



Corporate Headquarters
120 N. LaSalle Street
Suite 1250
Chicago, IL 60602
(312) 443-8028 fax

East Coast Headquarters
116 Defense Highway
Suite 501
Annapolis, MD 21401
(410) 571-8493 fax

Dallas Headquarters
15455 Dallas Parkway
Suite 600
Addison, TX 75001
(972) 764-3231 fax

London Headquarters
90 Long Acre
London WC2E 9RZ
United Kingdom
011 44 207 849 3175 fax



Ambiron Trust Wave

Fax Cover Sheet

Date: 22 August 2006

From: John F Salmon

To: Sharon Thompson - Bid Clerk

Subject: RFQ 1SC60023

Fax Number: (304) 558-3920

Number of pages including cover: 36

Comments:

Buyer: Krista Franzell
(304) - 558-2596

Bid Opening: August 23, 2006
1:30 PM

This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law if the reader of the message is not the intended recipient or the employee or agent responsible for delivering the message to the intended recipient. You are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone (collect), and return the original message to us at the above address via the U.S. Postal Service. Thank you.



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER: ISCG0023

PAGE: 1

ADDRESS CORRESPONDENCE TO ATTENTION OF:
 KRISTA FERRELL
 304-558-2596

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

VENDOR

SHIP TO

DATE PRINTED 08/09/2006	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
BID OPENING DATE: 08/23/2006 BID OPENING TIME 01:30PM				

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
0001	1	LS		205-43		
INTRUSION DETECTION SYSTEM (IDS) PER THE ATTACHED REQUEST FOR QUOTATION THE WEST VIRGINIA PURCHASING DIVISION FOR THE AGENCY, THE WEST VIRGINIA DEPARTMENT OF ADMINISTRATION'S OFFICE OF TECHNOLOGY, IS SOLICITING BIDS TO PROVIDE THE AGENCY WITH SUPPORT ON AN INTRUSION DETECTION SYSTEM FOR THE STATE OF WEST VIRGINIA CAPITOL COMPLEX BACKBONE, MONITOR A GIGABIT FULL DUPLEX INTERFACE CARRYING TRAFFIC BETWEEN THE CAPITOL COMPLEX BACKBONE AND THE WEST VIRGINIA STATE UNIFIED NETWORK, USING THE EXISTING SENSOR IDENTIFIED IN THE ATTACHED DIAGRAM, AND PROVIDE RAPID WARNINGS TO THE WEST VIRGINIA OFFICE OF TECHNOLOGY POINT OF CONTACT TO ALERT HIM/HER TO POSSIBLE NETWORK SECURITY THREATS PER THE ATTACHED SPECIFICATIONS. THE MONITORING SHALL COMMENCE WITHIN 30 DAYS FOLLOWING THE ISSUANCE OF THE PURCHASE ORDER TO THE SUCCESSFUL BIDDER. START DATES WILL BE ESTABLISHED BY CHANGE ORDER. EXHIBIT 3 LIFE OF CONTRACT: THIS CONTRACT BECOMES EFFECTIVE ON UPON AWARD AND EXTENDS FOR A PERIOD OF ONE (1) YEAR OR UNTIL SUCH "REASONABLE TIME" THEREAFTER AS IS						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**Request for
 Quotation**

RFQ NUMBER:
 ISCG0023

PAGE:
 2

ADDRESS CORRESPONDENCE TO ATTENTION OF:
 KRISTA FERRELL
 304-558-2596

VENDOR

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

SHIP TO

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

DATE PRINTED 08/09/2006	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
BID OPENING DATE: 08/23/2006	BID OPENING TIME 01:30PM			

