3/21/2014

Is your firm a **Small Business Enterprise** certified by the Department of Minority Business Enterprise? Yes_____ No__X__

If yes, certification number: _____ Certification date:_____

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Minority Business Enterprise? Yes_____ No__X__

If yes, certification number: _____ Certification date:_____

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Minority Business Enterprise? Yes____ No__X__

If yes, certification number: _____ Certification date:_____

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

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

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

Program, all certified women-owned businesses are also a small business enterprise.

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

All small, women, and minority owned businesses must be certified by the Commonwealth of

Virginia Department of Minority Business Enterprise (DMBE) to be counted in the SWAM program. Certification applications are available through DMBE at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at www.dmbe.virginia.gov (Customer Service)

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

Procurement Name and Number: Security Incident and Event Management System, MLO-773
Listing of Sub-Contractors, to include, Small, Woman Owned and Minority Owned Businesses for this Bid/Proposal and Subsequent Contract

3/21/2014_____
Date Form Completed

Offeror / Proposer:

AccessIT Group, Inc.	9256 Bendix Road, Suite 306, Columbia, MD 21045	Mike Korwek/410-782-4805
Firm	Address	Contact Person/No.

Sub-Contractor's Name and Address	Contact Person & Phone Number	DMBE Certification Number or FEIN No.	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)	Federal Employer Identification Number
Not Applicable						

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

VII. VASCUPP Business

While AccessIT Group does have contacts within higher education institutions that participate in and/or hold the VASCUPP member institution in high regard, we currently have recorded zero dollars of sales during the last twelve months with any member of VASCUPP.

VIII. Proposed Cost

QUANTITY	REQUIRED?	ONE-TIME/ON-GOING COST?	DESCRIPTION	LIST PRICE	UNIT PRICE	EXT PRICE
1	REQUIRED	ONE-TIME	**ETM-5600L**	$71,994.00	$41,737.00	**$41,737.00**
			INSTITUTION ELITE MFE ENTERPRISE SECURITY MANAGER 5600 APPL 1U+			
1	REQUIRED	ON-GOING	**ETM5600ARMAL**	$14,398.80	$13,109.00	**$13,109.00**
			INSTITUTION ELITE MFE ENTERPRISE SECURITY MANAGER 5600 1YR GL+ARMA 1U+			
2	REQUIRED	ONE-TIME	**ERC-2600L**	$44,992.50	$26,083.00	**$52,166.00**
			INSTITUTION ELITE MFE EVENT RECEIVER 2600 APPL 1U+			
2	REQUIRED	ON-GOING	**ERC2600ARMAL**	$8,998.50	$8,193.00	**$16,386.00**
			INSTITUTION ELITE MFE EVENT RECEIVER 2600 1YR GL+ARMA 1U+			
1	REQUIRED	ONE-TIME	**ELM-5600L**	$47,994.00	$27,823.00	**$27,823.00**
			INSTITUTION ELITE MFE ENTERPRISE LOG MANAGER 5600 APPL 1U+			
1	REQUIRED	ON-GOING	**ELM5600ARMAL**	$9,598.80	$8,739.00	**$8,739.00**
			INSTITUTION ELITE MFE ENTERPRISE LOG MANAGER 5600 1YR GL+ARMA 1U+			
1	OPTIONAL	ONE-TIME	**ACE-3450L**	$51,993.50	$30,142.00	**$30,142.00**
			INSTITUTION ELITE MFE ADVANCED CORRELATION ENGINE 3450 APPL 1U+			
1	OPTIONAL	ON-GOING	**ACE3450ARMAL**	$10,398.70	$9,467.00	**$9,467.00**
			INSTITUTION ELITE MFE ADVANCED CORRELATION ENGINE 3450 1YR GL+ARMA			
1	OPTIONAL	ONE-TIME	**APM-3450L**	$25,794.00	$14,954.00	**$14,954.00**
			INSTITUTION ELITE MFE APPLICATION DATA MONITOR 3450 APPL 1U+			
1	OPTIONAL	ON-GOING	**APM3450ARMAL**	$5,158.80	$4,697.00	**$4,697.00**
			INSTITUTION ELITE MFE APPLICATION DATA MONITOR 3450 1YR GL+ARMA 1U+			
1	OPTIONAL	ON-GOING	**GTEETM5600GIEAD**	$5,760.00	$3,345.00	**$3,345.00**
			MFE GLOBAL THREAT INTELLIGENCE ENTERPRISE SECURITY MANAGER (ESM) MODULE FOR ETM5600 1:1GL			
	REQUIRED	ONE-TIME	**Shipping, Handling, and Insurance Charges (estimated)**			**$750.00**
			VA State Sales Tax (6%)			**EXEMPT**
					TOTAL	**$223,315.00**

(Please note that all pricing provided above is in US Dollars and all On-Going Costs are for 1 Year)

IX. Appendix A

McAfee SIEM Supported Devices

Last Updated
2/5/2014

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
A10 Networks	Load Balancer (ASP)	Load Balancer	All	ASP	Syslog	9.1 and greater	AX Series
Accellion	Secure File Transfer (ASP)	Application	All	ASP	Syslog	9.1 and greater	
Access Layers	Portnox (ASP)	NAC	2.x	ASP	Syslog	9.1 and greater	
Adtran	Bluesocket (ASP)	Wireless Access Point	All	ASP	Syslog	9.1.1 and greater	
	NetVanta (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
AirTight Networks	SpectraGuard (ASP)	Application	All	ASP	Syslog	9.1 and greater	
Alcatel-Lucent	NGN Switch (ASP)	Switch	All	ASP	Syslog	9.2 and greater	
	VitalQIP (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
American Power Conversion	Uninterruptible Power Supply (ASP)	Power Supplies	All	ASP	Syslog	9.1 and greater	
Apache Software Foundation	Apache HTTP Server	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	1.x, 2.x	Code Based	Syslog	9.1 and greater	
	Apache Web Server (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	1.x, 2.x	ASP	Syslog	9.1 and greater	
Apple Inc.	Mac OS X (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
Arbor Networks	Peakflow SP	Network Switches & Routers	2.x	Code Based	Syslog	9.1 and greater	
	Peakflow SP (ASP)	Network Switches & Routers	2.x and above	ASP	Syslog	9.2 and greater	
	Peakflow X	Network Switches & Routers	2.x	Code Based	Syslog	9.1 and greater	
	Peakflow X (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	Pravail (ASP)	IDS/IPS	All	ASP	Syslog	9.1 and greater	
ArcSight	Common Event Format (ASP)	Event Format	All	ASP	Syslog	9.2 and greater	
Aruba	Aruba OS	Wireless Access Point	N/A	Code Based	Syslog	9.1 and greater	
	ClearPass (ASP)	Wireless Access Point	5.x	ASP	Syslog	9.1 and greater	
Avecto	Privilege Guard (ePO)	IAM / IDM	3.x	ASP	SQL	9.2 and greater	
Axway	SecureTransport (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
Barracuda Networks	Spam Firewall (ASP)	Security Appliances / UTMs	3.x, 4.x	ASP	Syslog	9.1 and greater	
	Web Application Firewall (ASP)	Security Appliances / UTMs	All	ASP	Syslog	9.1 and greater	
	Web Filter (ASP)	Security Appliances / UTMs	All	ASP	Syslog	9.1 and greater	
BeyondTrust	BeyondTrust REM	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
	BeyondTrust Retina	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
Bit9	Bit9 Parity Suite - CEF (ASP)	Application	All	ASP	Syslog	9.2 and greater	
	Bit9 Parity Suite (ASP)	Application	All	ASP	Syslog	9.1 and greater	
Blue Coat	Director (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.2 and greater	
	ProxySG (ASP)	Web Content / Filtering / Proxies	4.x-6.x	ASP	Syslog	9.1 and greater	Access Log
Blue Lance, Inc.	LT Auditor+ for Novell NetWare	Application	9.x	Code Based	SQL	9.1 and greater	
Blue Martini Software	Blue Martini	Application	6.5	Code Based	Syslog	9.1 and greater	
Blue Ridge Networks	BorderGuard (ASP)	Firewall	5000, 6000	ASP	Syslog	9.1 and greater	
BlueCat Networks	BlueCat DNS/DHCP Server (ASP)	Application	All	ASP	Syslog	9.1 and greater	
Bradford Networks	Campus Manager (ASP)	NAC / Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
Brocade	BigIron, FastIron and NetIron (ASP)	Network Switches & Routers	7.5 and above	ASP	Syslog	9.1 and greater	
	IronView Network Manager (ASP)	NAC / Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	VDX Switch (ASP)	Network Switches & Routers	All	ASP	Syslog	9.2 and greater	
CA Technologies	DataMinder - CEF (ASP)	DLP	All	ASP	Syslog	9.1 and greater	CEF Format
	SiteMinder (ASP)	Web Access	All	ASP	Syslog	9.1 and greater	
Cerner	Cerner P2 Sentinel	Healthcare Auditing	All	Code Based	McAfee Event Format	9.1 and greater	
Check Point	Check Point (ASP)	Firewall	All	ASP	OPSEC	9.3.0 and above	
	Check Point via Splunk (ASP)	Firewall	All	ASP	Syslog	9.2 and greater	Using Splunk app
Cimcor	CimTrak Management Console	Configuration Management	All	Code Based	McAfee Event Format	9.1 and greater	
	ASA NSEL	Firewall / Flow	All	Netflow	Netflow	9.1 and greater	
	CATOS v7xxx (ASP)	Host / Server / Operating Systems / Network Switches & Routers	6.x, 7.x	ASP	Syslog	9.1 and greater	
	Content Services Switches (ASP)	Other	All	ASP	Syslog	9.1 and greater	
	CSA Console	Host / Server / Operating Systems / IDS / IPS	5.x, 6.x	Code Based	SQL	9.1 and greater	
	Guard DDoS Mitigator (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater	
	Identity Services Engine (ASP)	Other	All	ASP	Syslog	9.1 and greater	
	IDS (4.x+ RDEP protocol)	IDS / IPS	4.x and above	SDEE		9.1 and greater	
	IOS (ASP)	IDS / IPS / Network Switches & Routers	12.x and above	ASP	Syslog	9.1 and greater	ACL, IOS FW, IOS IDS and DSP
	IOS ACL	Network Switches & Routers	12.x and above				Use Cisco IOS (ASP) data source

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
Cisco	IOS EAP	IDS / IPS / Network Switches & Routers	12.x and above				Use Cisco IOS (ASP) data source
	IOS Firewall	Firewall / Network Switches & Routers	12.x and above				Use Cisco IOS (ASP) data source
	IOS IDS	IDS / IPS / Network Switches & Routers	12.x and above				Use Cisco IOS (ASP) data source
	IOS IPS (SDEE protocol)	Application Protocol	All	SDEE		9.1 and greater	
	IronPort Email Security (ASP)	Email Security	6.x, 7.x	ASP	Syslog	9.1 and greater	
	IronPort Web Security Appliance (ASP)	Web Content / Filtering / Proxies	6.x, 7.x	ASP	Syslog	9.1 and greater	
	MDS (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	NAC Appliance (ASP)	NAC / Network Switches & Routers	All	ASP	Syslog	9.1 and greater	Formerly Clean Access
	NAC Appliance (Clean Access)	NAC / Network Switches & Routers	4.x	Code Based	HTTP	9.1 and greater	
	NX-OS (ASP)	IDS / IPS / Network Switches & Routers	4.x, 5.x	ASP	Syslog	9.1 and greater	
	Open TACACS+ (ASP)	Authentication	All	ASP	Syslog	9.1 and greater	
	PIX IDS	IDS / IPS / Network Switches & Routers	12.x and above				Use Cisco PIX/ASA/FWSM (ASP) data source
	PIX/ASA/FWSM (ASP)	Firewall / IDS / IPS	5.x and above	ASP	Syslog	9.1 and greater	
	Secure ACS (ASP)	IDS / IPS	3.x, 4.x	ASP	Syslog	9.1 and greater	
	Unified Computing System (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	VSM/VPN Concentrator	Virtual Private Network	2.x – 4.x	Code Based	Syslog	9.1 and greater	
	WAAS (ASP)	Applications / Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	WAP200 (ASP)	Wireless Access Point	All	ASP	Syslog	9.1 and greater	
	Wireless Control System (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	Wireless Lan Controller (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
Citrix	NetScaler (AppFlow)	Flow	All	IPFix	IPFix	9.2 and greater	
	NetScaler (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	Secure Gateway & NetScaler Web also supported
	Secure Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.2 and greater	
Cluster Labs	Pacemaker (ASP)	Application	1.x	ASP	Syslog	9.1 and greater	
Code Green	Data Loss Prevention (ASP)	DLP	8.x	ASP	Syslog	9.1 and greater	
Cooper Power Systems	Cybectec RTU (ASP)	Network Switches & Routers	5.x, 6.x	ASP	Syslog	9.1 and greater	
	Yukon IED Manager Suite (ASP)	Application	All	ASP	Syslog	9.1 and greater	
Corero	Corero IPS (ASP)	IDS/IPS	All	ASP	Syslog	9.1 and greater	
Critical Watch	Critical Watch FusionVM	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
CyberArk	Enterprise Password Vault (ASP)	Application	5.x	ASP	Syslog	9.1 and greater	
	Privileged Identity Management Suite - CEF (ASP)	Application	All	ASP	Syslog	9.1 and greater	
CyberGuard	CyberGuard	Firewall	5.x	Code Based	Syslog	9.1 and greater	Includes FS, SG, SL
Cyrus	Cyrus IMAP & SASL (ASP)	Messaging	2.x	ASP	Syslog	9.1 and greater	
D-Link	NetDefend UTM Firewall (ASP)	UTM	All	ASP	Syslog	9.2 and greater	
Damballa	Failsafe (ASP)	Anti-Malware	All	ASP	Syslog	9.1.1 and greater	
Dell	PowerConnect Switches (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
DG Technology - InfoSec	Mainframe Event Acquisition System (ASP)	MainFrame	5.x, 6.x	ASP	Syslog	9.1 and greater	DG Technology MEAS agent, DB2/IMS/Datacom/IDMS, CICS, FTP, MasterConsole, RACF/Top Secret/ACF2, Telnet, VSAM/BDAM/PDS, TCP/IP, SMP/E, Authorized Load Libraries, RMF Performance Data, Batch Job and Started, Tasks Start/Stop, Top Secret, Type 80
Digital Defense	Digital Defense Frontline	Vulnerability Systems	All	N/A	N/A	9.1.4 and greater	
Econet	Sentinel IPS (ASP)	IDS/IPS	All	ASP	Syslog	9.2 and greater	
EdgeWave	iPrism Web Security (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
Enforcive	System z SMF DB2 (ASP)	MainFrame	All	ASP	Syslog	9.1 and greater	Formerly Bsafe, AS/400, DB2/IMS/Datacom/IDMS, FTP, RACF/Top Secret/ACF2, Telnet, VSAM/BDAM/PDS
Enterasys Networks	Dragon Sensor	IDS/IPS	1.x-7.x	Code Based	SQL	9.1 and greater	
	Dragon Squire	IDS/IPS	1.x-7.x	Code Based	SQL	9.1 and greater	
	Enterasys N and S Switches (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.1 and greater	

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
	Enterasys Network Access Control (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.1 and greater	
Entrust	**IdentityGuard (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
Extreme Networks	**ExtremeWare XOS (ASP)**	Network Switches & Routers	7.x, 8.x	ASP	Syslog	9.1 and greater	Alpine, BlackDiamond and Summit
F5 Networks	**BIG-IP Access Policy Manager (ASP)**	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	BIG-IP Application Security Manager - CEF (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.2 and greater	
	Firepass SSL VPN (ASP)	Virtual Private Network	All	ASP	Syslog	9.1 and greater	
	Local Traffic Manager - LTM (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
FairWarning	**Patient Privacy Monitoring**	Application Security	2.9.x	Code Based	McAfee Event Format	9.1 and greater	
Fidelis	**Fidelis XPS (ASP)**	Network Security Applicance	All	ASP	Syslog	9.1 and greater	
FireEye	**FireEye Malware Protection System - CEF (ASP)**	Antivirus/Malware	5.x and above	ASP	Syslog	9.1 and greater	
Fluke Networks	**AirMagnet Enterprise (ASP)**	Network Switches & Routers	8.x	ASP	Syslog	9.1 and greater	
Force10 Networks	**FTOS (ASP)**	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
ForeScout	**CounterACT (ASP)**	Network Switches & Routers	5.x and 6.x	ASP	Syslog	9.1 and greater	
	CounterACT CEF (ASP)	Network Switches & Routers	7.x and above	ASP	Syslog	9.1 and greater	
Fortinet	**FortiGate Antivirus**	Antivirus	All	Code Based	Syslog	9.1 and greater	
	FortiGate Firewall	Firewall	3.x	Code Based	Syslog	9.1 and greater	
	FortiGate IDS	IDS / IPS	All	Code Based	Syslog	9.1 and greater	
	FortiGate UTM - Comma Delimited - (ASP)	Firewall	All	ASP	Syslog	9.1 and greater	
	FortiGate UTM - Space Delimited - (ASP)	Firewall	All	ASP	Syslog	9.1 and greater	
	FortiManager (ASP)	Firewall	All	ASP	Syslog	9.1 and greater	
	FortiWeb Web Application Firewall (ASP)	Firewall	All	ASP	Syslog	9.1 and greater	
FreeRADIUS	**FreeRADIUS (ASP)**	Authentication	All	ASP	Syslog	9.1 and greater	
Generic	**Advanced Syslog Parser**	Other	All	ASP	Syslog	9.1 and greater	
	CIFS/SMB File Source	Other	N/A	Code Based	File pull	9.2 and greater	ELM only
	FTP/FTPS File Source	Other	N/A	Code Based	File pull	9.2 and greater	ELM only
	HTTP/HTTPS File Source	Other	N/A	Code Based	File pull	9.2 and greater	ELM only
	McAfee Event Format	Other	N/A	Code Based	McAfee Event Format	9.2 and greater	
	NFS File Source	Other	N/A	Code Based	File pull	9.2 and greater	ELM only
	SCP File Source	Other	N/A	Code Based	File pull	9.2 and greater	ELM only
	SFTP File Source	Other	N/A	Code Based	File pull	9.2 and greater	ELM only
GFI	**GFI LanGuard**	VA Scanner	All	Code Based	File pull	9.1 and greater	
Gigamon	**GigaVUE (ASP)**	Switches & Routers	All	ASP	Syslog	9.1.1 and greater	
Global Technology Associates	**GNAT Box (ASP)**	Firewall	5.3.x	ASP	Syslog	9.1 and greater	
Good Technology	**Good Mobile Control (ASP)**	Application	All	ASP	Syslog	9.2 and greater	
HBGary	**Active Defense (ASP)**	UTM	All	ASP	Syslog	9.1 and greater	
Hewlett-Packard	**3Com Switches (ASP)**	Switches & Routers	All	ASP	Syslog	9.1 and greater	
	LaserJet Printers (ASP)	Printers	All	ASP	Syslog	9.1 and greater	
	OpenVMS (ASP)	Operating Systems	1.x	ASP	Syslog	9.1 and greater	
	ProCurve (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
IBM	**Guardium (ASP)**	Database Activity Monitoring	6.x, 7.x	ASP	Syslog	9.2 and greater	
	ISS Real Secure Server Sensor	Host / Server / Operating Systems	5.5 – 7.x	Code Based	SQL	9.1 to 9.3.2	
	ISS SiteProtector	Security Management	All	Code Based	SQL	9.1 and greater	
	MainFrame	MainFrame	All				Use DG Technoloty MEAS Parser
	Proventia GX (ASP)	Other	All	ASP	Syslog	9.1 and greater	
	System Z DB2	Database	All				Use DG Technoloty MEAS Parser
	Tivoli Endpoint Manager - BigFix (ASP)	Host / Server / Operating Systems / Other	All	ASP	Syslog	9.1 and greater	Linux Agent Required
	Tivoli Identity Manager (ASP)	IAM / IDM	All	ASP	SQL	9.2 and greater	
	z/OS, z/VM	MainFrame					Use DG Technoloty MEAS Parser
Imperva	**WAF/DAM - CEF (ASP)**	Database	All	ASP	Syslog	9.2 and greater	
Infoblox	**NIOS (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
InfoExpress	**CyberGatekeeper LAN**	Network Switches & Routers	All	Code Based	Syslog	9.1 and greater	
InterSect Alliance	**Snare for AIX (ASP)**	Other	All	ASP	Syslog	9.1 and greater	
	Snare for Solaris (ASP)	Other	All	ASP	Syslog	9.1 and greater	
	Snare for Windows (ASP)	Other	All	ASP	Syslog	9.1 and greater	
Invincea	**Enterprise - CEF (ASP)**	Host / Server / Operating Systems / Other	All	ASP	Syslog	9.1 and greater	
IPFIX	**IPFIX**	Network Flow Collection	All	IPFix	IPFix	9.1 and greater	
Ipswitch	**WS_FTP (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
Itron	**Itron Enterprise Edition (ASP)**	Smart Grid Application	All	ASP	Syslog	9.1 and greater	
Jflow	**Jflow (Generic)**	Network Flow Collection	5, 7, 9	Netflow		9.1 and greater	
Juniper Networks	**Juniper Secure Access/MAG (ASP)**	VPN	All	ASP	Syslog	9.1 and greater	
	JUNOS - Structured-Data Format (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	JUNOS Router (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	NetScreen / IDP (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	NetScreen Firewall	Firewall	4.x, 5.x	Code Based	Syslog	9.1 and greater	
	NetScreen IDP	IDS / IPS	3.x, 4.x	Code Based	Syslog	9.1 and greater	