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>NECESSARY TO OBTAIN A NEW CONTRACT OR RENEW THE ORIGINAL CONTRACT. THE "REASONABLE TIME" PERIOD SHALL NOT EXCEED TWELVE (12) MONTHS. DURING THIS "REASONABLE TIME" THE VENDOR MAY TERMINATE THIS CONTRACT FOR ANY REASON UPON GIVING THE DIRECTOR OF PURCHASING 30 DAYS WRITTEN NOTICE.</p> <p>UNLESS SPECIFIC PROVISIONS ARE STIPULATED ELSEWHERE IN THIS CONTRACT DOCUMENT, THE TERMS, CONDITIONS AND PRICING SET HEREIN ARE FIRM FOR THE LIFE OF THE CONTRACT.</p> <p>RENEWAL: THIS CONTRACT MAY BE RENEWED UPON THE MUTUAL WRITTEN CONSENT OF THE SPENDING UNIT AND VENDOR, SUBMITTED TO THE DIRECTOR OF PURCHASING THIRTY (30) DAYS PRIOR TO THE EXPIRATION DATE. SUCH RENEWAL SHALL BE IN ACCORDANCE WITH THE TERMS AND CONDITIONS OF THE ORIGINAL CONTRACT AND SHALL BE LIMITED TO TWO (2) ONE (1) YEAR PERIODS.</p> <p>CANCELLATION: THE DIRECTOR OF PURCHASING RESERVES THE RIGHT TO CANCEL THIS CONTRACT IMMEDIATELY UPON WRITTEN NOTICE TO THE VENDOR IF THE COMMODITIES AND/OR SERVICES SUPPLIED ARE OF AN INFERIOR QUALITY OR DO NOT CONFORM TO THE SPECIFICATIONS OF THE BID AND CONTRACT HEREIN.</p> <p>OPEN MARKET CLAUSE: THE DIRECTOR OF PURCHASING MAY AUTHORIZE A SPENDING UNIT TO PURCHASE ON THE OPEN MARKET, WITHOUT THE FILING OF A REQUISITION OR COST ESTIMATE, ITEMS SPECIFIED ON THIS CONTRACT FOR IMMEDIATE DELIVERY IN EMERGENCIES DUE TO UNFORESEEN CAUSES (INCLUDING BUT NOT LIMITED TO DELAYS IN TRANSPORTATION OR AN UNANTICIPATED INCREASE IN THE VOLUME OF WORK.)</p> <p>QUANTITIES: QUANTITIES LISTED IN THE REQUISITION ARE</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**Request for
 Quotation**

RFQ NUMBER
 ISCG0023

PAGE
 3

ADDRESS: CORRESPONDENCE TO ATTENTION OF:
 KRISTA FERRELL
 304-558-2596

VENDOR

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

SHIP TO

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

DATE PRINTED: 08/09/2006	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
BID OPENING DATE: 08/23/2006	BID OPENING TIME			01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>APPROXIMATIONS ONLY, BASED ON ESTIMATES SUPPLIED BY THE STATE SPENDING UNIT. IT IS UNDERSTOOD AND AGREED THAT THE CONTRACT SHALL COVER THE QUANTITIES ACTUALLY ORDERED FOR DELIVERY DURING THE TERM OF THE CONTRACT, WHETHER MORE OR LESS THAN THE QUANTITIES SHOWN.</p> <p>BANKRUPTCY: IN THE EVENT THE VENDOR/CONTRACTOR FILES FOR BANKRUPTCY PROTECTION, THIS CONTRACT IS AUTOMATICALLY NULL AND VOID, AND IS TERMINATED WITHOUT FURTHER ORDER.</p> <p>THE TERMS AND CONDITIONS CONTAINED IN THIS CONTRACT SHALL SUPERSEDE ANY AND ALL SUBSEQUENT TERMS AND CONDITIONS WHICH MAY APPEAR ON ANY ATTACHED PRINTED DOCUMENTS SUCH AS PRICE LISTS, ORDER FORMS, SALES AGREEMENTS OR MAINTENANCE AGREEMENTS, INCLUDING ANY ELECTRONIC MEDIUM SUCH AS CD-ROM.</p> <p>REV. 04/11/2001</p> <p style="text-align: center;">VENDOR PREFERENCE CERTIFICATE</p> <p>CERTIFICATION AND APPLICATION* IS HEREBY MADE FOR PREFERENCE IN ACCORDANCE WITH WEST VIRGINIA CODE, 5A-3-37 (DOES NOT APPLY TO CONSTRUCTION CONTRACTS).</p> <p>A. APPLICATION IS MADE FOR 2.5% PREFERENCE FOR THE REASON CHECKED:</p> <p>() BIDDER IS AN INDIVIDUAL RESIDENT VENDOR AND HAS RESIDED CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR</p> <p>() BIDDER IS A PARTNERSHIP, ASSOCIATION OR CORPORA-</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS			
SIGNATURE	TELEPHONE	DATE	
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE	

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**Request for
 Quotation**

RFQ NUMBER
 ISCG0023

PAGE
 4

ADDRESS CORRESPONDENCE TO ATTENTION OF
 KRISTA FERRELL
 304-558-2596

V
E
N
D
O
R

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

S
H
I
P
T
O

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/09/2006				

BID OPENING DATE: 08/23/2006 BID OPENING TIME 01:30PM

LINE	QUANTITY	UOP	CAT. NO.	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>TION RESIDENT VENDOR AND HAS MAINTAINED ITS HEAD- QUARTERS OR PRINCIPAL PLACE OF BUSINESS CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR 80% OF THE OWNERSHIP INTEREST OF BIDDER IS HELD BY ANOTHER INDIVIDUAL, PARTNERSHIP, ASSOCIATION OR CORPORATION RESIDENT VENDO WHO HAS MAINTAINED ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS CONTINUOUSLY IN WEST VIRGINIA FOR FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION; OR</p> <p>() BIDDER IS A CORPORATION NONRESIDENT VENDOR WHICH HAS AN AFFILIATE OR SUBSIDIARY WHICH EMPLOYS A MINIMUM OF ONE HUNDRED STATE RESIDENTS AND WHICH HAS MAINTAINED ITS HEAQUARTERS OR PRINCIPAL PLACE OF BUSINESS WITHIN WEST VIRGINIA CONTINUOUSLY FOR THE FOUR (4) YEARS IMMEDIATELY PRECEDING THE DATE OF THIS CERTIFICATION.</p> <p>B. APPLICATION IS MADE FOR 2.5% PREFERENCE FOR THE REASON CHECKED:</p> <p>() BIDDER IS A RESIDENT VENDOR WHO CERTIFIES THAT, DURING THE LIFE OF THE CONTRACT, ON AVERAGE AT LEAST 75% OF THE EMPLOYEES WORKING ON THE PROJECT BEING BID ARE RESIDENTS OF WEST VIRGINIA WHO HAVE RESIDED IN THE STATE CONTINUOUSLY FOR THE TWO YEARS IMMEDIATELY PRECEDING SUBMISSION OF THIS BID; OR</p> <p>() BIDDER IS A NONRESIDENT VENDOR EMPLOYING A MINIMUM OF ONE HUNDRED STATE RESIDENTS OR IS A NONRESIDENT VENDOR WITH AN AFFILIATE OR SUBSIDIARY WHICH MAINTAINS ITS HEADQUARTERS OR PRINCIPAL PLACE OF BUSINESS WITHIN WEST VIRGINIA EMPLOYING A MINIMUM OF ONE HUNDRED STATE RESIDENTS WHO CERTIFIES THAT, DURING THE LIFE OF THE CONTRACT, ON AVERAGE AT LEAST</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE TELEPHONE DATE

TITLE FEIN ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

Request for Quotation

RFQ NUMBER: ISCG0023

PAGE: 5

ADDRESS CORRESPONDENCE TO ATTENTION OF:
 KRISTA FERRELL
 304-558-2596

VENDOR

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

SHIP TO

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

DATE PRINTED: 08/09/2006	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
BID OPENING DATE: 08/23/2006		BID OPENING TIME 01:30PM		

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>75% OF THE EMPLOYEES OR BIDDERS' AFFILIATE'S OR SUBSIDIARY'S EMPLOYEES ARE RESIDENTS OF WEST VIRGINIA WHO HAVE RESIDED IN THE STATE CONTINUOUSLY FOR THE TWO YEARS IMMEDIATELY PRECEDING SUBMISSION OF THIS BID.</p> <p>BIDDER UNDERSTANDS IF THE SECRETARY OF TAX & REVENUE DETERMINES THAT A BIDDER RECEIVING PREFERENCE HAS FAILED TO CONTINUE TO MEET THE REQUIREMENTS FOR SUCH PREFERENCE, THE SECRETARY MAY ORDER THE DIRECTOR OF PURCHASING TO: (A) RESCIND THE CONTRACT OR PURCHASE ORDER ISSUED; OR (B) ASSESS A PENALTY AGAINST SUCH BIDDER IN AN AMOUNT NOT TO EXCEED 5% OF THE BID AMOUNT AND THAT SUCH PENALTY WILL BE PAID TO THE CONTRACTING AGENCY OR DEDUCTED FROM ANY UNPAID BALANCE ON THE CONTRACT OR PURCHASE ORDER.</p> <p>BY SUBMISSION OF THIS CERTIFICATE, BIDDER AGREES TO DISCLOSE ANY REASONABLY REQUESTED INFORMATION TO THE PURCHASING DIVISION AND AUTHORIZES THE DEPARTMENT OF TAX AND REVENUE TO DISCLOSE TO THE DIRECTOR OF PURCHASING APPROPRIATE INFORMATION VERIFYING THAT BIDDER HAS PAID THE REQUIRED BUSINESS TAXES, PROVIDED THAT SUCH INFORMATION DOES NOT CONTAIN THE AMOUNTS OF TAXES PAID NOR ANY OTHER INFORMATION DEEMED BY THE TAX COMMISSIONER TO BE CONFIDENTIAL.</p> <p>UNDER PENALTY OF LAW FOR FALSE SWEARING (WEST VIRGINIA CODE 61-5-3), BIDDER HEREBY CERTIFIES THAT THIS CERTIFICATE IS TRUE AND ACCURATE IN ALL RESPECTS; AND THAT IF A CONTRACT IS ISSUED TO BIDDER AND IF ANYTHING CONTAINED WITHIN THIS CERTIFICATE CHANGES DURING THE TERM OF THE CONTRACT, BIDDER WILL NOTIFY THE PURCHASING DIVISION IN WRITING IMMEDIATELY.</p> <p>BIDDER: <i>Ambraon Trustwave</i></p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**Request for
 Quotation**