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
	NetScreen SSL VPN Secure Access	VPN	5.x – 7.x	Code Based	Syslog	9.1 and greater	
	Network and Security Manager - NSM (ASP)	Applications / Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater	
	Secure Access version 7 (ASP)	VPN	5.x-7.x	ASP	Syslog	9.1 and greater	
	Steel Belted Radius (ASP)	Radius Server	5.x and above	ASP	Syslog	9.1 and greater	
Kaspersky	**Administration Kit - SQL Pull (ASP)**	Antivirus	All	ASP	SQL	9.2.1 and greater	
KEMP Technologies	**LoadMaster (ASP)**	Network Switches & Routers	4.x, 5.x	ASP	Syslog	9.1 and greater	
Lancope	**StealthWatch**	IDS / IPS / Network Switches & Routers	4.x-5.6	Code Based	Syslog	9.1 and greater	
	StealthWatch (ASP)	IDS / IPS / Network Switches & Routers	6.x and above	ASP	Syslog	9.1 and greater	
Legacy	**Event Center (ASP)**	Other	All	ASP	Syslog	9.1 and greater	
	Informant (ASP)	IDS / IPS	All	ASP	Syslog	9.3.0 and above	
Lieberman	**Enterprise Random Password Manager (ASP)**	Application	All	ASP	Syslog	9.1.1 and greater	XML
Locum	**RealTime Monitor (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
Lumension	**Bouncer - CEF (ASP)**	Application	5.x and above	ASP	Syslog	9.2 and greater	
	Bouncer (ASP)	Application	4.x	ASP	Syslog	9.1 and greater	
	Lumension	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
MailGate, Ltd.	**MailGate Server (ASP)**	Applications / Security Management / Host / Server / Operating Systems	3.5	ASP	Syslog	9.1 and greater	
McAfee	**AntiSpyware (ePO)**	Antivirus	All	ASP	ePO – SQL	9.2 and greater	
	Application and Change Control (ePO)	Web Content / Filtering / Proxies	All	ASP	ePO – SQL	9.2 and greater	
	Asset Manager Sensor (ASP)	Asset Management	All	ASP	Syslog	9.1.1 and greater	
	Correlation Engine	Other	All	Correlation		9.1 and greater	
	Database Security - CEF (ASP)	Database	All	ASP	Syslog	9.2 and greater	
	Database Security (ePO)	Database	All	ASP	ePO – SQL	9.2 and greater	
	DB2	Database	8.x, 9.x, 10.x			9.1 and greater	Supported by McAfee Database Event Monitor
	Deep Defender (ePO)	Other	All	ASP	ePO – SQL	9.2 and greater	
	Email and Web Security - CEF (ASP)	Web Content / Filtering / Proxies	6.x and above	ASP	Syslog	9.2 and greater	
	Email and Web Security v5 (ASP)	Web Content / Filtering / Proxies	5.x	ASP	Syslog	9.1 and greater	
	Email Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	ePO Audit Log (ePO)	Other	All	ASP	ePO – SQL	9.2 and greater	
	ePolicy Orchestrator (ASP)	Other	All	ASP	ePO – SQL	9.2 and greater	
	ePolicy Orchestrator Agent (ePO)	Applications / Security Management / Host / Server / Operating Systems	3.x and above	ASP	ePO – SQL	9.2 and greater	
	Firewall Enterprise (ASP)	Firewall / IDS / IPS	8.x	ASP	Syslog	9.2 and greater	
	Greenplum	Database	8.2.15			9.1 and greater	Supported by McAfee Database Event Monitor
	GroupShield for Domino (ePO)	Web Content / Filtering / Proxies	All	ASP	ePO – SQL	9.2 and greater	
	GroupShield for Exchange (ePO)	Web Content / Filtering / Proxies	All	ASP	ePO – SQL	9.2 and greater	
	Host Data Loss Prevention (ePO)	DLP	All	ASP	ePO – SQL	9.2 and greater	
	Host Intrusion Prevention (ePO)	IDS / IPS	6.x and above	ASP	ePO – SQL	9.2 and greater	
	Informant (ASP)	IDS / IPS	All	ASP	Syslog	9.3.0 and above	
	Informix	Database	11.5			9.1 and greater	Supported by McAfee Database Event Monitor
	InterSystems Cache	Database	2011.1.x			9.1 and greater	Supported by McAfee Database Event Monitor
	McAfee Advanced Correlation Engine	Correlation	All			9.1 and greater	
	McAfee Application Data Monitor	Application	All	Code Based		9.1 and greater	
	McAfee Database Event Monitor for SIEM	Database	All	Code Based		9.1 and greater	
	McAfee Vulnerability Manager	Vulnerability Systems	All	N/A	N/A	9.1.2 and greater	
	MOVE AntiVirus (ePO)	Antivirus	All	ASP	ePO – SQL	9.2 and greater	
	MSSQL	Database	7, 2000, 2005, 2008, 2012			9.1 and greater	Supported by McAfee Database Event Monitor
	MySQL	Database	(32 bit, Windows) 4.x, 5.x, 6.x			9.1 and greater	Supported by McAfee Database Event Monitor
	Network Access Control (ePO)	Other	All	ASP	ePO – SQL	9.2 and greater	
	Network DLP Monitor (ASP)	DLP	All	ASP	Syslog	9.1 and greater	
	Network Security Manager - SQL Pull (ASP)	IDS / IPS	6.x and above	ASP	SQL	9.1.2 and greater	Formerly IntruShield
	Network Security Manager (ASP)	IDS / IPS	6.x and above	ASP	Syslog	9.1 and greater	Formerly IntruShield
	Network Threat Response (ASP)	IDS / IPS	4.0.0.5 and above	ASP	Code Based API	9.3.0 and above	
	Next Generation Firewall - Stonesoft (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater	
	Nitro IPS	IDS / IPS	All	ASP	Syslog	9.1 and greater	
	Oracle	Database	8.x, 9.x, 10g, 11g, 11g R2			9.1 and greater	Supported by McAfee Database Event Monitor

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
	PIServer	Database				9.1 and greater	Supported by McAfee Database Event Monitor
	Policy Auditor (ePO)	Policy Server	All	ASP	ePO – SQL	9.2 and greater	
	PostgreSQL	Database	7.4.x, 8.4.x, 9.0.x, 9.1.x			9.1 and greater	Supported by McAfee Database Event Monitor
	SaaS Web Protection (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	SiteAdvisor (ePO)	Other	All	ASP	ePO – SQL	9.2 and greater	
	Sybase	Database	11.x, 12.x, 15.x			9.1 and greater	Supported by McAfee Database Event Monitor
	Teradata	Database	12.x, 13.x, 14.x			9.1 and greater	Supported by McAfee Database Event Monitor
	UTM Firewall (ASP)	Firewall	All	ASP	Syslog	9.1 and greater	
	Vertica	Database	5.1.1-0			9.1 and greater	Supported by McAfee Database Event Monitor
	VirusScan (ePO)	Antivirus	All	ASP	ePO – SQL	9.2 and greater	
	Web Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	WebShield (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
MEDITECH	**Caretaker (ASP)**	HealthCare Application	All	ASP	Syslog	9.1 and greater	
Microsoft	**ACS – SQL Pull (ASP)**	Applications / Host / Server / Operating Systems	All	ASP	SQL	9.1.3 and greater	
	Adiscon Windows Events	Applications / Host / Server / Operating Systems	All	Code Based	Syslog	9.1 and greater	
	Assets via Active Directory	Asset	All			9.1 and greater	
	Event Forwarding	Applications / Host / Server / Operating Systems	2008	WMI	MEF – McAfee SIEM Agent	9.1 and greater	
	Exchange (ASP)	Applications / Host / Server / Operating Systems	2007, 2010	ASP	File pull / McAfee SIEM Agent	9.1 and greater	Message tracking logs
	Forefront Client Security (ASP)	HIPS	2010	ASP	SQL	9.1.1 and greater	
	Forefront Endpoint Protection – SQL Pull (ASP)	HIPS	2010	ASP	SQL	9.1 and greater	
	Forefront Threat Management Gateway – SQL Pull (ASP)	IDS / IPS	2010	ASP	SQL	9.3.0 and above	
	Forefront Unified Access Gateway (ASP)	IDS / IPS	2010	ASP	Syslog	9.1.1 and greater	
	Internet Authentication Service - Formatted (ASP)	Web Content/Filtering/Proxies	2003, 2008	ASP	Syslog	9.1 and greater	
	Internet Authentication Service - XML (ASP)	Web Content/Filtering/Proxies	2003, 2008	ASP	Syslog	9.1 and greater	
	Internet Information Services	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	Code Based	Syslog	9.1 and greater	
	Internet Information Services - FTP (ASP)	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	File pull / McAfee SIEM Agent	9.1 and greater	
	Internet Information Services (ASP)	Host / Server / Operating Systems / Web Content / Filtering / Proxies	All	ASP	File pull / McAfee SIEM Agent	9.1 and greater	
	Internet Security and Acceleration (ASP)	Firewall / Host / Server / Operating Systems / Web Content / Filtering / Proxies / Virtual Private Networks	All	ASP	Syslog	9.1 and greater	
	Microsoft Active Directory	Other	All	WMI	WMI	9.1 and greater	
	Microsoft Exchange Server	Other	2007, 2010	WMI	WMI	9.1 and greater	
	Microsoft SQL Server	Database	All	WMI	WMI	9.1 and greater	
	MSSQL Error Log (ASP)	Database	All	ASP	Syslog	9.2 and greater	
	MSSQL Server C2 Audit	Database	2000, 2005, 2008	Code Based	MEF – McAfee SIEM Agent	9.1 and greater	
	Network Policy Server (ASP)	Policy Server	All	ASP	Syslog	9.1 and greater	
	Operations Manager	Host / Server / Operating Systems	All	Code Based	SQL	9.1 and greater	
	PhoneFactor (ASP)	Application	All	ASP	Syslog	9.1 and greater	
	SharePoint (ASP)	Host / Server / File Management	2007, 2010	ASP	Syslog	9.1 and greater	
	System Center Operations Manager	Security Management	2007	Code Based	MEF – McAfee SIEM Agent	9.1 and greater	
	Windows DHCP (ASP)	Debug DHCP Logs	2003, 2008	ASP	File pull / McAfee SIEM Agent	9.1 and greater	
	Windows DNS (ASP)	Debug DNS Logs	2003, 2008	ASP	File pull / McAfee SIEM Agent	9.1 and greater	
	Windows Event Log - CEF (ASP)	Applications / Host / Server / Operating Systems	All	ASP	Syslog	9.2 and greater	
	Windows Event Log - WMI	Applications / Host / Server / Operating Systems	All	WMI	WMI	9.1 and greater	
Mirage Networks	**CounterPoint**	NAC / Network Switches & Routers	2.3.1	Code Based	Syslog	9.1 and greater	
Motorola	**AirDefense (ASP)**	Wireless Switch	All	ASP	Syslog	9.1 and greater	

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
Motorola	**AirDefense Enterprise**	Wireless Switch	All	Code Based	Syslog	9.1 and greater	
NetApp	**Data ONTAP (ASP)**	Storage	7.x	ASP	Syslog	9.1 and greater	
	DataFort (ASP)	Storage Switch	All	ASP	Syslog	9.1 and greater	
	FAS	Storage	All			9.1 and greater	Use NetApp Data OnTap (ASP) data source
NetFlow	**Generic NetFlow**	Flow	5, 7, 9	NetFlow	NetFlow	9.1 and greater	
NetFort Technologies	**LANGuardian (ASP)**	Applications / Security Management / Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater	
NetIQ	**Security Manager (ASP)**	Network Switches & Routers / Security Management	5.1	ASP	Syslog	9.1 and greater	
	Sentinel Log Manager (ASP)	Network Switches & Routers / Security Management	All	ASP	Syslog	9.1 and greater	
NetWitness	**Informer - CEF (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
	Spectrum - CEF (ASP)	Malware	All	ASP	Syslog	9.2 and greater	URL Integration
NGS	**NGS SQuirreL**	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
Niksun	**NetDetector (ASP)**	Other	All	ASP	Syslog	9.1 and greater	
Nokia	**IPSO**	Firewall	All	Code Based	Syslog	9.1 and greater	
Nortel Networks	**Contivity VPN**	Network Switches & Routers	7.x	Code Based	Syslog	9.1 and greater	
	Passport 8000 Series Switches (ASP)	Network Switches & Routers	7.x	ASP	Syslog	9.1 and greater	
	VPN Gateway 3050 (ASP)	Virtual Private Network	8.x	ASP	Syslog	9.1 and greater	
Novell	**eDirectory (ASP)**	Applications / Security Management / Host / Server / Operating Systems	All	ASP	Syslog	9.2 and greater	
	Identity and Access Management - IAM (ASP)	IAM / IDM	All	ASP	Syslog	9.1 and greater	
nPulse	**CPX Flow & Packet Capture**	Packet Capture	All	N/A	N/A	9.1 and greater	URL Integration
OpenVAS	**OpenVAS**	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
OpenVPN	**OpenVPN (ASP)**	VPN	2.1 and above	ASP	Syslog	9.1 and greater	
Oracle	**Identity Manager – SQL Pull (ASP)**	IAM / IDM		ASP	SQL	9.3.2 and above	
	Oracle Audit - SQL Pull (ASP)	Database	10g, 11g	ASP	SQL	9.2.1 and greater	Support grain and fine grain logs
	Oracle Audit (ASP)	Database	All	ASP	Syslog	9.2.1 and greater	
	Solaris Basic Security Module - BSM (ASP)	Host / Server / Operating Systems	9.x, 10.x	ASP	Syslog	9.1 and greater	
	WebLogic (ASP)	Other	8.1.x	ASP	Syslog	9.1 and greater	
Osiris	**Host Integrity Monitor (ASP)**	Host / Server / Operating Systems / IDS / IPS		ASP	Syslog	9.1 and greater	ISAKMP, RADIUS, SECURITY, Accounting, RIP, VR messages only
Palo Alto Networks	**Palo Alto Firewalls (ASP)**	Firewall	All	ASP	Syslog	9.1 and greater	
Postfix	**Postfix (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
PostgreSQL	**PostgreSQL (ASP)**	Database	All	ASP	Syslog	9.1 and greater	
PowerTech	**Interact - CEF (ASP)**	Host	All	ASP	Syslog	9.2 and greater	
Proofpoint	**Messaging Security Gateway (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
Qualys	**Qualys QualysGuard**	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
Quest	**ChangeAuditor for Active Directory**	Applications	All	WMI	WMI	9.1 and greater	
Radware	**AppDirector (ASP)**	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
	AppWall (ASP)	Firewall	All	ASP	Syslog	9.2 and greater	
	DefensePro	IDS / IPS	2.4.3 and above	Code Based	Syslog	9.1 and greater	
	DefensePro (ASP)	IDS / IPS	2.4.3 and above	ASP	Syslog	9.1 and greater	
	LinkProof/FireProof (ASP)	Network Switches & Routers	All	ASP	Syslog	9.1 and greater	
Rapid7	**Rapid7 Metasploit Pro**	Vulnerability Systems	3.x and above	N/A	N/A	9.1 and greater	
	Rapid7 Nexpose	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
Raytheon	**SureView (ASP)**	Application	All	ASP	Syslog	9.1 and greater	
Raz-Lee Security	**iSecurity Suite (ASP)**	Application	All	ASP	Syslog	9.2 and greater	
RedSeal Networks	**RedSeal 6 (ASP)**	Risk Complianace	All	ASP	Syslog	9.1 and greater	
Riverbed	**Steelhead (ASP)**	Security Appliances / UTMs	5.x	ASP	Syslog	9.1 and greater	
RSA	**Authentication Manager (ASP)**	Authentication	7.x	ASP	Syslog	9.1 and greater	
SafeNet	**Hardware Security Modules (ASP)**	Application Security	All	ASP	Syslog	9.1 and greater	
Saint	**Saint**	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
SAP	**SAP Version 5 (ASP)**	Applications / Security Management / Host / Server / Operating Systems	5.x and 6.x	ABAP Module & ASP	Syslog	9.1 and greater	
Savant Protection	**Savant - CEF (ASP)**	Anti-Malware	3.x	ASP	Syslog	9.2 and greater	
Secure Crossing	**Zenwall (ASP)**	Applications / Security Management / Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater	
SecureAuth	**IEP - Single Sign On (ASP)**	Authentication	5.x	ASP	Syslog	9.1 and greater	
Securonix	**Risk and Threat Intelligence**	Application		Code Based	McAfee Event Format	9.1 and greater	
SendMail	**Sentrion**	Messaging	All				Use Unix – Linux data source
Sentrigo	**Hedgehog - CEF (ASP)**	Database	All	ASP	Syslog	9.2 and greater	
sFlow	**Generic sFlow**	Network Flow Collection	All	sFlow	sFlow	9.1 and greater	
Silver Spring Networks	**Network Infrastructure (ASP)**	Smart Grid	All	ASP	File pull / McAfee SIEM Agent	9.1 and greater	
SnapLogic	**SnapLogic (ASP)**	Cloud Integration	All	ASP	Syslog	9.2 and greater	