RFQ NUMBER
 ISCG0023

PAGE
 6

ADDRESS CORRESPONDENCE TO ATTENTION OF
 KRISTA FERRELL
 304-558-2596

VENDOR FOR

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

SHIP TO

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/09/2006				
BID OPENING DATE: 08/23/2006		BID OPENING TIME 01:30PM		

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
<p>DATE: <u>August 22, 2006</u></p> <p>SIGNED: <u><i>Joseph Patanella</i></u></p> <p>TITLE: <u>PRESIDENT</u></p>						
<p>* CHECK ANY COMBINATION OF PREFERENCE CONSIDERATION(S) IN EITHER "A" OR "B", OR BOTH "A" AND "B" WHICH YOU ARE ENTITLED TO RECEIVE. YOU MAY REQUEST UP TO THE MAXIMUM 5% PREFERENCE FOR BOTH "A" AND "B". (REV. 12/00)</p>						
<p>NOTICE</p> <p>A SIGNED BID MUST BE SUBMITTED TO:</p> <p>DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION BUILDING 15 2019 WASHINGTON STREET, EAST CHARLESTON, WV 25305-0130</p>						
<p>THE BID SHOULD CONTAIN THIS INFORMATION ON THE FACE OF THE ENVELOPE OR THE BID MAY NOT BE CONSIDERED:</p> <p>SEALED BID</p>						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'



State of West Virginia
 Department of Administration
 Purchasing Division
 2019 Washington Street East
 Post Office Box 50130
 Charleston, WV 25305-0130

**Request for
 Quotation**

RFQ NUMBER:
 ISCG0023

PAGE:
 7

ADDRESS CORRESPONDENCE TO ATTENTION OF:
 KRISTA FERRELL
 304-558-2596

*128131410 410-573-6910
 TRUSTWAVE CORP
 201 DEFENSE HWY
 SUITE 205
 ANNAPOLIS MD 21401

DEPARTMENT OF ADMINISTRATION
 IS&C - CHIEF FINANCIAL OFFICER
 1 DAVIS SQUARE
 CHARLESTON, WV
 25301 304-558-5472

DATE PRINTED	TERMS OF SALE	SHIP VIA	F.O.B.	FREIGHT TERMS
08/09/2006				
BID OPENING DATE: 08/23/2006		BID OPENING TIME 01:30PM		

LINE	QUANTITY	UOP	CAT NO	ITEM NUMBER	UNIT PRICE	AMOUNT
BUYER:				21		
RFQ. NO.:				ISCG0023		
BID OPENING DATE:				08/23/2006		
BID OPENING TIME:				1:30 PM		
PLEASE PROVIDE A FAX NUMBER IN CASE IT IS NECESSARY TO CONTACT YOU REGARDING YOUR BID:						
				(410) 571-8493		
CONTACT PERSON (PLEASE PRINT CLEARLY):						
				John F. Selman		
				(410) 804-1600		
***** THIS IS THE END OF RFQ ISCG0023 ***** TOTAL:						

SEE REVERSE SIDE FOR TERMS AND CONDITIONS

SIGNATURE	TELEPHONE	DATE
TITLE	FEIN	ADDRESS CHANGES TO BE NOTED ABOVE

WHEN RESPONDING TO RFQ, INSERT NAME AND ADDRESS IN SPACE ABOVE LABELED 'VENDOR'

West Virginia Office of Technology
Intrusion Detection RFQ - ISCG0023

008

A. Introduction

The successful vendor will partner with the West Virginia Office of Technology (WV-OT) on the support of an Intrusion Detection System (IDS) (24x7x365) for the State of West Virginia Capitol Complex backbone, monitor a Gigabit full duplex interface carrying traffic between the Capitol Complex backbone and the West Virginia State Unified Network, using the existing sensor identified in the attached diagram, and provide rapid warnings to the WEST VIRGINIA OFFICE OF TECHNOLOGY point of contact to alert him/her to possible network security threats.

B. Overview:

The West Virginia State Capitol backbone consists of nine Routers distributed around the Capitol complex and connected by a Gigabit fiber optical cable. The Router in the communication vault connects to the WVSUN network, and eventually to the Internet. The WVSUN network and backbone are protected from the internet by firewalls, but the host population inside of the firewalls is large, and includes Colleges, Universities, and libraries throughout the state. A diagram of this configuration is attached

The successful vendor will install an Intrusion Detection System (24x7x365) for the State of West Virginia Capitol Complex backbone, monitor the traffic flowing in and out of the backbone and the outside world, and provide warnings to the WEST VIRGINIA OFFICE OF TECHNOLOGY POC to alert him/her to possible network security threats.