Vendor	Name	Device Type	Version(s) Supported	Parser	Method of Collection	ESM Version	Notes
Software Product Research	**DB2 Access Recording Services DBARS (ASP)**	Database	All	ASP	Syslog	9.1 and greater	
SonicWall	**Aventail (ASP)**	Virtual Private Network	10.x	ASP	Syslog	9.1 and greater	
	SonicOS (ASP)	Firewall	All	ASP	Syslog	9.1 and greater	
	SonicWall Firewall/VPN	Firewall	All	Code Based	Syslog	9.1 and greater	
	SonicWall IPS	IDS / IPS	All	Code Based	Syslog	9.1 and greater	
Sonus	**GSX (ASP)**	VOIP	All	ASP	Syslog	9.1 and greater	
Sophos	**Email Security and Data Protection (ASP)**	Email Security	All	ASP	Syslog	9.1 and greater	
	Sophos Antivirus	Antivirus	All	Code Based	SQL	9.1 and greater	
	Web Security and Control (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	Snort NIDS	IDS / IPS	All				Use SourceFire NS/RNA (ASP) data source
	SourceFire eStreamer	IDS / IPS	All	Code Based	eStreamer	9.1.1 and greater	
	SourceFire NS/RNA (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater	Includes Snort IDS
Squid	**Squid**	Web Content / Filtering / Proxies	1.x	Code Based	Syslog	9.1 and greater	
	Squid (ASP)	Web Content / Filtering / Proxies	2.5	ASP	Syslog	9.1 and greater	
StillSecure	**Strata Guard (ASP)**	Firewall / Security Management / IDS / IPS / Virtual Private Networks	5.x, 6.x	ASP	Syslog	9.1 and greater	
Stonesoft Corporation	**Next Generation Firewall (ASP)**	IDS / IPS	All				Use McAfee Next Generation Firewall - Stonesoft (ASP)
Sun	**iPlanet**	Web Server	All	Code Based	Syslog	9.1 and greater	
Symantec	**Altiris Management Console**	Asset	7.x and above			9.2 and greater	
	Antivirus Corporate Edition Server	Antivirus	8.x, 9.x	Code Based	SQL	9.1 and greater	
	Critical System Protection	IDS / IPS	5.2	Code Based	SQL	9.1 and greater	
	Endpoint Protection	Antivirus	11.x	Code Based	Syslog	9.1 and greater	
	Endpoint Protection (ASP)	Antivirus	11.x	ASP	Syslog	9.1 and greater	
	PGP Universal Server (ASP)	Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater	
	Symantec Data Loss Prevention (ASP)	DLP	All	ASP	Syslog	9.1 and greater	
	Symantec Messaging Gateway (ASP)	Messaging	2.x and above	ASP	Syslog	9.1 and greater	
	Symantec Web Gateway (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
Synology	**DiskStation Manager (ASP)**	Application	All	ASP	Syslog	9.2 and greater	
Tenable	**Tenable Nessus**	Vulnerability Systems	3.x, 4.x, 5.x, 6.x	N/A	N/A	9.1 and greater	
TippingPoint	**SMS (ASP)**	Security Management	2.x and above	ASP	Syslog	9.1 and greater	
	TippingPoint	Security Management	1.x, 2.x	Code Based	Syslog	9.1 and greater	
	UnityOne (ASP)	IDS / IPS	All	ASP	Syslog	9.1 and greater	
Tofino Security	**Tofino Firewall LSM (ASP)**	Firewall	All	ASP	Syslog	9.1 and greater	
Topia Technology	**Skoot (ASP)**	Application	All	ASP	Syslog	9.2 and greater	
Townsend Security	**AS/400 - CEF (ASP)**	Host / Server / Operating Systems	All	ASP	Syslog	9.2 and greater	
Trapezoid	**Trust Control Suite (ASP)**	Application	All	ASP	Syslog	9.2 and greater	
Trend Micro	**Control Manager**	Antivirus / Vulnerability Systems	3.x, 5.x, 6.x	Code Based	SQL	9.1 and greater	
	Control Manager - SQL Pull (ASP)	Antivirus / Vulnerability Systems	5.x	ASP	SQL	9.1.3 and greater	
	Deep Discovery - CEF (ASP)	Antivirus / Vulnerability Systems	All	ASP	Syslog	9.2 and greater	
	Deep Security - CEF (ASP)	HIDS	6.x and above	ASP	Syslog	9.1 and greater	
	Deep Security Manager - CEF (ASP)	HIDS	6.x and above	ASP	Syslog	9.1 and greater	
	InterScan Web Security Suite (ASP)	Web Content / Filtering / Proxies	All	ASP	Syslog	9.1 and greater	
	OfficeScan (ASP)	Antivirus / Vulnerability Systems	All	ASP	Syslog	9.2 and greater	
	OSSEC (ASP)	FIM / HIDS	1.x, 2.x	ASP	Syslog	9.1 and greater	
Tripwire	**Tripwire / nCircle IP360**	Vulnerability Systems	All	N/A	N/A	9.1 and greater	
	Tripwire Enterprise (ASP)	Database / Security Management	4.x	ASP	Syslog	9.1 and greater	
	Tripwire For Server	Database / Security Management	4.x	Code Based	Syslog	9.1 and greater	
Trustwave	**Network Access Control (ASP)**	NAC	3.x	ASP	Syslog	9.1 and greater	
	Vericept - CEF (ASP)	DLP	8.x	ASP	Syslog	9.2 and greater	
	WebDefend (ASP)	Web Content / Filtering / Proxies	4.x	ASP	Syslog	9.1 and greater	
Type80 Security Software	**SMA_RT**	Host / Server / Operating Systems	All	Code Based	Syslog	9.1 and greater	
UNIX	**Linux (ASP)**	Host / Server / Operating Systems	All	ASP	Syslog	9.1 and greater	
	UNIX OS (Solaris, Red Hat Linux, HP-UX, IBM AIX)	Host / Server / Operating Systems	All	Code Based	Syslog	9.1 and greater	
VanDyke Software	**VShell (ASP)**	Application	2.x, 3.x	ASP	Syslog	9.1 and greater	
VMware	**vCenter Server (ASP)**	Application	All	ASP	Code Based API	9.3.2 and above	
	VMware (ASP)	Application	1.x-5.x	ASP	Syslog	9.1 and greater	
Vormetric	**Data Security (ASP)**	Application	4.x	ASP	Syslog	9.1 and greater	
WatchGuard Technologies	**Firebox and X Series (ASP)**	Firewall	8.x-11.x	ASP	Syslog	9.1 and greater	
Wave Systems Corp	**Safend Protector (ASP)**	DLP	All	ASP	Syslog	9.2 and greater	
Websense	**Websense - CEF, Key Value Pair (ASP)**	Web Content / Filtering / Proxies	7.7 and above	ASP	Syslog	9.2 and greater	
	Websense Enterprise (ASP)	Web Content / Filtering / Proxies	6.x	ASP	SQL	9.1 and greater	
Xirrus	**802.11abgn Wi-Fi Arrays (ASP)**	Switches & Routers	All	ASP	Syslog	9.1 and greater	
Zenprise	**Secure Mobile Gateway (ASP)**	Security Mobile Gateway	5.x and above	ASP	Syslog	9.1 and greater	

X. Appendix B

McAfee Gold Business Support Handbook

Version 1-2011

Contents

Welcome to McAfee Gold Business Support. Our goal is to help you get the most from your products and provide your organization the best possible security. McAfee Support helps you combat today's threats , provides best practices to deploy and maintain your products, and addresses potential issues quickly and efficiently so you can focus on your business.

Product updates/upgrades

- Stay secure with the latest versions of your products – included with Gold Business Support
- Protection from the latest threats with daily updates of anti-virus signature files
- New update notifications through the Support Notification Service

Online services

- Online KnowledgeBase for easy access to solutions
- McAfee Virtual Technician to resolve many common issues automatically
- Chat and web support for opening and monitoring cases
- Online documentation and FAQs for each product
- Video tutorials showing product demonstrations and configuration walkthroughs
- Notification of changes in open support service requests

Telephone access to skilled technicians

- Support that is available 24/7, whenever a problem or outbreak may occur
- Unlimited number of calls to McAfee Technical Support
- Regular updates on the status of open cases
- Support technicians who are certified with high-skill security qualifications
- Remote debugging and re-configuration tools for rapid fault resolution
- Support in multiple local languages

Product evaluations

- Online McAfee Global Solutions Lab to test upgrades, new products, and new configurations
- Free trials of new products available for download
- New feature requests for enhancements to products

Outbreak analysis and alerts

- Submit spam or virus samples for analysis
- New threat notification

Support Terms and Conditions

For information on McAfee's Support Terms and Conditions, see:

http://www.mcafee.com/us/support/support_terms_n_conditions.html

NOTE: Some support services may not be available on all products.

Getting Started

McAfee provides a wide range of tools and resources to help you get the most from your products and ensure that any problems are resolved as quickly as possible.

Grant Number

Your Grant Number is the key to obtaining the benefits of your McAfee support, including product downloads, updates, access to the McAfee Technical Support ServicePortal and Technical Support Technicians. You should receive your Grant Number by email after purchasing a McAfee product. Your Grant Number should be kept in a safe place as without a Grant Number, it may take significantly longer to submit a support call or access online content.

If you lose your Grant Number you can re-request your Grant Number by contacting McAfee Customer Service here: https://secure.mcafee.com/apps/support/customer-service/request-form.aspx.

Setting up your ServicePortal Account

Setting up an account on the McAfee ServicePortal https://mysupport.mcafee.com/ enables you to submit online support cases, track cases, use online Chat Assistance and customize ServicePortal content.

To set up an account for the first time, click “New User” in the User Login section of the ServicePortal. You will be prompted for your name, email address, Grant Number, and preferred language. Passwords must include uppercase characters, numbers, and at least one special character.

The email address domain name you use should match all other users registered with that Grant Number. If you need to register with a different domain name, contact Customer Service.

Checking your Entitlements

Once you have logged into the McAfee ServicePortal you can check your support Entitlements by selecting View All My Company Entitlements under Interactive Support.

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Deploying your Products

Deployment Assistance Tools

Before installing a product McAfee recommends users review the tools available within the McAfee ServicePortal https://mysupport.mcafee.com to assist you in making your product deployment and configuration as easy as possible.

Product Documentation and Walkthrough Guides

The Product Documentation link on the McAfee ServicePortal provides access to product release notes, installation guides and product guides by product, allowing users to quickly obtain important information of their products.

Quick Tip Videos

The McAfee Multimedia Library hosts a number of quick tip videos that cover some of the useful configuration and installation options f deploying McAfee products.

http://www.mcafee.com/apps/view-all/multimedia.aspx

Online Evaluation Environments

The Global Solutions Lab (GSL) gives you hands-on access to test the deployment and upgrading of McAfee products in virtual environments before deploying to a live environment. These environments allow you to walk through a full product upgrade to familiarize yourself with any changes and enhancements and to mitigate any possible issues you might encounter.

Register using your email address at https://www.mcafee.com/gsl.

Training and Professional Services

If you would like assistance with your deployment or checking the health of your installation McAfee offers a number of professional services. For on-site assistance contact McAfee Solution Services at solution_Services@mcafee.com

Smaller organizations can use our QuickStart services http://www.mcafeequickstart.com/ that offer remote deployment and health check services.

McAfee also provides a number of comprehensive online and classroom training courses, for more information visit:
http://www.mcafee.com/us/enterprise/services/education/index.html

Downloading Your Products

McAfee constantly enhances its products to combat new attacks and prevent data loss. Regularly upgrading products ensures that systems have the maximum level of protection, while minimizing the possibility of encountering an issue that has already been addressed in a later version.

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

McAfee Downloads Portal

McAfee software can be downloaded from the McAfee Downloads portal. Authenticate with your Grant number to display all of the products available for download under your support contract.

http://www.mcafee.com/us/downloads/

Patches and Hotfixes

Software updates for most McAfee products are available from the ServicePortal. Click the **Download Product Updates** link under **Self-Service**.

To access software patches and upgrades for former Secure Computing products, see:
https://www.securecomputing.com/index.cfm?skey=246

Hardware Support

McAfee Hardware Technical Support provides a maintenance program for service and repair of McAfee appliances. There are several Hardware Support Programs available to assist customers with the peace of mind to have their appliance diagnosed quickly in the event of a failure or other issue. For more information on McAfee Hardware Support, see:

http://mcafee.com/us/local_content/datasheets/hardware_support_user_guide.pdf

Activations

Some McAfee products including McAfee Firewall Appliances, McAfee SmartFilter, and McAfee Web Reporter require activations.

If your product requires activation, go to:
https://www.securecomputing.com/index.cfm?skey=231

Configuring ePolicy Orchestrator for Updates/Upgrades

McAfee recommends that you use McAfee ePolicy Orchestrator® (ePO™) to automate the deployment of your McAfee software, updates, and virus definitions. For instructions on how to deploy updates via ePolicy Orchestrator, see the ePolicy Orchestrator Product Guide.
https://mysupport.mcafee.com/Eservice/productdocuments.aspx

A QuickTips video walkthrough is also available:
http://www.mcafee.com/us/resources/tutorials/epolicy-orchestrator-quicktips-video.html

Keeping your Products Current

To address the constantly evolving threat landscape and deliver the most innovative and cost-effective products, McAfee regularly releases new product versions and discontinues old ones.

To ensure you are using the most current product version, see:

https://www.mcafee.com/us/enterprise/support/customer_service/end_life.html

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Staying Protected

To keep you up to date on the latest threats and product updates, McAfee offers a number of alerting services and online resources.

Alerts

Support Notification Service

The Support Notification Service (SNS) delivers product information to you by email — End of Life, patch and upgrade notifications, threat reports, DAT notices, and critical alerts that require immediate attention. This information helps you get the most out of your McAfee security investment — and helps you avoid problems by keeping you up to date.

To sign up for SNS, go to:

http://my.mcafee.com/content/SNS_Subscription_Center

McAfee Labs Security Advisories

McAfee Labs Security Advisories are notifications created by the global research team to map high-profile threats to the McAfee technologies that remediate against that threat.

Sign up for McAfee Labs Security Advisories at:

https://www.mcafee.com/us/threat_center/securityadvisory/signup.aspx

McAfee Labs DAT Notification Service

McAfee Labs DAT notifications inform you when DATs are ready to download. Every Monday through Friday, McAfee Labs posts the latest DATs to ensure that your product contains the most up-to-date detection and repair capabilities. In the event a security threat is discovered and McAfee Labs assigns a risk assessment to the threat that is Medium or above, you will be notified of the emergency DAT posting.

Sign up for the McAfee Labs DAT notification service at:

https://secure.mcafee.com/apps/mcafee-labs/dat-notification-signup.aspx

McAfee Labs Threat News

McAfee Labs Threat News is a notification about the latest information regarding threats that reach Low-Profiled, Medium, Medium-On-Watch, High, or High-Outbreak assessment levels. Details on the classification of threat levels are available at:

https://www.mcafee.com/us/threat_center/outbreaks/virus_library/risk_assessment.html

Sign up for McAfee Labs Security Advisories at:

http://www.mcafee.com/apps/mcafee-labs/signup.aspx

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Online Resources

McAfee Threat Center

The McAfee Threat Center provides a comprehensive list of top vulnerabilities and threats. It also contains links to useful tools for virus removal and McAfee Foundstone® tools that can simulate a vulnerable site to highlight common weaknesses.

The McAfee Threat Center includes:

- Sage journal—McAfee Labs' security journal, which provides insights into future security threats
- McAfee AudioParasitics—Podcasts on the latest threats
- McAfee Labs blog—Blogs from McAfee malware researchers
- Current malware and vulnerability descriptions—Rankings on the latest threats

Visit the McAfee Threat Center at:

https://www.mcafee.com/us/threat_center/default.asp

McAfee TrustedSource

The McAfee Trusted Source website provides precise information about email sender reputation by domain and IP address. It provides you with a view into current and historical reputation and sending patterns of sends, as well as analytical information such as country of origin, network ownership, and hosts for known senders within each domain.

It also includes a URL checking tool that provides status, categorization, and web reputation information for URLs in the TrustedSource Web Database (URLs organized into categories and reputation ratings for use in web filtering policies). You can also suggest categorization changes for URLs.

Visit TrustedSource at:

http://www.trustedsource.org

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Online Access to Definition Files

Many McAfee products require definition files, or DATs. The DATs contain the information that the anti-malware engine requires to properly detect threats and clean infections. The table below describes the various types of DAT files and when they are issued or used.

DAT type	Description
Daily DAT	The daily DATs contain only the latest virus information (with no scan engine) and are updated on a daily basis. Daily DAT files are downloaded automatically by your McAfee products. If you need to download a copy of the latest daily DATs, go to: http://www.mcafee.com/apps/downloads/security-updates/security-updates.aspx
SuperDAT	A SuperDAT is a one step executable update for your regular DAT files and the anti-malware engine used by your product. A SuperDAT can be used to update the DATs and engine when other update methods have failed, or if a system must be taken off the network. To download SuperDATs, go to: http://www.mcafee.com/apps/downloads/security-updates/security-updates.aspx
Beta DAT	Beta DATs are hourly builds of the daily DAT files with additional malware definitions that have been received recently. Beta DATs receive limited false positive testing and are recommended for use primarily on high risk systems or when an infection is not detected by the daily DATs. To download Beta DATS, go to: http://www.mcafee.com/apps/mcafee-labs/beta/dat-file-updates.aspx
Extra.DAT	Extra.DATs are temporary definition files delivered directly by McAfee Labs in response to submitted malware that is not yet covered in the daily DAT files. Extra.DATs are intended to provide emergency coverage until the new malware can be incorporated into the daily DATs. Extra.DATs automatically expire and are deleted when the extra detections are added to the daily DATs.

In addition to the regular DAT files, several McAfee products such as VirusScan Enterprise make use of our Global Threat Intelligence technology. Global Threat Intelligence supplements detection in the DAT signatures with real-time behavior analysis. You can reduce your company's potential exposure to threats by enabling this feature.

How it works

1. A user receives a file that the scan agent deems suspicious (for example, an encrypted or packed file) and for which there is no signature in the current local DAT files.
2. Using Global Threat Intelligence, the agent sends a fingerprint of the file for instant lookup in the comprehensive real-time database at McAfee Labs.
3. If the fingerprint is identified as malicious, an appropriate response is sent to the user to block or quarantine the new threat.

Getting Help

Customer Service

Non-technical questions regarding licensing and support entitlements, such as recalling a forgotten Grant Number can be addressed by McAfee Customer Service via telephone or online submission, or review the most common customer issues at:

http://www.mcafee.com/us/support/customer-service-faq.aspx

Frequently Asked Questions about products formerly provided by Secure Computing can be found at: https://www.securecomputing.com/index.cfm?skey=297

Online Technical Resources

In addition to the features covered in the Deployment Assistance Tools section of this document, McAfee also provides online tools to resolve issues quickly and easily. The McAfee ServicePortal (https://mysupport.mcafee.com) is your starting place for a comprehensive, searchable collection of support tools, including the KnowledgeBase, product documentation, and software downloads. Make sure you log in to get the most value from the ServicePortal.