C. Delivery: The monitoring shall commence within thirty days (30) days following issuance of a Purchase Order.

D. Contract: West Virginia Office of Technology is requesting a one (1) year contract with the possibility of two (2) one (1) year renewals for a total of three years.

E. Technical Requirements:

1. At the time of award of this contract West Virginia Office of Technology will designate an individual to be the primary point of contact for IDS and other network security related matters. This individual may temporarily or permanently appoint additional individuals to share these duties. These individuals are referred to in this document as the "West Virginia Office of Technology Points of Contact (POC)." A call-down order for POC notification will be provided by the WV-OT.

General:

2. The successful vendor will monitor the traffic between the Capitol Complex backbone and the West Virginia State Unified Network, and advise the West Virginia Office of Technology POC rapidly in the event of the detection of a possible network security threat.

West Virginia Office of Technology**Intrusion Detection RFQ ISCG0023**

010

not limit in any way the additional actions which the State may take regarding the vendor's breach of contract. Upon termination of any contract resulting from this RFQ, under normal end-of-contract conditions, all data collected by the vendor about the State's network and network traffic will be returned or destroyed.

Software, Installation and Maintenance

9. The West Virginia Office of Technology will maintain a licensed copy of the Enterasys Dragon software and the current version of Red Hat Linux Operating System software.

10. The West Virginia Office of Technology maintains one server loaded with the Linux OS, Dragon Sensor, Dragon Policy Manager, and replication agent. A second server is loaded with Linux OS and configured with the Dragon Event Flow Process, Real Time Console, and Forensic Tool

11. The vendor shall be responsible for updating any new software patches, maintenance, security updates (for the Dragon software and operating system), or updated attack signatures as they become available from the manufacturer. All changes necessary to preserve system security must be performed. The vendor shall notify the West Virginia Office of Technology POC of any and all maintenance work performed on the servers (patches, updates, etc)

12. The West Virginia Office of Technology POC will be notified 24 hours in advance when any maintenance procedure will be performed.

Hardware:

13. West Virginia Office of Technology currently maintains two Dell PowerEdge 1550 Servers (each server has the following configuration: 1.2 GHz processor, 512 MB RAM, 36GB 15,000 RPM Ultra 3 Hard Disk, Floppy Drive, CD Drive and Dual 100 Mb Intel NICs). These systems are to be utilized for system scans, as needed and requested by the West Virginia Office of Technology.

14. West Virginia Office of Technology's Technical Resource Center will provide hardware maintenance support for these servers.

15. West Virginia Office of Technology has installed a sensor at the point of connection between the State Backbone network and the WWSUN/Internet network.

Network Monitoring:

16. The vendor will, through his Network Security Center (NSC), monitor the IDS system continuously (24x7x365) and promptly advise the West Virginia Office of Technology POC of threats to network security in a timely manner appropriate to the threat. Prompt notification of severe threats or attacks-in progress must be given 24 hours per day, and, depending upon threat severity, the notification response time frame shall not exceed 15 minutes. See Notification and Escalations Procedures table in this document for additional details about vendor and State responsibilities.

West Virginia Office of Technology

Intrusion Detection RFQ ISCG0023

012

9) False positive rule sets,

c. In addition to the above reports, the vendor will provide the ability for the West Virginia Office of Technology POC to run additional reports as needed via the secure web portal.

A high-level diagram of the network will be available upon request from qualified vendors.

West Virginia Office of Technology**Intrusion Detection RFQ ISCG0023**

013

Responsibilities Matrix

As part of this Intrusion Detection service, both the "Successful Vendor" and the State of West Virginia will generally perform, and have responsibility for, specific tasks following an incident. This section details those proposed responsibilities and duties.

Phase	Successful Vendor	State of West Virginia
Initial Startup	The Successful Vendor will provide the facilities, equipment and staff to collect IDS events and work closely with the State to establish effective connectivity to enable monitoring of traffic and detection of incidents	The State will work closely with the successful vendor to ensure that all connections required for effective network traffic monitoring are properly established and operational. WV will provide POC listing, and provide calldown instructions for various scenarios.
Incident Detection	The SV will report attacks-in-progress, or other severe threats to the State POC within 15 minutes of detection, and document successful contact (event type, severity level, person successfully reached, time, etc.). Less severe threats (such as the detection of traffic associated with file sharing programs in common use), will be reported to the POC utilizing e-mail, the WEB reporting portal, and any other "channel" specified by the State.	Once the IDS is configured, the State of West Virginia should not need to be involved in the initial Detection of incidents.
Verification and Response	The SV will provide expert skills to assist the WV State POC in the analysis of any notification sent by the SV to the State, in order to clarify the assessment of severity, and to provide any other assistance that is reasonably requested, and within the skill set of the SV.	The State of West Virginia (or contracted staff) will analyze the threat notification and the potential for negative impact, and take any required actions to prevent or contain the threat or attack.
Stabilization and Assessment	The SV will continue to reasonably assist the WV POC as needed during the incident	The State of West Virginia will maintain active communication with the SV during the

RFQ No. ISCG0023**A F F I D A V I T**

016

West Virginia Code §5A-3-10a states:

No contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and the debt owned is an amount greater than one thousand dollars in the aggregate.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Debtor" means any individual, corporation, partnership, association, limited liability company or any other form or business association owing a debt to the state or any of its political subdivisions.

"Political subdivision" means any county commission; municipality; county board of education; any instrumentality established by a county or municipality; any separate corporation or instrumentality established by one or more counties or municipalities, as permitted by law; or any public body charged by law with the performance of a government function or whose jurisdiction is coextensive with one or more counties or municipalities.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceeds five percent of the total contract amount.

EXCEPTION:

The prohibition of this section does not apply where a vendor has contested any tax administered pursuant to chapter eleven of this code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

LICENSING:

The vendor must be licensed in accordance with any and all state requirements to do business with the state of West Virginia.

CONFIDENTIALITY:

The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures and rules. Vendors should visit www.state.wv.us/admin/purchase/privacy for the Notice of Agency Confidentiality Policies.

Under penalty of law for false swearing (West Virginia Code, §61-5-3), it is hereby certified that the vendor acknowledges the information in this said affidavit and are in compliance with the requirements as stated.

Vendor's Name: Ambirson Trust ServicesAuthorized Signature: Joseph A. PetanilloDate: 22 AUG 2006

Corporate Headquarters
120 N. LaSalle Street
Chicago, IL 60602
(877) 262-1111



AmbironTrustWave
www.atwcorp.com

Intrusion Detection System RFQ ISCG0023 Response

Presented To:

West Virginia Office of Technology

August 23, 2006

Prepared By:

John Salmon

john.salmon@atwcorp.com

Phone: (410) 804-1600

PROPRIETARY INFORMATION

This proposal may only be used for evaluating the planned services designated herein, and may contain information that is privileged, confidential or otherwise protected from disclosure. Dissemination, distribution or copying of this proposal or the information herein is prohibited without prior written permission of AmbironTrustWave.

Copyright © 2006 AmbironTrustWave. All Rights Reserved.

AMBIRONTRUSTWAVE PROPRIETARY INFORMATION



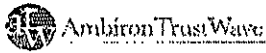


Table of Contents

EXECUTIVE OVERVIEW	9
RFQ REQUIREMENTS AND ASSUMPTIONS	10
Delivery	10
Contract.....	10
Technical Requirements	10
General.....	10
Software, Installation and Maintenance.....	11
Hardware	11
Network Monitoring	11
Reporting	12
PROGRAM MANAGEMENT	13
Discovery	13
Kickoff Meeting	13
Project Definition and Development	13
Coordination of Project and Testing.....	13
STATEMENT OF WORK	14
IDS Integration and Tuning	14
Services Integration.....	14
Dragon Sensor Tuning.....	14
Installation Documentation.....	14
IDS Management and Monitoring Service Components.....	15
Change Control Procedures.....	15
Recurring Solution Review	15
IDS Maintenance	15
Notification and Escalation Procedures.....	16
Web-Portal Access and Reporting	18
Event Reporting and Management Architecture	19
Network Vulnerability Scanning.....	20
TrustKeeper Scan Parameters and Connections	20
TrustKeeper Operation	21
COST PROPOSAL, PREREQUISITES AND CONTACT INFORMATION	23
Cost Proposal.....	23
Prerequisites and Contact Information	23
TERMS AND CONDITIONS	24
SIGNATURES	27

EXECUTIVE OVERVIEW

AmbironTrustWave ("ATW") will partner with the West Virginia Office of Technology ("WV-OT" and "Client") on the support of an Intrusion Detection System (IDS) (24x7x365) for the West Virginia Office of Technology Capitol Complex backbone, monitor a Gigabit full duplex interface carrying traffic between the Capitol Complex backbone and the West Virginia State Unified Network, using the existing sensor identified in RFQ ISCG0023, and provide rapid warnings to the West Virginia Office of Technology point of contact to alert him/her to possible network security threats.