KnowledgeBase

The McAfee KnowledgeBase contains over 15,000 articles and provides a quick and easy way to find resolutions to your questions. It offers a powerful search feature and quick links to top searches, recently added content, common issues.

The **Search the KnowledgeBase** link on the McAfee ServicePortal provides the ability to use a query based search to find solutions to questions about McAfee Products. Query results can then be refined using filters on the left side of the page.

Up to 50 articles can be flagged as favorites on the KnowledgeBase home page, by clicking “Add to Favorites” at the top of an article. To removing an article from your Favorites, click My Favorites on the right side of the page, then click Remove beside the article name.

You can also **Browse the KnowledgeBase** by product and version.

McAfee Community

The McAfee Community enables you to connect with other customers to learn and share solutions about McAfee products. Community members can post discussions, form user groups, share documents, and write blog posts. You must register to post, so join today!

Visit the McAfee Community at http://community.mcafee.com.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

How to Submit Virus or Malware Samples to McAfee Labs

When submitting a sample to McAfee Labs for review, you may use either of two delivery methods:

- **McAfee ServicePortal**
  This is the preferred method for McAfee Labs to receive submissions from customers. When you use this method we can process and respond to samples more rapidly. You'll find instructions for using the McAfee ServicePortal/Platinum Portal in McAfee KnowledgeBase article **KB68030**.

- **Email**
  You can submit samples directly to McAfee Labs by attaching the file(s) in an email to virus_research@mcafee.com. When submitting samples via email, you must archive them in a password-protected Zip file with the password "infected" (all lowercase). For instructions on how to create a Zip file and password protect it, see these Microsoft articles:

  Using WinZip

  Using Windows File Compression

Submission Information

To help us speed the sample review process, please provide the following information along with your sample:

- A list of all files contained in the sample submission, including a brief description of where or how you found them
- What symptoms cause you to suspect that the sample is malicious
- Whether any security products find a virus (tell us the security vendor, its product name, the version number, and the virus name assigned to the sample)
- Your McAfee product information (product name, engine, and .DAT version)
- Any system details that may be relevant, including operating system and service packs

Finding Samples to Submit

McAfee KnowledgeBase Article KB53094 can assist customers in finding malicious samples on their systems.

What Not to Submit

Please do not send screenshots, anti-virus or HijackThis logs, or prefetch files through McAfee ServicePortal/Platinum Portal or email. Send only the suspected malicious files.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Automatic Diagnosis and Remediation

One of the quickest ways to resolve a technical problem is with McAfee Virtual Technician (MVT). This is an automated tool can determine if McAfee products are installed, updated, and working correctly. An easy-to-follow interface allows for a seamless experience. Issues are proactively diagnosed and resolved where appropriate.

MVT can be run remotely on a client device using ePolicy Orchestrator (ePO-MVT)

https://kc.mcafee.com/corporate/index?page=content&id=PD22556

MVT-ePO packages can be downloaded here

http://mer.mcafee.com/enduser/downloadepomvt.aspx

MVT also can be manually executed on a client machine using http://mvt.mcafee.com from that client.

For detailed information on how to use MVT and a list of supported products, see:

https://mvt.mcafee.com/mvt/Documents/WalkThruGuide/en-us/MVTWalkThroughGuide.pdf

Endpoint Encryption Code of the Day

Customers with McAfee Endpoint Encryption who need to access to certain functions within the McAfee device encryption disaster recovery toolkit (SafeTech/WinTech toolkit), require a unique code that changes on a daily basis.

To access the Endpoint Encryption Code of the Day, log into the ServicePortal https://mysupport.mcafee.com and select **Endpoint Encryption Code of the Day** under **Additional Services** on the website banner.

Minimum Escalation Requirements (MER) Tool

The MER tool is a utility for collecting McAfee product and general system information to assist our technicians with diagnosing issues. The information collected by the MER tool includes an MSD report (or other OS equivalent), event logs, McAfee registry keys, McAfee log files, and current McAfee .EXE files. The exact files collected will differ by product and version. After the tool collects the necessary data, it will create a .TGZ (compressed) file you can send to our technician to analyze or escalate.

The MER tool is updated regularly. Download the latest version at:
https://kc.mcafee.com/corporate/index?page=content&id=KB59385

For additional information on how to use the MER tool, see:
http://mer.mcafee.com/enduser/lang/English/WebMERWalkthrough.pdf

Due to limitations in some operating systems and other concerns, the MER tool is not available for all products.

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Assisted Technical Support

If you require assistance from a Support Technician McAfee Gold Business Support provides Online Service Requests, Chat, and Telephone support. To help us resolve your issue as quickly as possible, please ensure that you have the following information available:

- Technical Support Grant Number
- Geographic location of the software installation
- Detailed description of the problems or errors
- Description of the hardware that the software is installed on, including the serial number or service tag where applicable (hardware must meet published McAfee specifications)
- Name and versions of any operating system, network, and software running with the McAfee software, including patches and fixes
- Minimum Escalation Requirements (MER) tool output (optional)
- If your service request needs to be escalated to a higher level of support you may be asked for additional files or details on your installation.

Service Request Number

A Service Request Number will be created for each new case opened and should be quoted on all queries regarding that request.

The status of open Service Requests can be viewed by logging into the ServicePortal https://mysupport.mcafee.com and selecting “View my open Service Requests” under “Interactive Support”.

Details for a specific service request can be viewed by clicking it on the status field. In the Updates section, you can see comments added by Support or add information that may help us resolve your issue.

Create an Online Service Request

To create a new Service Request, log in to the ServicePortal and click **Create a Service Request**. Complete all of the required fields and attach any additional log files or information that will assist your support technician.

Use the ServicePortal to submit non-critical issues. If you have a Severity 1 or 2 issue, please use phone support.

A McAfee support technician should respond to your service request within 24 hours.. Depending on the complexity of the issue, the technician may contact you by phone.

McAfee Support will make three attempts to contact you, each at least one business day apart. If we receive an out-of-office notification, we will postpone follow up attempts for that period. After three unsuccessful attempts, we will assume that your issue is resolved and send a notification that the request has been closed. You can call McAfee Support at any time within the next 30 days to reopen the request.

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Checking the Status of your Service Requests

The McAfee ServicePortal offers several options for viewing the status of your Service Requests.

- View My Open Service Requests
- View All My Service Requests
- View All My Company Service Requests

Chat Support with Remote Assistance

Log in to the ServicePortal to use chat support. You can use chat to check the status of existing cases or work with a technician for interactive problem solving. Currently, chat support is offered in English only and is not available for all products.

After you initiate a chat session, a chat window opens and gives a status on where you are in the queue. The chat window allows you to discuss your issue with a technician, and it also allows you to send files to the engineer.

With your permission, McAfee technical support technicians can also open a remote control/share connection to view your desktop and work directly with you to diagnose and resolve issues.

Phone Support

McAfee Gold Business Support provides telephone access to our technical support technicians 24 hours a day, 365 days a year. Commercially reasonable effort is made to provide local language support in most countries during business hours, and in English at other times. Local language phone support my not be available for all products. To use phone support you will be asked to provide your McAfee Grant number.

Check the McAfee website at https://www.mcafee.com/us/about/contact/index.html for the latest Technical Support telephone numbers for your country.

Quality assurance through our Witness program

McAfee Technical Support strives to provide the best possible service and has invested in a comprehensive call management tool that enables management and the business excellence team to recover all details regarding a specific case. The Witness tool records data as it is entered into our system, including engineers' keystrokes and mouse positions, and it synchronizes this with the recorded call or chat session. This information is used to provide feedback to our engineers for training on best practices.

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Customer Feedback Program

McAfee is committed to delivering world-class customer service and support and has partnered with industry leader Walker Information as part of our Customer Feedback Program.

Customer Satisfaction Surveys are sent out at the closure of service requests in the form of a web-based survey delivered via an email invitation from support@walkerinfo.com. Not all service requests will generate surveys to limit the number of emails sent to a given customer.

The information in the survey is confidential and is used only for improvements in the service that McAfee provides and to ensure that you are satisfied with the service you received. Survey information is not shared with any entity outside of McAfee.

McAfee®

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Response Charter

McAfee Gold Business Support customer Service Requests begin at the Tier I support level and are assigned a Service Request number to manage the resolution of the issue. We attempt to resolve every issue on the first call. Unresolved customer issues are evaluated based on severity and priority of resolution. Based on this information, they are assigned an impact level value.

If tier resources have been exhausted or the issue is assigned a high-impact level, it is escalated to successive tiers as needed for resolution. Each tier in the McAfee Support organization will use all available resources to resolve the customer issue. These processes apply to all Service Requests that are escalated within the McAfee Technical Support organization.

Escalation and response times

Depending on the severity level, the McAfee response charter sets out clear guidelines as to how frequently you'll be contacted by our technicians about the status of a service request. The charter also provides the maximum duration a Service Request can be open before it is automatically escalated to the next tier.

Severity	Tier I Response (Phone)	Tier I Escalation to Tier II	Tier II Escalation to Tier III	Tier III Escalation to Development	Status Updates
1. Business has stopped	Average under 5 minutes	30 minutes	30 minutes	4 hours	Continuous phone bridge
2. Business is severely impeded	Average under 5 minutes	2 hours	2 hours	6 hours	Hourly
3. Business impeded but functioning	Average under 5 minutes	3 days	5 days	5 days	Daily
4. Business not affected, symptoms exist	Average under 5 minutes	10 days	15 days	25 days	Weekly
5. Request for information	Average under 5 minutes	15 days	20 days	30 days	Every two weeks

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Severity definitions

McAfee defines the “severity” of an issue based on how it impacts your ability to conduct business. A severity code is associated with all service requests, failures, and enhancement requests to indicate the impact and the urgency of the request.

Severity 1—Business has stopped

- Your organization cannot conduct business or business is severely impacted
- The product is not functioning
- Internet connectivity or email flow has stopped
- Your organization is unable to provide available virus protection to the network
- There is no viable workaround for this issue

Severity 2—Business is severely impeded

- Your organization’s business is impeded but can continue to operate
- A major product feature, such as reporting or updating, is not functioning
- There are widespread symptoms across your organization’s infrastructure
- Issues include installation failures, conflicts with major brand software, or specific email flow problems
- Your organization is generally able to provide available virus protection to the network, but specific resources cannot be updated

Severity 3—Business is impacted, but your organization can function normally

- Your organization’s ability to conduct business is not affected
- Symptoms affect a single system or isolated parts of the environment
- Specific functionality is not working

Severity 4—Business is not affected, but there are noticeable problems

- Your organization’s ability to conduct business is not affected
- Symptoms affect only a few systems
- Functionality loss has an easy workaround

Severity 5—Requests for information or feature modifications

- Requests for product documentation or other information that does not require troubleshooting and issue resolution
- Requests for modifications to the functionality or design of McAfee products

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Premium Support Offerings

McAfee strives to provide the highest level of service with McAfee Gold Business support but some customers with complex or mission critical environments can reduce their own internal support costs by choosing a more proactive and personalized support solution.

Gold Enhanced Business Support

Ideally suited for businesses with more complex security environments that could normally take longer to identify root causes and resolve problems. Gold Enhanced Business Support provides all of the benefits of Gold Business Support, but also included direct access to Product Specialists. Their expertise and security knowledge ensure that your complex issues are resolved quickly to minimize risk to your business.

Platinum Enterprise Support

Enterprises worried about business continuity and compliance need a higher level of accountability and predictive support. An assigned Support Account Manager (SAM) provides personalized support, risk assessments, proactive advice, and escalation for complex technical issues. Customers also gain the benefit of direct access to Product Specialists for detailed technical assistance on their products.

Platinum Global Enterprise Support

Platinum Global Enterprise Support is ideal for multi-national organizations centrally managed from a headquarters location. An assigned Global Support Account Manager provides centralized account management in addition to Product Specialists in each region. By leveraging our support Product Specialists worldwide, we resolve issues faster, anytime, anywhere. We will provide you with complete product, technical, and problem-solving expertise when and where you need it.

Platinum Large Enterprise Support

Tailored to large and complex organizations focused on minimizing disruptions and reducing their total cost of ownership. The Large Support Account Manager acts as an extension to your IT security team, working closely with them on solutions planning assistance, pre-emptive advice, and direct intercession on your behalf for the fastest possible resolution to complex technical issues. Assigned Product Specialists are on call to provide detailed technical assistance when required.

Platinum Resident Enterprise Support

Organizations requiring the highest level of pre-emptive assistance to manage their complex environments gain significant benefit from a dedicated Resident Support Account Manager or Product Specialist embedded with their IT security team. An onsite expert can engage directly with pre-deployment planning and best practice to maximize protection and minimize risk.

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Additional Services

Solution Services

Many customers do not have the time or resources to fully deploy their security products, McAfee Professional Services can help you quickly realize the full value of your McAfee security solution and accelerating your return on investment. Additionally an improperly configured security product could result in reduced protection, increased vulnerability to attack and degradation of system performance. McAfee Professional Services consultants provide onsite assistance utilizing their extensive experience in deploying McAfee products

http://www.mcafee.com/us/services/solution-services/index.aspx

Quickstart Services

Smaller organizations can use benefit of security experts for installation, deployment, configuration, or fine-tuning assistance with McAfee's Quickstart services. These experts can remotely connect to your system and take the effort out of implementing, optimizing and configuring your McAfee security solutions

http://www.mcafeequickstart.com/

McAfee Product Education

Learn the real-world skills you need to effectively fight today's attacks and tomorrow's threats. McAfee Product Education combines hands-on experience with expert instruction so you can get the most from your McAfee security products.

http://www.mcafee.com/us/services/solution-services/index.aspx

Foundstone Consulting

Foundstone is the pre-eminent leader in network security consulting, serving hundreds of high profile organizations in the Fortune 500, federal and state governments, and the military. Our bonded consultants are recognized experts, educators, and technical authors who can assist in Network Assessments, Health checks and Software and Application Services (SASS)

http://www.mcafee.com/us/services/mcafee-foundstone-practice.aspx

Strategic Security Education

Give your in-house security team the tools and methodologies they need to defend your business. Foundstone combines interactive classroom demonstrations with hands-on labs. Your students leave armed with a real-world understanding of critical security issues, and how to address them.

http://www.mcafee.com/us/services/strategic-security-education/index.aspx

McAfee®
McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

Feedback on This Document

If you would like to see additional information included in this guide or you discover any errors, please contact us at customer_feedback@mcafee.com. We welcome your feedback!

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

XI. Appendix C

Privacy Notice

This Notice provides information about data we use for security purposes and our commitment to using the personal data we collect in a respectful fashion.

Go here for our complete notice.

McAfee Privacy Notice

McAfee and its family of companies ("McAfee", "we", "us") are wholly owned subsidiaries of Intel Incorporated. We care deeply about your privacy and security and your safety is a significant part of our essential mission. We appreciate your decision to trust us with helping to protect your digital life from theft, disruption, and unauthorized access to your personal information and systems.

This privacy notice is designed to inform you about how your personal information is collected, managed, and used to:

- Safeguard devices and data
- Manage our relationship with you
- Improve security products and services to predict future vulnerabilities
- Protect data

By collecting and processing data, we can help to predict threats and protect you, your devices and your information. McAfee is committed to becoming as transparent as possible to help you understand how your data is processed, why it takes data to protect data, and our commitment to using the personal data we collect for the purposes discussed in this Notice. Every time you turn on a device, connect to a network or open a file, you face significant risk from hackers, spammers, malware, spyware and other forms of unauthorized access to your data. This is why it is important to use security products and services such as McAfee's.

To defend against these threats and the thousands of new threats that emerge each day, McAfee technologies may:

- Analyze data sent to your devices for signs of risk or suspicious activity in order to take corrective action
- Assess the reputation of the sending device to determine whether access should be allowed or if the transaction should be continued;
- Adapt responses to new threats based on intelligence from our global network. .

Please read about our privacy practices and let us know if you have any questions.

Scope

This Privacy Notice applies to personal information we obtain from individuals interacting with McAfee and its websites, products, services, and applications. This Notice does not apply to personal information we obtain in our capacity as an employer.

Notice

We provide access to our Privacy Notice by:

- Linking to it throughout our websites
- Referencing it in our terms of use and end user license agreements
- Incorporating it into our contracts and other legal agreements as necessary

The Information we collect

McAfee collects some information that is personal (i.e., information that identifies an individual either alone or in combination with other data). McAfee also collects non-personal information that does not, on its own, identify an individual person. When non-personal information is combined with other information so that it does identify an individual person, we treat that combination as personally identifiable information.

McAfee collects personal information when you or someone acting on your behalf provides it to us. We also collect information when you obtain or use McAfee products, services or when you communicate with a device using McAfee's services.

The following are examples of the type of personal information that may be collected, directly from you (or someone acting on your behalf)

- Contact information (including name, email address, mailing address, telephone and fax number)
- Payment information (including payment card and bank account information);
- Shipping, billing and other information provided in connection with the purchase or shipment of McAfee products and services;
- Information about transactions with us (such as purchase history) and use of our products and services;
- Information provided by you through McAfee-related communication channels such as forums, technical support, and customer service;
- Username, password and other information used to verify identity; and
- Photographs or other biometrics when submitted

The following are examples of the type of information that may be collected by McAfee, from your web browser or from interactions with our products and services:

- Details about your computers, devices, applications and networks (including IP address, browser characteristics, device ID and characteristics, device operating system information and system language preferences);
- activities on our websites and usage patterns of products and services; referring URLs, dates and times of website visits, and clickstream data such as information commonly recorded in web server logs; and
- details about Internet or network usage (such as the URLs or domain names of websites you visit, information about applications that attempt to access your network, or traffic data);
- data about files and communications, such as potential malware or spam (which may include computer files, emails and attachments, email addresses, metadata and traffic data related to files and communications, or portions or hashes -- a hash file is a file that has been converted into a numerical string by a mathematical algorithm -- of any of this information); this may include similar information from third parties interacting with you;
- other information used in the operation of our products and services (such as information regarding the number of checked, suspicious, infected or unwanted files or emails; the number of malware infections); and
- Information that may be included in a virus or malware sample or a file you consider to be suspicious that you submit to McAfee for review.

IP Addresses

An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device (e.g., computer, printer, server) participating in a computer network that uses the Internet Protocol for communication. It is how devices such as computers find each other on the network.

Where it is sometimes possible that IP addresses can be associated with a single individual's system, they most often are associated with a group of systems, one system shared by many users or a gateway into a group of systems or devices. For instance, IP addresses included in an email communication are typically associated with the respective email service provider and not with your device.

McAfee security products and services, like those of many security companies, depend on IP addresses to protect your information, your devices and your privacy. For example, we may detect that a system or a group of systems associated with a particular IP address has been compromised and is sending malware or spam to some of our users.

Even without identifying who owns a compromised system or who compromised it, we can assign a score to that IP address to reflect the heightened threat it poses. Our products and services can then divert your traffic away from this IP address or block this IP address from sending malware to your McAfee-protected device before your device is a victim of an attack.