ATW proposes to support the West Virginia Office of Technology's existing Enterasys Dragon Intrusion Detection System by providing the products, consulting and managed security services defined in this Statement of Work (SOW). The specific areas to be addressed and the products and services included to attain the defined goals are:

- Provide the West Virginia Office of Technology with expert 24x7 remote monitoring and management of the currently ATW deployed and managed Enterasys Dragon Intrusion Detection System.
- Provide the West Virginia Office of Technology with TrustKeeper Enterprise Vulnerability Scanning and Management.

The West Virginia State Capitol backbone consists of nine Routers distributed around the Capitol complex and connected by a Gigabit fiber optical cable. The Router in the communication vault connects to the WVSUN network, and eventually to the Internet. The WVSUN network and backbone are protected from the internet by firewalls, but the host population inside of the firewalls is large, and includes Colleges, Universities, and libraries throughout the state. A diagram of this configuration is attached

ATW will maintain and continue to provide Intrusion Detection System services (24x7x365) for the West Virginia Office of Technology Capitol Complex backbone, monitor the traffic flowing in and out of the backbone and the outside world, and provide warnings to the West Virginia Office of Technology POC to alert him/her to possible network security threats.

During this effort, ATW will work with the West Virginia Office of Technology to identify/confirm the assets being protected, the alert scenarios that may be expected, and the networking environment and organization capabilities where the IDS is deployed. ATW will continue the management and monitoring of the currently deployed Intrusion Detection System.

For the purpose of this Statement of Work, ATW has identified the following areas of focus:

Managed Intrusion Detection - ATW will remotely monitor and administer the Dragon IDS to provide the West Virginia Office of Technology 24x7 protection by expert security professionals. ATW will continue to provide an effective and efficient IDS monitoring solution including complete alert signatures and system management. ATW's staff will configure, test, and tune the IDS while working with the State to update and confirm response procedures tailored to the organization's needs. Experienced security staff working in ATW's Network Security Operations Center will continue to monitor and manage the IDS 24/7/365.

TrustSentry® Web Portal - ATW's TrustSentry® Web will continue to provide a secure browser interface to the TrustSentry® site allowing designated West Virginia Office of Technology staff to securely log in, submit and view trouble tickets and status, look at their device status, raw data, and generate custom reports in real-time. The TrustSentry Web Portal provides a complete view into the security infrastructure protecting their enterprise.

Vulnerability Scanning - ATW will continue the existing vulnerability scanning capabilities at the West Virginia Office of Technology site Capitol Complex site.

RFQ REQUIREMENTS AND ASSUMPTIONS

Delivery

The monitoring shall commence within thirty days (30) days following issuance of a Purchase Order.

Contract

West Virginia Office of Technology is requesting a one (1) year contract with the possibility of two (2) one (1) year renewals for a total of three years.

Technical Requirements

At the time of award of this contract West Virginia Office of Technology will designate an individual to be the primary point of contact for IDS and other network security related matters. This individual may temporarily or permanently appoint additional individuals to share these duties. These individuals are referred to in this document as the "West Virginia Office of Technology Points of Contact (POC)." A call-down order for POC notification will be provided by the WV-OT.

General

ATW will monitor the traffic between the Capitol Complex backbone and the West Virginia State Unified Network, and advise the West Virginia Office of Technology POC rapidly in the event of the detection of a possible network security threat.

ATW complies and/or exceeds the following West Virginia Office of Technology RFQ requirements:

- ATW is a National Security Agency IAM (Information Assurance Methodology) certified provider. This organization is certified by NSA to carry out Critical Infrastructure Assessments based on the INFOSEC Methodology as laid out by NSA and NIST.
- ATW currently supports no fewer than 50 locations, and in at least 20 of these installations are monitoring Gigabit links.
- ATW has been providing intrusion monitoring and reporting services for 10+ years.
- ATW employs 30+ CISSP (Certified Information System Security Professionals) full time on staff.

ATW has provided a detailed notification and escalation procedure that ensures rapid involvement of senior management and technical personnel on problems and issues supporting the Dragon IDS. ATW's notification and escalation procedures include the time constraints between different steps.

From time to time, as requested by the West Virginia Office of Technology POC, ATW shall scan the State's public Class B address space, including routers, fire walls, servers, and workstations, to identify security vulnerabilities. ATW will prioritize such vulnerabilities and advise the West Virginia Office of Technology POC of the vulnerabilities and appropriate remedial action ATW has quoted, as a separate line item, the fee for this service. ATW will provide both a summary and a detailed scan report to the West Virginia Office of Technology POC within seven days of the scan.

Upon request from the West Virginia Office of Technology POC, ATW will conduct a scan of the State's private Class A address space, or a Class B or Class C portion of it, including routers, firewalls, servers, and workstations, to identify security vulnerabilities. ATW will prioritize such vulnerabilities and advise the West Virginia Office of Technology POC of the vulnerabilities and appropriate remedial action, ATW has quoted, as separate line item, the fee for this service. ATW will provide both a summary and a detailed report to the West Virginia Office of Technology POC within seven days of the scan.