The use of IP addresses and other machine data is critical to the ability to keep security protections current, relevant and effective as cyber threats and attacks evolve over time.

McAfee protects the collection of IP addresses – regardless of whether they are associated with any particular individual's system or a group of systems. We do not use IP addresses that our security tools gather for marketing purposes such as online behavioral advertising or to push marketing messages.

Cookies

McAfee uses "cookies" to remember user preferences and to maximize the performance of our website and services. Additionally, cookies help us to identify returning users so, for example, we don't need to ask them to enter their email and password on every visit.

Please note the information gathered by cookies is necessary to provide some McAfee services, including certain subscriptions. We do not provide those services to users who do not give their consent to the data processing carried out through cookies or whose browsers are set to reject all cookies. For example, when you purchase a subscription to an online technology, a cookie is set that identifies the version of the protective software and when it expires. We use this information to alert you that a newer version is available or if your subscription is going to terminate and, thus, leave your system open to attack.

Cookies may also be used to control the type and/or frequency of ads, promotions, or other marketing messages the customer views. These ads may be placed by third-party advertising companies which are our vendors McAfee also uses "web beacons" (small transparent image files) to count visitors to our sites and analyze how visitors use our sites. The information collected is generally anonymized and is not used to identify any particular user.

As is common on the Internet, McAfee maintains log files of the traffic that visits our sites. For example, our servers may automatically record the information you or your browser send when you visit a website. These log files may include information such as your requests, IP address, browser type, browser language, the date and time of your request, and one or more cookies that may uniquely identify your system.

Use of the Personal Information we collect

McAfee uses the information it collects in ways that serve your security and privacy needs, including the following:

- Provide threat prediction and protection products and services;
- Provide security advisories, information and product updates;
- Conduct research and analysis (for example, market and consumer research, security research and analysis, and trend analysis);
- Analyze users' behavior when using McAfee products and services to customize users' preferences;
- Establish and manage McAfee accounts;
- Collect and process payments and complete transactions;
- Provide customer support, manage subscriptions and respond to requests, questions and comments;
- Communicate about, and administer participation in, special events, programs**,** surveys, contests, sweepstakes, and other offers and promotions;
- Enable posting on our blogs and other communications;
- Customize, measure, and improve our websites properties and advertising;
- Analyze and develop new products, services and websites;
- Perform accounting, auditing, billing, reconciliation and collection activities;
- Prevent detect, identify, investigate, and protect against potential or actual claims, liabilities, prohibited behavior, and criminal activity;
- Comply with and enforce applicable legal requirements, agreements and policies; and
- Perform other activities consistent with this Notice.

Products and Services Data Processing

If you use one of our products or services, software will operate in the background of your computer system or device environment to perform specific security and privacy protections including:

- Spam protection
- Virus protection
- Intrusion protection
- Threat Prevention and Prediction
- Home Network Defense
- Data Encryption
- Mobile Device Lockdown

Product Updating and Reporting

Our products and services may also process certain data to provide updates and reports. These update functions may check your system to see whether files relating to the services need to be refreshed or modernized.

For example, products and services may transmit report files to McAfee. These files contain information, including the number of checked, suspicious, infected or unwanted files or emails, the number of infections, the date and hash values of the detected infections and the number of false negatives/false positives. The purpose of these reports is to analyze the frequency of particular infections or the prevalence of threats. McAfee will also adapt the product where necessary to user preferences based on actual use of the product.

Personal Information We Share

We may share personal information with:

- Other members of the McAfee family of companies for the purposes described in this Privacy Notice, such as to (i) provide services and joint content (such as registration, sales, and customer support); (ii) help detect and prevent potentially illegal acts and violations of our policies; and (iii) guide our decisions about our products, services and communications.
- Service providers and authorized partners who perform services for us (such as data storage, sales, fraud investigations and bill collection) based on our instructions. These third parties are not authorized by us to use or disclose personal information except as necessary to perform services on our behalf or comply with legal requirements.
- Third parties with your consent. For example, co-marketing with a business partner or sharing limited information as necessary with security research analysts;
- Other business entities legally related to McAfee, such as our parent company, Intel, Inc. or any third party that may take over all or part of McAfee's functions in the future (provided that such party agrees to use such personal information in a manner that is consistent with this Privacy Notice). Should a further combination occur, we will require that the new combined entity follow this Privacy Notice with respect to your personal information.

We may also disclose personal information (i) if we are required to do so by law or legal process ; (ii) in response to requests by government agencies, such as law enforcement authorities or other authorized third-parties; (iii) as may be required for purposes of national security; or (iv) when we believe disclosure is necessary and appropriate to prevent physical, financial or other harm, injury or loss or in connection with an investigation of suspected or actual illegal activity or exposure to legal liability.

McAfee will not disclose your personal information to non-affiliate third parties for their own marketing purposes unless you have provided consent.

McAfee family companies may share personal information with each other and use it in a manner that is consistent with this Notice. We may also combine it with other information to provide and improve our products, services, content and advertising.

Where we share this personal information with a third party with a contractual relationship with us (such as a provider of services to McAfee) these entities must comply with standards at least as stringent as McAfee's processing standards and are limited to those standards unless you wish to create your own independent relationship with that provider.

California Shine the Light Law

McAfee does not share your personal information with third parties for their own marketing use without your permission.

Security

We use administrative, organizational, technical and physical safeguards to protect the personal information we maintain and ensure it is used according to this Notice. Our security controls are designed to restrict access to the information to authorized personnel only. We regularly test our website for security vulnerabilities. When you make a payment on our website using your credit card, we use SSL encryption in the transmission to McAfee of the credit card number. We require Service Providers maintain at least the same level of security we expect of ourselves.

McAfee complies with the Payment Card Industry Data Security Standard that requires merchants to implement security measures for credit card information.

How you can manage and control your personal information

We offer certain choices about how we communicate with our users and what personal information we obtain about them. Many McAfee products allow users to make choices about the personal information collected.

- You may choose not to receive marketing email communications from us by clicking on the unsubscribe link or other instructions in our marketing emails, visiting the My Account section on our website or contacting us as specified in the "How to Contact Us" section below.

- Many McAfee products contain settings that allow users or administrators to control how the products collect information. Please refer to the relevant product manual or contact us through the appropriate technical support channel for assistance.

- To remove your personal information from a McAfee website testimonial, please contact customer service.

If you chose to no longer receive marketing information, McAfee may still legitimately communicate with you regarding such things as security updates, product functionality, responses to service requests or other transaction related communications.

How you can access and correct inaccuracies

If you wish to contact us in relation to any personal information you may request access to such information so that we can correct or amend the information by contacting us as indicated below. In certain circumstances we may be required to retain data we have about you (such as for tax or other business purposes or if required by law or by authorities).

Data Retention

The time periods for which we retain your personal information depend on the purposes for which we use it. McAfee will keep your personal information for as long as you are a registered subscriber or user of our products and, thereafter, for no longer than is reasonably necessary for internal reporting and reconciliation purposes pursuant to legal requirements and to provide you with any feedback or information you might request or require.

Storage of the information we collect from you

The information we collect may be stored in servers in the United States and wherever McAfee and its service providers have facilities, as well as your web browser (see section on cookies above).

Children's Privacy

McAfee complies with the Children's Online Privacy Protection Act of the United States of America where it applies to our information protection activities. McAfee does not knowingly collect personal information from children under the age of 13. If we learn we have collected personal information on a child under the age of 13 without proper consent, we will delete that data from our systems.

Data Transfer

We may transfer the personal information we obtain to countries other than the country in which the information originally was collected. Those countries may not have as comprehensive data protection laws as the country from which McAfee initially obtained the information. When we transfer the information to other countries, we will protect that information as described in this Privacy Notice.

If you are located in the European Economic Area or Switzerland, we comply with applicable legal requirements providing adequate protection for the transfer of personal information to countries outside of the EEA or Switzerland. McAfee is certified under the Safe Harbor privacy framework as set forth by the U.S. Department of Commerce, the European Commission and Switzerland regarding the collection, storage, use, transfer and other processing of personal data transferred from the European Economic Area or Switzerland to the U.S. Click here to view our Safe Harbor Certification

Updating the Privacy Notice

We may update this Notice at any time by posting additions or modifications on this web page. If at any point we decide to use personal information in a manner materially different from that stated at the time it was collected, we will notify users by email or via a prominent notice on our website, and where necessary we will seek the prior consent of our users.

Links to Other Websites

Our websites may contain links to other websites for your convenience and information. These websites may be operated by companies not affiliated with McAfee. Linked websites may have their own privacy policies or notices, which we strongly suggest you review if you visit any linked websites. We are not responsible for the content of any websites that are not affiliated with McAfee, any use of those websites, or the privacy practices of those websites.

In certain circumstances, where the information of third parties is collected by us by virtue of the third-party's interaction with you (such as the information of those individuals who send communications to your computer), we rely on you to provide the relevant third parties with any requisite notice and to obtain any requisite consent.

Your agreement to our Privacy Notice

You expressly consent to McAfee's processing of information as described in this Privacy Notice when you:

- Provide information to us through our websites;
- Buy or license our products or services and accept the terms of user or end-user license; or
- Sign a contract with McAfee for products and services.

In addition, through these uses and interactions with McAfee Products, Services or Websites, you specifically consent to our collection of personal information by automated means, such as cookies or the intended functionality of a product or

service, and to our subsequent processing of the information in accordance with this Privacy Notice and to the storage and transfer of the information to locations wherever McAfee and its service providers have facilities.

Contact Us

If you have questions or concerns regarding this Privacy Notice, or would like to update information we have about you or your preferences, please contact us by:

- Emailing the Privacy Program Office of McAfee, Inc. at privacy@mcafee.com;
- Calling us at 972-963-7902;
- Writing to us at:

Privacy Program Office - McAfee, Inc.
2821 Mission College Blvd.
Santa Clara, CA 95054

If you do not receive a response, contact the Consumer Privacy Response Team of McAfee, Inc. by emailing consumer_privacy_response_team@mcafee.com or by writing to Consumer Privacy Response Team, 5000 Headquarters Drive, Plano, Texas 75024.

If you are located in the European Economic Area, please write to:

Privacy Program Office - McAfee Security S.A.R.L.
26, Boulevard Royal
2449 Luxembourg, Luxembourg

In addition to McAfee, Inc., the McAfee entity with which you have a business relationship is responsible for ensuring your personal information is collected and processed according to this Notice.

For the U.S., Mexico, Central America, South America, and the Caribbean, this is: McAfee, Inc., 2821 Mission College Blvd., Santa Clara, California 95054

For Canada, Europe, the Middle East, Africa, Asia, and the Pacific Rim, this is: McAfee Security S.A.R.L., 26, Boulevard Royal, 2449 Luxembourg, Luxembourg

For Japan, this is: McAfee Co., Ltd., Shibuya Mark City West Building 12-1, Dogenzaka 1-Chrome, Shibuya-ku, Tokyo 150-0043, Japan

Last Modified December 19, 2012.

To view previous version, click here.

JAMES MADISON UNIVERSITY

March 13, 2014

ADDENDUM NO. TWO

TO ALL OFFERORS:

REFERENCE:	Request for Proposal No:	**RFP# MLO-773**
	Dated:	**February 12, 2014**
	Commodity:	**Security Incident and Event Management System**
	RFP Closing On:	~~**March 18, 2014 at 2:30 p.m.** ***(Eastern)***~~ **March 25, 2014 at 2:30 p.m. (*Eastern*)**

Please note the clarifications and/or changes made on this proposal program:

1. The RFP closing date and time has been extended to **March 25, 2014 at 2:30 p.m. (*Eastern*).**

2. QUESTION: The Netflow information below supersedes the information provided in the Summary of IT Infrastructure handout?

   ANSWER: *From Friday, February 28th through Thursday, March 6th, a report produced using nfsen showed the internet router generating 5,000 flows per second. The router was configured to collect Netflow ingress data on all interfaces.*

   Spring break started the week of March 10th. On March 10th and 11th, the internet router was reported to generate 2,000 flows/second. This information is included only to put the flow rates for the core routers, described next, in context.

   Netflow collection on the two campus core routers and the two data center routers did not start until Tuesday, March 11th. This was after students left for spring break. Routers were configured to collect Netflow ingress data on all interfaces except the interfaces connected to other routers (i.e. internet routers, core routers, and data center routers). During the afternoon of Wednesday, March 12th, each of the two campus core routers were reported to generate 1,200 flows per second and each of the two data center routers 1,500 flows/second. Additionally, during the morning of March 13 two of the core routers reported 2500 flows/second for about an hour and one of the cores reported 4000 flows per second for 15 minutes. Flow rates are expected to increase when students return from spring break.

3. QUESTION: What is the list of devices expected to gather logs from?

   ANSWER: *Questions 9 – 12 in Section IV. Statement of Needs indicate the important sources that are significantly important to us. They are described in more detail in the Summary of IT Infrastructure document. The 484 data center servers mentioned in that document include:*

   a. *Six Active Directory servers (4 production plus 2 root).*
   b. *111 Microsoft IIS web servers.*
   c. *1 Microsoft Exchange system consisting of four edge servers, two hub servers, and four mailbox servers.*
   d. *Symantec Antivirus management server.*

JAMES MADISON UNIVERSITY

4. QUESTION: What are the quantities of device types and software versions of the applications mentioned in the RFP?
   ANSWER: *Refer to Summary of IT Infrastructure document. All components of the JMU infrastructure use product versions currently supported by the associated vendors.*

5. QUESTION: What are the event rates these devices will generate?
   ANSWER: *Refer to Page 3 of the Summary of IT Infrastructure document and the Netflow data rate changes described herein.*

6. QUESTION: Will the system be kept centralized at one data center or is there a need to spread out across multiple data centers? If multiple, what are the locations?
   ANSWER: *We have three major data centers that are all located on the JMU campus and connected with a layer 2, 10 Gigabit network.*

7. QUESTION: Is High Availability a requirement for architectural design?
   ANSWER: *No; however, in the event of a malfunction of a provided component we expect replacement within 48 hours.*

8. QUESTION: In regard to Section IV, Question # A. 21 of the RFP, how do you plan on getting the Oracle logs to the SIEM?
   ANSWER: *JMU is aware there are multiple possibilities and does not have a specific way in mind. The intent of the question is to understand the way(s) your proposed solution can obtain and use intelligence from Oracle products whether it is from logs, database tables, or the Oracle Middleware Audit Framework and what are the recommended ways(s) for that solution.*

9. QUESTION: In regard to Section IV, Question # A. 21 of the RFP, what is the number of Oracle databases?
   ANSWER: *53 Oracle servers and 31 SQL Server.*

10. QUESTION: In regard to Section IV, Question # A. 21 of the RFP, what is the volume of logs/expected EPS? Were these included in the IT Infrastructure PDF you provided?
    ANSWER: *Some data JMU collected related to EPS was included on Page 3 of the Summary of IT Infrastructure document. Note the change in Netflow rates included herein.*

11. QUESTION: In regard to Section IV, Question # A. 21 of the RFP, would JMU be willing to install an agent on database servers?
    ANSWER: *JMU would consider it after assessing its benefits and risks to stability and security.*

12. QUESTION: Section V-B-33 requests "A written narrative statement to include, but not limited to the expertise, qualifications, and experience of the firm and resumes of specific personnel to be assigned to perform the work." Since JMU isn't formally soliciting any professional services in the RFP, can you shed light on what/whose resumes should be provided? Do you need to see resumes of any sales representatives that are working on/involved in the proposal preparation for this RFP? Also, please bear in mind that if we propose optional professional services, it is very difficult to send over resumes for the folks that would be assisting with that work this early in the selection process.
    ANSWER: *Resumes of the sales and/or technical representatives that would be assigned to JMU if awarded a contract.*

Signify receipt of this addendum by initialing *"Addendum #_____"* on the signature page of your proposal.

Sincerely,

Matasha Owens, VCO
Buyer Senior
Phone: (540-568-3137)

JAMES MADISON UNIVERSITY

March 6, 2014

ADDENDUM NO. ONE

TO ALL OFFERORS:

REFERENCE:	Request for Proposal No:	**RFP# MLO-773**
	Dated:	**February 12, 2014**
	Commodity:	**Security Incident and Event Management System**
	RFP Closing On:	**March 18, 2014 at 2:30 p.m.** ***(Eastern)***

Please note the clarifications and/or changes made on this proposal program:

1. Attendance roster for the Optional Pre-Proposal Conference held on February 27, 2014 is attached to this addendum.

2. QUESTION: What is the timeline for this purchase?
   ANSWER: *The selected SIEM system will be purchased no later than June 30, 2014.*

3. QUESTION: When will the Evaluation Committee begin evaluating proposals?
   ANSWER: *The Evaluation Committee will begin evaluating proposals immediately after the RFP closes on March 18, 2014. The first evaluation of proposals received will be conducted on April 1, 2014.*

4. QUESTION: Is there any requirement for offerors to submit anything in eVA in addition to the proposal that has to be prepared and mailed?
   ANSWER: *No; however, eVA registration is a condition of award. See item U. eVA Business-To-Government Vendor Registration, Contracts, and Orders on Page 17 of the RFP.*

5. QUESTION: Is there any prerequisite or weight placed on our past business dealings with organizations/schools in the VASCUPP program?
   ANSWER: *No.*

6. QUESTION: Is there any official "registration" process or anything else that we need to do prior to submitting a proposal to JMU Procurement Services?
   ANSWER: *No.*

7. QUESTION: An electronic copy of the proposal is also required. Can Offerors email an electronic copy directly to Procurement Services or is there a preferred, alternative method for delivery of the electronic copy (i.e. flash drive)?
   ANSWER: *No.*

8. QUESTION: Is there a preference for SIEM vendors? Has the University received presentations from SIEM vendors in the last 6 months?
   ANSWER: *No preference. The University explored the current VASCUPP contract with Accuvant. An RFP was issued to obtain proposals for additional solution options.*

9. QUESTION: Would a Virtual Machine solution be acceptable?

ANSWER: *Yes. Offerors are encouraged to review RFP Section IV. Statement Of Needs. Offerors should list all additional components for a fully functional system in their proposal. If the solution will work with commodity components with similar performance and operating characteristics, it would be economically advantageous for JMU to use them. All proposed solutions will be evaluated.*

10. QUESTION: Is the University planning to rely upon their current IT Support for operations and maintenance of the hardware deployed, analysis, help-desk support and incident resolution, or will these activities be outsourced to the contract awardee?
    ANSWER: *The University will rely on current staff.*

11. QUESTION: Will University policies allow software agents to be deployed to all end point devices were possible?
    ANSWER: *There are no policies preventing this.*

12. QUESTION: What is the desired storage retention time?
    ANSWER: *60-90 days depending on price.*

13. QUESTION: What is JMU's preference for storage – internal or external to the system?
    ANSWER: *Storage may be internal or external to the system. Offerors are encouraged to review RFP Section IV. Statement Of Needs. Offerors should list all additional components for a fully functional system in their proposal. If the solution will work with commodity components with similar performance and operating characteristics, it would be economically advantageous for JMU to use them. All proposed solutions will be evaluated.*

14. QUESTION: Is network packet storage desired and if so, does it need to meet the same retention time?
    ANSWER: *Network packet storage is desired but not required. JMU may choose to offload network packet storage to open source, commodity products unless there is a significant advantage to having it done in the SIEM. Such functionality should be listed as a separate line item. Retention time for network storage may be less than storage for event and flow data.*

    It is strongly desired that if a product is able to perform deep packet inspection that the collecting device store any packet contents, and preferably full session contents, that resulted in generating a notifying event.

15. QUESTION: What are the anticipated increase in log levels associated with wireless NAT and additional desktop logging?
    ANSWER: *JMU is unable to provide an answer to this question at this time.*

16. QUESTION: Are intra-datacenter flows of interest and if so, what is their volume?
    ANSWER: *JMU is unable to provide an answer to this question at this time.*

17. QUESTION: Are services needed?
    ANSWER: *At this time, JMU does not anticipate purchasing services for installation or tuning; however, that may change due to project time constraints. Offerors should list services as a separate line item.*

JAMES MADISON UNIVERSITY

18. QUESTION: What are JMU's priorities for a SIEM system?
ANSWER:

a. *Accurate detection and management of high risk events*
   i. *Concentrate design, resources, and incident response on incidents most likely to result in high loss associated with critical and/or sensitive assets and accounts*
      1. *Indicators of compromise*
      2. *Active threats with high probability of success*
      3. *High risk vulnerabilities*
   ii. *Offload and/or front-end the processing, storage, and/or analysis of less critical intelligence on resources other than the SIEM in an effort to maintain SIEM responsiveness, focus on high risk incidents, minimize costs, and deliver more useful, pre-qualified information to SIEM.*
b. *Responsive, comprehensive intelligence analysis platform for those high risk events*
c. *Automated, methodical, incident response workflow and record keeping associated with those high risk events*
d. *Ability to publish situational awareness dashboards to various campus communities*

19. QUESTION: Any other additions to the current infrastructure?
ANSWER: *No.*

20. QUESTION: How many events will be forwarded from change management system?
ANSWER: *Change management system is not expected to generate a significant number of events.*

21. QUESTION: Where did the SRX firewall log event rate figures come from?
ANSWER: *Log file data from Juniper Security Threat Response Manager on loan for log capture purposes.*

22. QUESTION: How will the proposed systems be tested?
ANSWER: *JMU is unable to provide an answer to this question at this time.*

Signify receipt of this addendum by initialing *"Addendum #_____"* on the signature page of your proposal.

Sincerely,

Matasha Owens, VCO
Buyer Senior
Phone: (540-568-3137)

JAMES MADISON UNIVERSITY

ATTENDANCE ROSTER

RFP NUMBER: MLO-773

PROJECT TITLE: Security Incident and Event Management System

PRE-PROPOSAL CONFERENCE: Mandatory [ ] Optional [X]

DATE: February 27, 2014 **TIME:** 2:00 p.m.

* Offerors present via conference call.

ALL OFFERORS SHALL COMPLETE THE INFORMATION REQUESTED BELOW. Information shall be legible and complete, including P.O. Box Numbers, Street Numbers, Zip Codes, etc..

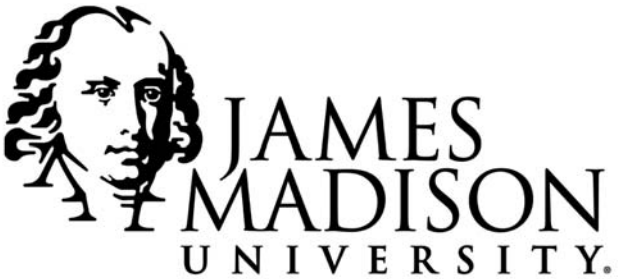
Failure to supply the University with requested information may result in offeror not receiving important addenda or information necessary to complete the proposal.

Please Print

	Representative Name	Company Name/Complete Address	Phone and Fax Numbers
1	Print: MATASHA OWENS Sign: Matasha Owens	JMU Procurement	Phone: 540-568-3137 Fax: 540-568-7936 Email: OWENSML@JMU.EDU
2	Print: Annie Korn Sign: A. Korn	JMU Procurement	Phone: 540-568-3133 Fax: 540-568-7936 Email: humphrja@jmu.edu
3	Print: David Evelyn Sign: David C. Evelyn	SLAIT Consulting	Phone: (804) 370-5781 Fax: (804) 270-1091 Email: david.evelyn@slaitconsulting.com
4	Print: Dennis Webb Sign: D=5M	CAS Severn	Phone: 301-776-3400 Fax: 301-776-3444 Email: dwebb@cassevern.com
5	Print: BOB NEWMAN Sign: Bob Newman	Sera-Brynn	Phone: (804) 338-4156 Fax: Email: bob.newman@sera-brynn.com

	Representative Name	Company Name/Complete Address	Phone and Fax Numbers
6	Print: GARY Flynn Sign:	JMU	Phone: 568-2364 Fax: Email: Flynngx@jmu.edu
7	Print: Bob Michie Sign:	PRESIDIO	Phone: 804-767-3272 Fax: - Email: bmichie@Presidio.com
8	Print: BARBARA RIGATTI Sign: Barbara Rigatti	Presidio	Phone: 540-904-0014 Fax: Email: brigattie presidio.com
9	Print: Brian Estes Sign:	EMC	Phone: 540-429-0205 Fax: Email: Brian.Estes@emc.com
10	Print: [illegible] Sign:	JMU	Phone: 568-5132 Fax: Email: millerem@jmu.edu
11	Print: Mike Bayne Sign: M Bayne	JMU	Phone: 8-1684 Fax: baynema@jmu.edu
12	Print: DICK JOHNSON Sign:	JMU	Phone: 8-8082 Fax: Email: JOHNSORV
13	Print: Dale Hulvey Sign: Dale Hulvey	JMU	Phone: 8-7063 Fax: Email: hulveydb
* 14	Print: Reginald Vigilant Sign: present (via Phone)	OmniSystems	Phone: 703-448-5300 x206 Fax: 703-448-5350 Email: reginald.vigilant@omnisystems.com
* 15	Print: Ashley Meston Sign: (present via phone)	X7 Systems Integration, an SDI Company	Phone: 703-691-1530 x104 Fax: 703-691-0880 Email: ameston@x7si.com

	Representative Name	Company Name/Complete Address	Phone and Fax Numbers
* 16	Print: Mike Lorenek Sign: (present by phone)	Access IT Group, Inc.	Phone: 410-782-4805 Fax: 410-558-6535 Email: mlorenek@accessitgroup.com
* 17	Print: John Zeledon Sign: (present by phone)	ADI Technologies	Phone: 703-734-9626 x201 Fax: 703-448-8591 Email: jzeledon@aditechnologies.com
* 18	Print: Olivier Beauchemin Sign: (present by phone)	Presidio	Phone: 540-904-0014 Fax: — Email: obeauchemin@presidio.com
* 19	Print: Randy Devlin Sign: (present by phone)	Accurant	Phone: 757-879-2562 Fax: ——— Email: rdevlin@accurant.com
* 20	Print: Steve Noble Sign: (present by phone)	McAfee	Phone: 646-728-3135 Fax: — Email: stephen_noble@mcafee.com
* 21	Print: Adam Waltman Sign: (present by phone)	McAfee	Phone: 646-728-3135 Fax: — Email: Adam_Waltman@mcafee.com
* 22	Print: James Hunt Sign: (present by phone)	McAfee	Phone: 646-728-3135 Fax: — Email: James_Hunt@mcafee.com
23	Print: Sign:		Phone: Fax: Email:
24	Print: Sign:		Phone: Fax: Email:
25	Print: Sign:		Phone: Fax: Email:



Request for Proposal

RFP # MLO-773

Security Incident and Event Management System

February 12, 2014

College of William and Mary
George Mason University
James Madison University
Old Dominion University
Radford University
The University of Virginia
Virginia Commonwealth University
Virginia Military Institute
Virginia Tech

REQUEST FOR PROPOSAL

RFP # MLO-773

Issue Date: **February 12, 2014**

Title: **Security Incident and Event Management System**

Issuing Agency: ***Commonwealth of Virginia***
James Madison University
Procurement Services MSC 5720
752 Ott Street, Wine Price Bldg.
First Floor, Suite 1023
Harrisonburg, VA 22807

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

Sealed Proposals Will Be Received Until 2:30 p.m. on March 18, 2014 For Furnishing The Services Described Herein.

OPTIONAL PRE-PROPOSAL: February 27, 2014 at 2:00 p.m. Offerors are required to register for this pre-proposal conference. See *Special Term and Condition DD. Optional Pre-Proposal Conference* for more information. Offerors are encouraged to attend the optional pre-proposal.

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

All Inquiries For Information and Clarification Should Be Directed To: Matasha Owens, VCO, Buyer Senior Procurement Services, owensml@jmu.edu, 540/568-3137, (Fax) 540/568-7936 not later than five business days before the proposal closing date.

NOTE: THE SIGNED PROPOSAL AND ALL ATTACHMENTS SHALL BE RETURNED
In compliance with this Request for Proposal and to all the conditions imposed herein, the undersigned offers and agrees to furnish the goods/ services in accordance with the attached signed proposal or as mutually agreed upon by subsequent negotiation.

Name and Address of Firm:

_____ By:_____
(Signature in Ink)

_____ Name:_____
(Please Print)

Title:_____ _____

Date: Phone:_____ _____

Web Address: _____ Fax #:_____

Email:_____

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

SMALL, WOMAN OR MINORITY OWNED BUSINESS:
☐ YES; ☐ NO; *IF YES* ⇒⇒ ☐ SMALL; ☐ WOMAN; ☐ MINORITY ***IF MINORITY:*** ☐ AA; ☐ HA; ☐ AsA; ☐ NW

Note: This public body does not discriminate against faith-based organizations in accordance with the *Code of Virginia*, § 2.2-4343.1 or against a bidder or offeror because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating to discrimination in employment.

REQUEST FOR PROPOSAL

RFP # MLO-773

TABLE OF CONTENTS

I. PURPOSE

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals from qualified sources to enter into a contract to provide a Security Incident and Event Management System (SIEM) for James Madison University (JMU), an agency of the Commonwealth of Virginia. Initial contract shall be for one (1) year with an option to renew for nine (9) additional one-year periods.

II. BACKGROUND

James Madison University (JMU) is a comprehensive public institution in Harrisonburg, Virginia with an enrollment of approximately 20,000 students and 3,000 faculty and staff. There are over 600 individual departments on campus that support seven academic divisions. The University offers over 120 majors, minors, and concentrations. Further information about the University may be found at the following website: http://www.jmu.edu.

Contact Matasha Owens at owensml@jmu.edu to request a summary of JMU's IT environment for information about event sources, log volume, etc.

III. SMALL, WOMAN-OWNED AND MINORITY (SWAM) PARTICIPATION

It is the policy of the Commonwealth of Virginia to contribute to the establishment, preservation, and strengthening of small businesses and businesses owned by women and minorities and to encourage their participation in State 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, and other contractual opportunities. Attachment B contains information on reporting spend data with subcontractors.

IV. STATEMENT OF NEEDS

James Madison University is seeking a Security Incident and Event Management System (SIEM) that provides accurate detection and management of high risk events. The Offeror shall have available and be able to demonstrate their proposed solution.

The following are areas of significant importance to James Madison University in selection of a SIEM system:

- Event Detection and Noise Reduction
    - Detect unauthorized changes in critical host files. File changes are monitored and reported using OSSEC. Minimize false positives due to normal operations and patching by altering sensitivity to changes during published change management times and other mechanisms (*detect compromised host*).
    - Detect logins originating from a list of high risk networks to the Peoplesoft Portal, campus Exchange, or Juniper SSLVPN (*detect compromised account or high risk activity*).
    - Detect logins from multiple geographically separated locations over a specified time to the Peoplesoft Portal, campus Exchange, and Juniper SSLVPN (*detect compromised account*).
    - Detect logins to multiple accounts on Peoplesoft Portal, campus Exchange, or Juniper

SSLVPN from a single address or network that is not on a white list (*detect multiple compromised accounts*).

- Detect high risk servers and endpoints trying to reach IP addresses, domains, and URLs on a watch list (*detect compromised host or endpoint or high risk activity*).

- Detect network scanning and network access violations from a VPN session, high risk endpoint, or server (*detect compromised account or system*).

- Report anomalous outbound traffic from data center systems (*detect compromised host, test Netflow anomaly detection*).

- Detect and report a new process name or applocker block on any PCI endpoint. (*detect compromised endpoint or high risk activity*).

- Report a malware encounter followed by a new process name or Applocker block by a computer on a list of high risk endpoints (*detect compromised endpoint*).

- Behavior Detection

  - Detect use of administrator credentials from networks other than those on a whitelist (*detect compromised account or high risk activity*).

  - Detect high speed, distributed administrative logins (*detect possible worm, pass-the-hash, scripted attack*).

  - Detect outbound email anomalies from high risk accounts (*discover compromised accounts*).

- Correlation

  - Detect a high risk desktop downloading java/flash content followed within 5 minutes by the appearance of a new client process not on a whitelist running from the local profile directory tree (*detect endpoint exploit and compromise, test ability for layer seven traffic inspection, test process auditing event log handling*).

  - Detect an email message with a subject identified as "phishy" by a JMU written regular expression that is delivered to one or more accounts on a list of high risk recipients followed by two or more computers operated by those recipients accessing the same overseas URL within eight workday hours (*detect compromised accounts, test regular expression capabilities, test exchange log parsing, test ability to correlate IP address, endpoint, and eID*).

- Analysis

  - Querying and analysis capabilities will be tested using production data and events.

- Reporting/Dashboard

  - Provide accounts for support staff, management, system administrators, and network engineers delivering restricted data, report views, and customized information based on ID and role.

- Accept queries from a web site and return data that allows users to enter an account name on the web site and view information related to use of that account including such things as time/date, source with geolocation, target application, and source device characteristics. (*test integration capabilities*).

- Correlate IP address and time to identity (*test ability to query and understand NAT, nonNAT, NAC, wireless ACS, IPAM*).

- Miscellaneous

  - Acquire and use authentication/authorization information from OAM/OAAM/OID logs and database records.

Offerors shall provide detailed responses to the following:

A. Application Functionality:

1. Describe the design, detection, and incident response capabilities of the proposed Security Incident and Event Management System to include the ability to detect and report:

   a. Indicators of compromise

   b. Active threats with high probability of success

   c. High risk vulnerabilities

2. Describe the system's intelligence analysis components, design, and capabilities.

3. Describe the system's incident response workflow and record keeping capabilities.

4. Describe the system's ability to publish situational awareness dashboards to various campus communities.

5. Describe the system's ability to work in an environment that offloads and/or front-ends the processing, storage, and/or analysis of less critical intelligence on resources other than the SIEM.

6. Describe log and event data storage accessible in real-time at production speeds. Identify timeframes (*e.g. 60 days, 90 days*).

7. Describe the ability to configure variable archive times for log and event data of different types or originating from different sources.

8. Describe system's capability to use external storage for long term archive with ability to access from and/or re-import into SIEM to be used in data analysis and investigations.

9. Describe the system's ability to monitor and accept intelligence data from:

   a. Logs and events from all IT data center servers (*All layers – e.g. OS, database, web, application*).

   b. Logs from all firewalls, IDS/IPS devices, data center routers and switches, Internet, core routers, 1000 employee endpoints (*e.g. windows desktop event log information*).

c. Logs from a network management system monitoring employee switches indicating CAM table overloads, ARP poisoning, MAC address changes, or DHCP security activation.

d. Network traffic intelligence on Internet links, inside IT Data Centers, and on Core Campus routers with depth of knowledge equivalent to layer 4 or higher (*e.g. Netflow or layer 7 deep inspection*).

10. Describe the system's ability to accept, understand, and process all critical intelligence types as identified in Section II, Background. Include OSSEC file/ registry integrity and change reports from windows and linux clients, Oracle Middleware Audit Framework, Application ASCII log files, Nessus vulnerability scanner, DNS (*Bind and Bluecat*) , DHCP (*ISC and Bluecat*), web and application servers (*including Apache, IIS, Tomcat, Oracle, and PeopleSoft*), and Windows event logs (*including those associated with process, Applocker, and SACL auditing on high risk endpoints*).

11. Describe the system's ability to incorporate and correlate identity and role information in decision making processes allowing emphasis on high risk accounts and assets with information which may be obtained from Active Directory, Oracle Internet Director, Cisco NAC, IPAM, and SCCM.

12. Describe the system's ability to extract and correlate authentication transaction information through all layers including those that result in IP address changes and proxy accounts. This includes:

    authentication services (*e.g. Active Directory, Oracle Virtual Directory, Oracle Internet Directory, and Safenet*), middleware and infrastructure (*e.g. Oracle Access Manager, Oracle Adaptive Access Manager, shibboleth, Microsoft federation(possible future), Oracle federation (possible future), SSLVPN, F5, reverse proxies, wireless access points, and NAC)* and applications (*e.g. PeopleSoft app/web/proxy servers, Exchange RPC/OWA/O365, and SharePoint/sharepoint365*).

13. Describe the system's ability to configure and write rules that can query resources outside the SIEM (*e.g. whitelists, databases, and directories*) for information to supplement a detected event and have the SIEM alter response accordingly.

14. Describe the system's ability to consume reputation intelligence from internal and external sources.

15. Describe the system's ability to write custom intelligence parsing routines and classify and correlate them (*e.g. custom device log formats, custom data structures, custom events*). Include ability to write custom rules and algorithms with granular whitelist capabilities.

16. Describe the system's ability to cooperatively work with a preprocessing infrastructure providing custom intelligence events.

17. Describe system data analysis, search, query, and reporting capabilities.

18. Describe support for flexible automated notifications, dashboards, and reporting as well as incident handling workflow.

19. Describe the system's capacity to handle growth in events and network flows. Specify the percentage growth without an increase in cost.

20. Describe the system's capability for 100% growth in three (3) years with modular component

additions.

21. Describe the system's ability to utilize and/or import stored activity and event logs from Oracle databases. Describe ability to work with the Oracle Middleware Audit Framework.

22. Describe the system's ability to interface with external threat intelligence sources (*e.g. dns blacklists, spam blacklists, web site reputation systems*) provided by your firm or others and any associated costs. Indicate how your firm's product would make use of such information.

23. Describe any network connections between provided components, agents, or connectors that are not authenticated and encrypted.

24. Describe any network communications between provided components and outside vendors. State their purpose, content of data transferred, connection direction, and protocols involved.

25. Describe storage capacity for log, event, and network traffic data. Differentiate between storage of raw, unaltered data as received from sources and modified formats as applicable.

26. Describe the proposed solution's ability to archive historical log, event, and network traffic data both within the proposed solution storage and external storage. Describe ability to use the proposed solution's reporting and analysis tools to access on-board and off-board archived event and traffic data.

27. Describe the ability to query your data storage with external tools for log entries, events, network traffic, and/or incident records.

28. Based on storage capacity and the JMU environment, provide estimated log, event, and network traffic storage lifetime of the proposed solution.

29. Describe in detail licensing and pricing model. Include price boundaries for number of event sources, traffic flows, event volume, accounts, users, identities, roles, API connections, CPUs, cores, collectors, and/or any other parameter affecting price. State whether figures for events and flows are peak or average and if the latter, over what time period. Specify any costs in *Section X, Pricing Schedule* of this solicitation.

30. Provide definitions for an event, an event source, a flow, and a flow source. Specify the impact, if any, on pricing, licensing, or resource limits of accepting events, logs, or other data from the following sources:

    a. A Symantec management server forwarding client malware detection activity.

    b. An Identity Finder management server forwarding client sensitive data scan results.

    c. An SCCM desktop management server forwarding client patching and configuration activity.

    d. An OSSEC management server forwarding file integrity information about monitored servers.

    e. Nessus server forwarding client and server vulnerability information

    f. A database query tool running on an external system performing database queries across related databases (*e.g. on multiple Oracle Identity Management components*) and forwarding consolidated results to SIEM as a custom event.

g. A Windows event collector forwarding selected audit events from high risk endpoints.

31. Describe the ability to interface with external ticketing systems explaining the methods of integration and any product specific integration capabilities.

32. Describe the ability to support LDAPS authentication and LDAP group authorization for accounts used to access the SIEM by security staff, administrators, support staff, management, etc.

33. Specify the primary user interface for security staff, administrators, support staff, management, etc. (*e.g. HTML web browser, web browser with Flash, web browser with java, web browser with ActiveX control, standalone java client, standalone windows client, X session*). Provide interface requirements (*e.g. browsers supported, OS supported, requirements for Java, Flash, or other add-on software*).

34. Provide line item pricing in *Section X, Pricing Schedule* of this solicitation for all hardware, software, licenses, and other solution components. Indicate which can be purchased independently of others (*e.g. layer 7 deep packet inspection components, interfaces with external ticketing systems, interfaces with external reputation systems*). Specify what data and calculations were used to arrive at the proposed solution size and licensing.

35. Provide line item pricing for additional hardware, software, license, and other necessary components to increase capacity 100% should JMU determine, in its sole discretion, to do so. Specify what data and calculations were used to arrive at the proposed solution size and licensing.

36. Describe your firm's ability to provide an online demonstration environment for the proposed products to aid in assessment. Provide access information and describe the environment and the data feeding it.

37. Provide electronic copies of available product documentation including installation guides, user guides, administrator guides, APIs, integration guides, tuning guides, release notes, etc. or web site account and link where they can be downloaded.

38. Provide access to vendor and product knowledgebase. If unavailable, knowledgebase articles, whitepapers, support data and similar resources describing performance tuning and limitations, performance, integration methods, most common support calls, and most commonly requested event sources that are not supported.

39. Describe the training options and include a catalog of training offerings and their associated costs. Response should include differentiation between technical staff and end-user training.

40. Describe the support options available through your company including on-going support of the application. Describe what portions of support to be performed by IT, the customer versus the vendor.

41. JMU is interested in developing a strategic relationship with the successful vendor. Provide information regarding ideas on how such a relationship can prove mutually beneficial.

42. Describe active user groups and how they function.

43. Provide your privacy statement.

B. <u>Technical:</u>

1. Provide a detailed diagram of the typical architecture/technical environment required for the system. List all protocols and ports used for communications and indicate which components are clients and which are servers and whether the communications are fully, partially, or not encrypted. Specify any communications paths where unencrypted authentication or other sensitive data are passed. List all third party dependent integration points and data paths including any web content included from or sent to outside parties.

2. Describe the toolset from which your application is derived.

3. Describe hardware and software requirements for the proposed system(s) along with any sizing assumptions made to arrive at those requirements.

4. Describe supported server hardware and/or virtualized platforms. Describe support for the following operating systems: Linux and Windows. If virtualization is supported, what virtualization technologies are supported including what components can be virtualized?

5. Describe support for load balancing and system failover including any and all vendor specific preferences. Also include any vendor specific configuration guides.

6. Describe how scalability is accomplished as the criticality of the system(s) and number of users increase.

7. Describe the system capabilities and options for the backup and restoration of the system components (*example: database*)

8. Describe any standard and proprietary APIs, integration/connection resources, and development languages and tools that extend your toolset.

9. Describe requirements for application servers. Describe specific platform recommendations or requirements for certified configuration *(e.g. WebLogic, and Apache Tomcat);* include either specific application server version or required J2EE version.

10. Describe support for web servers *(i.e. Apache, Weblogic and IIS)*.

11. Describe the supported database platforms including versions and include any information on additional features required of the DBMS needed to support the functionality of your system as proposed.

12. Describe your SLA to stay current with versions of software utilized by your product.

13. Describe support for real-time access to data through some other method (*e.g. on-the-fly access to database through ODBC, ADO, JDBC, LDAP, etc. allowing dynamic web content and applications)*.

14. Describe storage including file formats.

C. <u>Maintenance and Support:</u>

Because consistency and stability of the operating environment and rapid correction of system failures are critical to James Madison University, major consideration will be given to the amount and extent of hardware and software maintenance coverage and to the quality of maintenance.

1. Describe services that may be required in the normal course of operating the system that are not

covered under the maintenance contract.

2. Describe the maintenance costs for the first year, and, on the basis of an annually renewable contract, the maintenance costs for each of the following five (5) years.

3. Describe the procedures for obtaining services for all types of maintenance *(e.g. installation of corrective code, enhancements, applicable "escalation" procedures for providing additional assistance in diagnosing a failure that is not resolved in a timely manner to include notification procedures and timing as well as what higher levels of assistance will be made available.)*

4. Describe procedure for handling upgrades. Specify how often upgrades are made to the application software and how "patches" and "fixes" to the systems are handled. Describe if and how your product impacts our ability to apply security updates in a timely manner to underlying or supporting products *(e.g. Windows, Linux, Java, Oracle, MS Office, Web server)*. Timely is defined as no later than 30 days from the time of vendor release.

5. Describe the nature of system enhancements in development that are scheduled for release in the next twelve months.

6. Describe all responsibilities of both the contractor and James Madison University in the isolation and diagnosis of system failures.

7. Describe your "escalation" procedure.

D. Trialing:

1. JMU may perform a thirty (30) or sixty (60) day production evaluation on proposed products selected at the sole discretion of the University. Notified Offerors shall provide the proposed products and solutions to JMU for evaluation and testing. JMU will install the proposed products and direct full production data streams to it. JMU will attempt to implement test scenarios to assess ability of the solution to meet JMU needs. Test scenarios may be conducted on the following: event detection and noise reduction, behavior detection, correlation, analysis, reporting/dashboard, and other miscellaneous items. Specify all components that will be needed by JMU for implementation of a complete evaluation and production solution and provide delivery timeframes. Time is of the essence. Specify any components not provided in your proposal (*e.g. hardware, operating systems, licenses*) that are needed for full evaluation and implementation.

2. Describe in detail how JMU can explore the performance and proper sizing of the solution during trialing of selected products at the sole discretion of the University. Describe system statistics, counters, logs, and/or other system tools that can be used to measure resource utilization, event rates, flow rates, dropped events and flows, license limits, headroom, etc.

V. PROPOSAL PREPARATION AND SUBMISSION

A. GENERAL INSTRUCTIONS:

To ensure timely and adequate consideration of your proposal, offerors are to limit all contact, whether verbal or written, pertaining to this RFP to the James Madison University Procurement Office for the duration of this Proposal process. Failure to do so may jeopardize further consideration of Offeror's proposal.

1. RFP Response: In order to be considered for selection, the **Offeror shall submit a complete response to this RFP**; and shall submit to the issuing Purchasing Agency:

   a. **One (1) original** and **two (2) copies** of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with 3.f below.

   b. **One (1) electronic copy in WORD format or searchable PDF** *(CD or flash drive)* of the entire proposal, INCLUDING ALL ATTACHMENTS. Any proprietary information should be clearly marked in accordance with 3.f below.

   c. Should the proposal contain **proprietary information**, provide **one (1) redacted hard copy** of the proposal and attachments **with proprietary portions removed or blacked out**. This copy should be clearly marked *"Redacted Copy"* on the front cover. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable. JMU shall not be responsible for the Contractor's failure to exclude proprietary information from this redacted copy.

      No other distribution of the proposal shall be made by the Offeror.

2. The version of the solicitation issued by JMU Procurement Services 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 JMU Procurement Services 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, JMU 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 Procurement Services.

3. Proposal Preparation:

   a. Proposals shall be signed by an authorized representative of the offeror. All information requested should be submitted. Failure to submit all information requested may result in the purchasing agency requiring prompt submissions 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. 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.

   c. Proposals should be organized in the order in which the requirements are presented in the RFP. All pages of the proposal should be numbered. Each paragraph in the proposal should reference the paragraph number of the corresponding section of the RFP. It is also helpful to cite the paragraph number, sub letter, and repeat the text of the requirement as it appears in the RFP. If a response covers more than one page, the paragraph number and sub letter should be repeated at the top of the next page. 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 the 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 where the

RFP requirements are specifically addressed.

d. As used in this RFP, the terms "must", "shall", "should" and "may" identify the criticality of requirements. "Must" and "shall" identify requirements whose absence will have a major negative impact on the suitability of the proposed solution. Items labeled as "should" or "may" are highly desirable, although their absence will not have a large impact and would be useful, but are not necessary. Depending on the overall response to the RFP, some individual "must" and "shall" items may not be fully satisfied, but it is the intent to satisfy most, if not all, "must" and "shall" requirements. The inability of an offeror to satisfy a "must" or "shall" requirement does not automatically remove that offeror from consideration; however, it may seriously affect the overall rating of the offeror' proposal.

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.

f. Ownership of all data, materials and documentation originated and prepared for the State pursuant to the RFP shall belong exclusively to the State and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by the offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act; however, the offeror must invoke the protection of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data is submitted. The written notice must specifically identify the data or materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret materials submitted must be identified by some distinct method such as highlighting or underlining and must indicate only the specific words, figures, or paragraphs that constitute trade secret or proprietary information. The classification of an entire proposal document, line item prices and/or total proposal prices as proprietary or trade secrets is not acceptable and will result in rejection and return of the proposal.

4. Oral Presentation: Offerors who submits a proposal in response to this RFP may be required to give an oral presentation of their proposal to James Madison University. This provides an opportunity for the offeror to clarify or elaborate on the proposal. This is a fact finding and explanation session only and does not include negotiation. James Madison University will schedule the time and location of these presentations. Oral presentations are an option of the University and may or may not be conducted. Therefore, proposals should be complete.

B. SPECIFIC PROPOSAL INSTRUCTIONS:

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

1. Return RFP cover sheet and all addenda acknowledgments, if any, signed and filled out as required.

2. Plan and methodology for providing the goods/services as described in Section IV *"Statement of Needs"* of this Request for Proposal.

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

4. Provide four references and contact information for customers using the proposed solution in an enterprise wide deployment. At least two references should be in higher education.

5. Offeror Data Sheet, included as *Attachment A* to this RFP.

6. Small Business Subcontracting Plan, included as *Attachment B* to this RFP. Offeror shall provide a Small Business Subcontracting plan which summarizes the planned utilization of DMBE-certified small businesses which include businesses owned by women and minorities, when they have received DMBE small business certification, under the contract to be awarded as a result of this solicitation. This is a requirement for all prime contracts in excess of $100,000.

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

8. Proposed Cost. See Section X. *"Pricing Schedule"* of this Request for Proposal.

VI. EVALUATION and AWARD CRITERIA

A. EVALUATION CRITERIA:

Proposals shall be evaluated by James Madison University using the following criteria:

1. Quality of products/services offered and suitability for the intended purposes.

2. Qualifications and experience of Offeror in providing the goods/services.

3. Specific plans or methodology to be used to perform the services.

4. Participation of Small, Women-Owned and Minority (SWAM) Businesses

5. Cost

B. **AWARD TO MULTIPLE OFFERORS:** Selection shall be made of two or more offerors deemed to be fully qualified and best suited among those submitting proposals on the basis of the evaluation factors included in the Request for Proposals, including price, if so stated in the Request for Proposals. Negotiations shall be conducted with the offerors so selected. Price shall be considered, but need not be the sole determining factor. After negotiations have been conducted with each offeror so selected, the agency shall select the offeror which, in its opinion, has made the best proposal, and shall award the contract to that offeror. The Commonwealth reserves the right to make multiple awards as a result of this solicitation. The Commonwealth 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 reasons why a particular proposal was not deemed to be the most advantageous. Should the Commonwealth determine in writing and in its sole discretion that only one offeror is fully qualified, or that one offeror is clearly more highly qualified than the others under consideration, 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 solicitation and the contractor's proposal as negotiated.

VII. GENERAL TERMS AND CONDITIONS *(Rev. 1/27/14 ABS)*

A. PURCHASING MANUAL: This solicitation 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 purchasing office. In addition, the manual may be accessed electronically at

http://www.jmu.edu/procurement or a copy can be obtained by calling Procurement Services at (540) 568-3145.

B. APPLICABLE LAWS AND COURTS: This solicitation 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 applicable federal, state and local laws and regulations.

C. ANTI-DISCRIMINATION: By submitting their proposals, offerors certify to the Commonwealth 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 §10 of the Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 (available for review at http://www.jmu.edu/procurement). 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. *(§6 of the Rules Governing Procurement)*

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. The contractor will not discriminate against any employee or applicant for employment because of race, religion, color, sex, national origin, age, disability, or any other basis prohibited by state law relating 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 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. IMMIGRATION REFORM AND CONTROL ACT OF 1986: By entering into a written contract with the Commonwealth of Virginia, the Contractor certifies that the Contractor does not, and shall not during the performance of the contract for goods and services in the Commonwealth, knowingly

employ an unauthorized alien as defined in the federal Immigration Reform and Control Act of 1986.

F. DEBARMENT STATUS: By submitting their proposals, offerors certify that they are not currently debarred by the Commonwealth of Virginia from submitting bids or 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. ANTITRUST: 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 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. MANDATORY USE OF STATE FORM AND TERMS AND CONDITIONS RFPs: Failure to submit a proposal on the official state 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. CLARIFICATION OF TERMS: If any prospective offeror has questions about the specifications or other solicitation documents, the prospective offeror should contact the buyer whose name appears on the face of the solicitation no later than five working days before the due date. Any revisions to the solicitation will be made only by addendum issued by the buyer.

J. 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 state 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 30 days will be regarded as requiring payment 30 days after invoice or delivery, whichever occurs last. This shall not affect offers of discounts for payment in less than 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 agency 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, the Commonwealth 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 an agency of its prompt payment obligations with respect to those charges which are not in dispute *(Rules Governing Procurement, Chapter 2, Exhibit J, Attachment 1 § 53; available for review at http://www.jmu.edu/procurement)*.

2. To Subcontractors:

a. A contractor awarded a contract under this solicitation is hereby obligated:

(1) To pay the subcontractor(s) within seven (7) days of the contractor's receipt of payment from the Commonwealth for the proportionate share of the payment received for work performed by the subcontractor(s) under the contract; or

(2) To notify the agency 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 the Commonwealth, 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 the Commonwealth.

3. Each prime contractor who wins an award in which provision of a SWAM procurement plan is a payment, evidence and certification of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the SWAM procurement plan. Final payment under the contract in question may be withheld until such certification is delivered and, if necessary, confirmed by the agency or institution, or other appropriate penalties may be assessed in lieu of withholding such payment.

4. The Commonwealth of Virginia encourages contractors and subcontractors to accept electronic and credit card payments.

K. PRECEDENCE OF TERMS: **:** Paragraphs A through J of these General Terms and Conditions and the Commonwealth of Virginia Purchasing Manual for Institutions of Higher Education and their Vendors, 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.

L. QUALIFICATIONS OF OFFERORS: The Commonwealth 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 the Commonwealth all such information and data for this purpose as may be requested. The Commonwealth reserves the right to inspect offeror's physical facilities prior to award to satisfy questions regarding the offeror's capabilities. The Commonwealth further reserves the right to reject any proposal if the evidence submitted by, or investigations of, such offeror fails to satisfy the Commonwealth 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.

M. TESTING AND INSPECTION: The Commonwealth reserves the right to conduct any test/inspection it

may deem advisable to assure goods and services conform to the specifications.

N. ASSIGNMENT OF CONTRACT: A contract shall not be assignable by the contractor in whole or in part without the written consent of the Commonwealth.

O. CHANGES TO THE CONTRACT: Changes can be made to the contract in any 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 Purchasing Agency 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 the Purchasing Agency 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 Purchasing Agency'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 the Purchasing Agency with all vouchers and records of expenses incurred and savings realized. The Purchasing Agency 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 the Purchasing Agency within thirty (30) days from the date of receipt of the written order from the Purchasing Agency. 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 Purchasing Manual for Institutions of Higher Education and their Vendors. Neither the existence of a claim nor 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 Purchasing Agency or with the performance of the contract generally.

P. DEFAULT: In case of failure to deliver goods or services in accordance with the contract terms and conditions, the Commonwealth, 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 the Commonwealth may have.

Q. INSURANCE: By signing and submitting a bid or proposal under this solicitation, the bidder or offeror certifies that if awarded the contract, it will have the following insurance coverage 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 *§ 25 of the Rules*

Governing Procurement – Chapter 2, Exhibit J, Attachment 1, and 65.2- 800 et. Seq. of the Code of Virginia (available for review at http://www.jmu.edu/procurement) The bidder or offeror further certifies that the contractor and any subcontractors will maintain these insurance coverage 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. Workers' Compensation – Statutory requirements and benefits. Coverage is compulsory for employers of three or more employees, to include the employer. Contractors who fail to notify the Commonwealth of increases in the number of employees that change their workers' compensation requirement under the Code of Virginia during the course of the contract shall be in noncompliance with the contract.

2. Employer's Liability - $100,000.

3. Commercial General Liability - $1,000,000 per occurrence and $2,000,000 in the aggregate. Commercial General Liability is to include bodily injury and property damage, personal injury and advertising injury, products and completed operations coverage. The Commonwealth of Virginia must be named as an additional insured and so endorsed on the policy.

4. Automobile Liability - $1,000,000 combined single limit. (*Required only if a motor vehicle not owned by the Commonwealth is to be used in the contract. Contractor must assure that the required coverage is maintained by the Contractor (or third party owner of such motor vehicle*.)

R. ANNOUNCEMENT OF AWARD: Upon the award or the announcement of the decision to award a contract over $50,000, as a result of this solicitation, the purchasing agency will publicly post such notice on the DGS/DPS eVA web site (www.eva.virginia.gov) for a minimum of 10 days.

S. 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 violations 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 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.

T. 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, faith-based organizational status, any other basis prohibited by state law relating to discrimination in employment or because the bidder or offeror employs ex-offenders unless the state agency, department or institution has made a written determination that employing ex-offenders on the specific contract is not in its best interest. 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.

U. 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 the Commonwealth. The eVA portal is the gateway for vendors to conduct business with state agencies and public bodies. All vendors desiring to provide goods and/or services to the Commonwealth shall participate in the eVA Internet eprocurement 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 the current fees are as follows:

a. For orders issued July 1, 2011 thru June 30, 2014, the Vendor Transaction Fee is:
(i) DMBE-certified Small Businesses: 0.75%, capped at $500 per order.
(ii) Businesses that are not DMBE-certified Small Businesses: 0.75%, capped at $1,500 per order.

b. For orders issued July 1, 2014 and after, the Vendor Transaction Fee is:
(i) DMBE-certified Small Businesses: 1%, capped at $500 per order.
(ii) Businesses that are not DMBE-certified Small Businesses: 1%, capped at $1,500 per order.

For orders issued prior to July 1, 2011 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 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.

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

W. BID PRICE CURRENCY: Unless stated otherwise in the solicitation, bidders/offerors shall state bid/offer prices in US dollars.

X. TAXES**:** Sales to the Commonwealth of Virginia are normally exempt from State sales tax. State sales and use tax certificates of exemption, Form ST-12, will be issued upon request. Deliveries against this contract shall usually be free of Federal excise and transportation taxes. The Commonwealth's excise tax exemption registration number is 54-73-0076K.

Y. USE OF BRAND NAMES: Unless otherwise provided in this solicitation, 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 equivalent 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 the Commonwealth 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. Normally in competitive

sealed bidding only the information furnished with the bid will be considered in the evaluation. Failure to furnish adequate data for evaluation purposes may result in declaring a bid nonresponsive. Unless the (bidder/offeror) clearly indicates in its (bid/proposal) that the product offered is an equivalent product, such (bid/proposal) will be considered to offer the brand name product referenced in the solicitation.

Z. 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.

VIII. SPECIAL TERMS AND CONDITIONS (Rev. 10/1/13 ABS)

A. AUDIT: The Contractor hereby agrees to retain all books, records, systems, 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 Commonwealth of Virginia, its authorized agents, and/or State auditors shall have full access to and the right to examine any of said materials during said period.

B. CANCELLATION OF CONTRACT: James Madison University reserves the right to cancel and terminate any resulting contract, in part or in whole, without penalty, upon 60 days written notice to the contractor. In the event the initial contract period is for more than 12 months, the resulting contract may be terminated by either party, without penalty, after the initial 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.

C. IDENTIFICATION OF PROPOSAL ENVELOPE: The signed proposal should be returned in a separate envelope or package, sealed and identified as follows:

From:_____
Name of Offeror Due Date Time

_____
Street or Box No. RFP Number

_____
City, State, Zip Code RFP Title

Name of Purchasing Officer: _____

The envelope should be addressed as directed on the title page of the solicitation.

The offeror takes the risk that if the envelope is not marked as described above, it 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.

D. 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 non-responsive 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 intra university mail system. It is the sole responsibility of the Offeror to ensure that its proposal reaches the issuing office by the designated date and hour.

E. UNDERSTANDING OF REQUIREMENTS: It is the responsibility of each offeror to inquire about and clarify any requirements of this solicitation that is not understood. The University will not be bound by oral explanations as to the meaning of specifications or language contained in this solicitation. Therefore, all inquiries deemed to be substantive in nature must be in writing and submitted to the responsible buyer in the Procurement Services Office. Offerors must ensure that written inquiries reach the buyer at least five (5) days prior to the time set for receipt of offerors proposals. A copy of all queries and the respective response will be provided in the form of an addendum to all offerors who have indicated an interest in responding to this solicitation. Your signature on your Offer certifies that you fully understand all facets of this solicitation. These questions may be sent by Fax to 540/ 568 -7936 or 540/568-7935.

F. RENEWAL OF CONTRACT: This contract may be renewed by the Commonwealth for a period of nine (9) successive one year periods under the terms and conditions of the original contract except as stated in 1. and 2. below. Price increases may be negotiated only at the time of renewal. Written notice of the Commonwealth's intention to renew shall be given approximately 90 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-year period, the contract price(s) for the additional one year shall not exceed the contract price(s) of the original contract increased/decreased by no more than the percentage increase/decrease of the other services 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.

2. If during any subsequent renewal periods, the Commonwealth elects to exercise the option to renew the contract, the contract price(s) for the subsequent renewal period shall not exceed the contract price(s) of the previous renewal period increased/decreased by more than the percentage increase/decrease of the other services 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.

G. SUBMISSION OF INVOICES: All invoices shall be submitted within sixty days of contract term expiration for the initial contract period as well as for each subsequent contract renewal period. Any invoices submitted after the sixty day period will not be processed for payment.

H. OPERATING VEHICLES ON JAMES MADISON UNIVERSITY CAMPUS: Operating vehicles on sidewalks, plazas, and areas heavily used by pedestrians is prohibited. In the unlikely event a driver should find it necessary to drive on James Madison University sidewalks, plazas, and areas heavily used by pedestrians, the driver must yield to pedestrians. For a complete list of parking regulations, please go to www.jmu.edu/parking; or to acquire a service representative parking permit, contact Parking Services at 540 .568.3300. The safety of our students, faculty and staff is of paramount importance to us. Accordingly, violators may be charged.

I. COOPERATIVE PURCHASING / USE OF AGREEMENT BY THIRD PARTIES: It is the intent of this solicitation and resulting contract(s) to allow for cooperative procurement. Accordingly, any public body, *(to include government/state agencies, political subdivisions, etc.),* cooperative purchasing organizations, public or private health or educational institutions or any University related foundation and affiliated corporations may access any resulting contract if authorized by the Contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) will be extended to the entities indicated above to purchase goods and services in accordance with contract terms. As a separate contractual relationship, the participating entity will place its own orders directly with the Contractor(s) and shall fully and independently administer its use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the University. No modification of this contract or execution of a separate agreement is required to participate; however, the participating entity and the Contractor may modify the terms and conditions of this contract to accommodate specific governing laws, regulations, policies, and business goals required by the participating entity. Any such modification will apply solely between the participating entity and the Contractor.

The Contractor will notify the University in writing of any such entities accessing this contract. The Contractor will provide semi-annual usage reports for all entities accessing the contract. The University 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 University is not responsible for the acts or omissions of any entity and will not be considered in default of the contract no matter the circumstances.

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

J. SMALL BUSINESS SUBCONTRACTING AND EVIDENCE OF COMPLIANCE:

1. It is the goal of the Commonwealth that 40% of its purchases are made from small businesses. This includes discretionary spending in prime contracts and subcontracts. All potential bidders/offerors are required to submit a Small Business Subcontracting Plan. Unless the bidder/offeror is registered as a DMBE-certified small business and where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such subcontracting opportunities to DMBE-certified small businesses. This shall not exclude DMBE-certified women-owned and minority-owned businesses when they have received DMBE small business certification. No bidder/offeror or subcontractor shall be considered a Small Business, a Women-Owned Business or a Minority-Owned Business unless certified as such by the Department of Minority Business Enterprise (DMBE) by the due date for receipt of bids or proposals. If small business subcontractors are used, the prime contractor agrees to report the use of small business subcontractors by providing the purchasing office at a minimum the following information: name of small business with the DMBE certification number or FEIN, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product/service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807.**

2. Each prime contractor who wins an award in which provision of a small business subcontracting plan is a condition of the award, shall deliver to the contracting agency or institution with every request for payment, evidence of compliance (subject only to insubstantial shortfalls and to shortfalls arising from subcontractor default) with the small business subcontracting plan. **This information shall be submitted to: JMU Office of Procurement Services, SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807.** When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm with the DMBE certification number or FEIN number, phone number, total dollar amount subcontracted, category type (small, women-owned, or minority-owned), and type of product or service provided. Payment(s) may be withheld until compliance with the plan is received and confirmed

by the agency or institution. The agency or institution reserves the right to pursue other appropriate remedies to include, but not be limited to, termination for default.

3. Each prime contractor who wins an award valued over $200,000 shall deliver to the contracting agency or institution with every request for payment, information on use of subcontractors that are not DMBE-certified small businesses. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office at a minimum the following information: name of firm, phone number, FEIN number, total dollar amount subcontracted, and type of product or service provided. **This information shall be submitted to: JMU Office of Procurement Services, Attn: SWAM Subcontracting Compliance, MSC 5720, Harrisonburg, VA 22807.**

K. ADDITIONAL GOODS AND SERVICES: The University may acquire other goods or services that the supplier provides than those specifically solicited. The University reserves the right, subject to mutual agreement, for the Contractor to provide additional goods and/or services under the same pricing, terms, and conditions and to make modifications or enhancements to the existing goods and services. Such additional goods and services may include other products, components, accessories, subsystems, or related services that are newly introduced during the term of this Agreement. Such additional goods and services will be provided to the University at favored nations pricing, terms, and conditions.

L. AUTHORIZATION TO CONDUCT BUSINESS IN THE COMMONWEALTH: A contractor organized as a stock or nonstock corporation, limited liability company, business trust, or limited partnership or registered as a registered limited liability partnership shall be authorized to transact business in the Commonwealth as a domestic or foreign business entity if so required by Title 13.1 or Title 50 of the *Code of Virginia* or as otherwise required by law. Any business entity described above that enters into a contract with a public body shall not allow its existence to lapse or its certificate of authority or registration to transact business in the Commonwealth, if so required under Title 13.1 or Title 50, to be revoked or cancelled at any time during the term of the contract. A public body may void any contract with a business entity if the business entity fails to remain in compliance with the provisions of this section.

M. PUBLIC POSTING OF COOPERATIVE CONTRACTS: James Madison University maintains a web-based contracts database with a public gateway access. Any resulting cooperative contract/s to this solicitation will be posted to the publicly accessible website. Contents identified as proprietary information will not be made public

N. CRIMINAL BACKGROUND CHECKS OF PERSONNEL ASSIGNED BY CONTRACTOR TO PERFORM WORK ON JMU PROPERTY: The Contractor shall obtain criminal background checks on all of their contracted employees who will be assigned to perform services on James Madison University property. The results of the background checks will be directed solely to the Contractor. The Contractor bears responsibility for confirming to the University contract administrator that the background checks have been completed prior to work being performed by their employees or subcontractors. The Contractor shall only assign to work on the University campus those individuals whom it deems qualified and permissible based on the results of completed background checks. Notwithstanding any other provision herein, and to ensure the safety of students, faculty, staff and facilities, James Madison University reserves the right to approve or disapprove any contract employee that will work on JMU property. Disapproval by the University will solely apply to JMU property and should have no bearing on the Contractor's employment of an individual outside of James Madison University.

O. 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:

(i) effective, interactive control and use of the Technology shall be readily achievable by nonvisual means;

(ii) 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;

(iii) nonvisual access technology shall be integrated into any networks used to share communications among employees, program participants or the public; and

(iv) 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, 2.2-3500 through 2.2-3504 of the *Code of Virginia*.

All information technology which, pursuant to this Agreement, 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. (http://www.section508.gov/). 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.*

P. CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION: The contractor assures that information and data obtained as to personal facts and circumstances related to clients will be collected and held confidential, during and following the term of this agreement, and will not be divulged without the individual's and the agency's written consent and only in accordance with federal law or the Code of Virginia. Contractors who utilize, access, or store personally identifiable information as part of the performance of a contract are required to safeguard this information and

immediately notify the agency of any breach or suspected breach in the security of such information. Contractors shall allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting. Contractors and their employees working on this project may be required to sign a confidentiality statement.

Q. EXCESSIVE DOWN TIME: Equipment or software furnished under the contract shall be capable of continuous operation. Should the equipment or software become inoperable for a period of more than 24 hours, the contractor agrees to pro- rate maintenance charges to account for each full day of inoperability. The period of inoperability shall commence upon initial notification. In the event the equipment or software remains inoperable for more than two (2) consecutive calendar days, the contractor shall promptly replace the equipment or software at no charge upon request of the procuring agency. Such replacement shall be with new, unused product(s) of comparable quality, and must be installed and operational within two (2) days following the request for replacement.

R. LATEST SOFTWARE VERSION: Any software product(s) provided under the contract shall be the latest version available to the general public as of the due date of this solicitation.

S. RENEWAL OF MAINTENANCE: Maintenance of the hardware or software specified in the resultant contract may be renewed by the mutual written agreement of both parties for an additional one-year periods, under the terms and conditions of the original contract except as noted herein. Price changes may be negotiated at time of renewal; however, in no case shall the maintenance costs for a succeeding one-year period exceed the prior year's contract price(s), increased or decreased by more than the percentage increase or decrease in the other services category of the CPI-W section of the US Bureau of Labor Statistics Consumer Price Index, for the latest twelve months for which statistics are available.

T. 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.

U. 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.

V. TERM OF SOFTWARE LICENSE: Unless otherwise stated in the solicitation, the software license(s) identified in the pricing schedule shall be purchased on a perpetual basis and shall continue in perpetuity. However the Commonwealth reserves the right to terminate the license at any time, although the mere expiration or termination of this contract shall not be construed as an intent to terminate the license. All acquired license(s) shall be for use at any computing facilities, on any equipment, by any number of users, and for any purposes for which it is procured. The Commonwealth further reserves the right to transfer all rights under the license to another state agency to which some or all of its functions are transferred.

W. 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.

X. TITLE TO SOFTWARE: By submitting a bid or proposal, the bidder or offeror represents and warrants that it is the sole owner of the software or, if 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.

Y. WARRANTY AGAINST SHUTDOWN DEVICES: The contractor warrants that the equipment and software provided under the contract shall not contain any lock, counter, CPU reference, 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.

Z. NEW EQUIPMENT: Unless otherwise expressly stated in this solicitation, any equipment furnished under the contract shall be new, unused equipment.

AA. OPERATIONAL COMPONENTS: Unless otherwise requested in the solicitation, stated equipment prices shall include all cables, connectors, interfaces, documentation for all components, and any other items necessary for full systems operation at the user site. This does not include consumable supplies such as paper, tapes, disks, etc., unless such supplies are expressly identified in the pricing schedule.

BB. REPAIR PARTS: In the event that the performance of maintenance services under the contract results in a need to replace defective parts, such items may only be replaced by new parts. In no instance shall the contractor be permitted to replace defective items with refurbished, remanufactured, or surplus items without prior written authorization of the Commonwealth.

CC. 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.

DD. OPTIONAL PRE-PROPOSAL CONFERENCE: An optional pre-proposal conference will be held at 2:00 p.m. on February 27, 2014 at Massanutten Hall, Room 203, 1031 South Main Street, Harrisonburg, VA 22807. **Offerors are required to register for this pre-proposal conference.** Offerors can register for the optional pre-proposal by emailing owensml@jmu.edu. Registration will end at 5 p.m. on February 26, 2014.

Offerors may also attend the pre-proposal via conference call. Conference call information will be provided at time of registration.

The purpose of this conference is to allow potential Offerors an opportunity to present questions and obtain clarification relative to any facet of this solicitation. While attendance at this conference will not be a prerequisite to submitting a proposal, Offerors who intend to submit a proposal are encouraged to attend. Bring a copy of the solicitation with you. Any changes resulting from this conference will be issued in a written addendum to the solicitation.

IF YOU ARE AN INDIVIDUAL WITH A DISABILITY WITH NEED OF REASONABLE ACCOMMODATIONS TO PARTICIATE IN THIS ACTIVITY, PLEASE NOTIFY MATASHA OWENS AT 540-568-3137 NO LATER THAN FEBRUARY 20, 2014. INDIVIDUALS WITH

HEARING/SPEECH DIS ABILITY ARE ENCO URAGED TO USE THE VIRGINIA RELAY SERVICE. TDD USERS – 800-828-1120.

IX. METHOD OF PAYMENT

The contractor will be paid on the basis of invoices submitted in accordance with the solicitation and any negotiations. James Madison University recognizes the importance of expediting the payment process for our vendors and suppliers. We are asking our vendors and suppliers to enroll in the Wells Fargo Bank single use Commercial Card Number process or electronic deposit (ACH) to your bank account so that future payments are made electronically. Additional information is available online at: http://www.jmu.edu/acctgserv/expenditures/vendor_pay_methods.shtml

X. PRICING SCHEDULE

Provide contract pricing for all products and services included in proposal indicating one-time and on-going costs.

XI. ATTACHMENTS

Attachment A: Offeror Data Sheet

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

Attachment C: Standard Contract Sample

ATTACHMENT A

OFFEROR DATA SHEET

TO BE COMPLETED BY OFFEROR

1. QUALIFICATIONS OF OFFEROR: Offerors must have the capability and capacity in all respects to fully satisfy the contractual requirements.

2. YEARS IN BUSINESS: Indicate the length of time you have been in business providing these types of goods and services.

   Years_____ Months_____

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

CLIENT	LENGTH OF SERVICE	ADDRESS	CONTACT PERSON/PHONE #

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

_____

_____

_____

_____

5. RELATIONSHIP WITH THE COMMONWEALTH OF VIRGINIA: Is any member of the firm an employee of the Commonwealth of Virginia who has a personal interest in this contract pursuant to the CODE OF VIRGINIA, SECTION 2.2-3100 – 3131?
   [ ] YES [ ] NO
   IF YES, EXPLAIN:_____

_____

_____

_____

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B

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

Offeror Name: _____ Preparer Name: _____
Date: _____

Is your firm a **Small Business Enterprise** certified by the Department of Minority Business Enterprise? Yes_____ No_____
If yes, certification number: _____ Certification date:_____

Is your firm a **Woman-owned Business Enterprise** certified by the Department of Minority Business Enterprise? Yes_____ No_____
If yes, certification number: _____ Certification date:_____

Is your firm a **Minority-Owned Business Enterprise** certified by the Department of Minority Business Enterprise? Yes____ No_____
If yes, certification number: _____ Certification date:_____

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

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

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

Program, all certified women-owned businesses are also a small business enterprise.

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

All small, women, and minority owned businesses must be certified by the Commonwealth of Virginia Department of Minority Business Enterprise (DMBE) to be counted in the SWAM program. Certification applications are available through DMBE at 800-223-0671 in Virginia, 804-786-6585 outside Virginia, or online at www.dmbe.virginia.gov (Customer Service).

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT B (CNT'D)

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

Procurement Name and Number: _____

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

_____
Date Form Completed

Offeror / Proposer:

_____ _____ _____
Firm Address Contact Person/No.

Sub-Contractor's Name and Address	Contact Person & Phone Number	DMBE Certification Number or FEIN No.	Services or Materials Provided	Total Subcontractor Contract Amount (to include change orders)	Total Dollars Paid Subcontractor to date (to be submitted with request for payment from JMU)	Federal Employer Identification Number

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

RETURN OF THIS PAGE IS REQUIRED

ATTACHMENT C

COMMONWEALTH OF VIRGINIA

STANDARD CONTRACT

Contract No._____

This contract entered into this_____day of_____20____,by _____ hereinafter called the "Contractor" and Commonwealth of Virginia, James Madison University called the "Purchasing Agency".

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

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

PERIOD OF PERFORMANCE: From _____ through _____

The contract documents shall consist of:

(1) This signed form;

(2) The following portions of the Request for Proposals dated _____:
   (a) The Statement of Needs,
   (b) The General Terms and Conditions,
   (c) The Special Terms and Conditions together with any negotiated modifications of those Special Conditions;
   (d) List each addendum that may be issued

(3) The Contractor's Proposal dated ____ _____and the following negotiated modification to the Proposal, all of which documents are incorporated herein.
   (a) Emails and written negotiations are to be incorporated by specific reference for each one of relevance.

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

CONTRACTOR: PURCHASING AGENCY:

By:_____ By:_____
(Signature) (Signature)

_____ _____
(Printed Name) (Printed Name)

Title:_____ Title:____ _____