Any and all transfer of data between IDS and ATW's network operation center will be protected by AES encryption at a minimum.

All network documentation, all captured data, and all information derived from these are confidential. Such data shall be stored only on secure systems in the West Virginia Office of Technology Communications Vault and/or secure systems in ATW's Network Security Center. During transport, the

data shall be protected by AES encryption. Captured data and all information derived from this data shall not be disclosed to any individual or entity except to the designated West Virginia Office of Technology points of contact. Upon any other disclosure, the State may, at its option, terminate for cause. This shall not limit in any way the additional actions which the State may take regarding the vendor's breach of contract. Upon termination of any contract resulting from this RFQ, under normal end-of-contract conditions, all data collected by ATW about the State's network and network traffic will be returned or destroyed.

Software, Installation and Maintenance

The West Virginia Office of Technology will maintain a licensed copy of the Enterasys Dragon software and the current version of Red Hat Linux Operating System software.

West Virginia Office of Technology maintains one server loaded with the Linux OS, Dragon Sensor, Dragon Policy Manager, and replication agent. A second server is loaded with Linux OS and configured with the Dragon Event Flow Process, Real Time Console, and Forensic Tool.

ATW will be responsible for updating any new software patches, maintenance, security updates (for the Dragon software and operating system), or updated attack signatures as they become available from the manufacturer. All changes necessary to preserve system security will be performed. ATW will notify and coordinate with the West Virginia Office of Technology POC for any and all maintenance work performed on the servers (patches, updates, etc).

The West Virginia Office of Technology POC will be notified 24 hours in advance when any maintenance procedure will be performed.

Hardware

West Virginia Office of Technology currently maintains two Dell PowerEdge 1550 Servers (each server has the following configuration: 1.2 GHz processor, 512 MB RAM, 36GB 15,000 RPM Ultra 3 Hard Disk, Floppy Drive, CD Drive and Dual 100 Mb Intel NICs). These systems are to be utilized for system scans, as needed and requested by the West Virginia Office of Technology.

West Virginia Office of Technology's Technical Resource Center will provide hardware maintenance support for these servers.

West Virginia Office of Technology has installed a sensor at the point of connection between the State Backbone network and the WVSUN/Internet network.

Network Monitoring

ATW will, through its Network Security Center (NSC), monitor the IDS system continuously (24x7x365) and promptly advise the West Virginia Office of Technology POC of threats to network security in a timely manner appropriate to the threat. Prompt notification of severe threats or attacks-in progress will be given 24 hours per day, and, depending upon threat severity, the notification response timeframe shall not exceed 15 minutes.

*See Notification and Escalations Procedures table in this document for additional details about ATW and State responsibilities.

ATW will provide new real-time statistics on the Dragon IDS which cover both in-bound and out-bound connections, and detail source and destination IP addresses, as well as the overall activity on the network.

ATW will work with the West Virginia Office of Technology POC to update and maintain appropriate rule sets for the IDS to eliminate false positive intrusion alerts. These rule sets shall be documented by the vendor and provided to the West Virginia Office of Technology POC on a daily basis

ATW will utilize the Dragon IDS to detect (where possible) virus activity to or from the West Virginia capitol complex.

When new threats or vulnerabilities identified in the computer security community or activities/scenarios brought to ATW's attention by the West Virginia Office of Technology point of contact, ATW shall begin

active monitoring for the new threat or exploitation of vulnerability within 2 hours upon release of signature by Enterasys and/or ATW.

ATW will provide the TrustSentry secure web portal interface to allow the West Virginia Office of Technology to view the Intrusion Detection System (IDS) status and configurations, submit and track change request and trouble tickets, generate tailored reports and view archived reports. ATW will provide West Virginia Office of Technology with passwords and necessary administrative information with which to be able to effectively use the TrustSentry web portal.

Reporting

ATW will meet the following IDS RFQ reporting requirements at a minimum:

Daily:

ATW will daily email, to the West Virginia Office of Technology POC, a summary of events which list any attempted intrusions, scans, or other unusual activity on the network during the previous 24 hours. At a minimum, this report shall include:

List of incidents which occurred during the reporting period, including

- Outside/inside IP addresses, port number, intrusion type, etc.
- Repetitive incidents or trends
- False positive rule sets

Monthly:

ATW will provide the West Virginia Office of Technology with a comprehensive activity report. This report will be provided in electronic format via ATW's TrustSentry web portal and e-mailed to West Virginia Office of Technology's POC. At a minimum, this report will include:

- A list of incidents which occurred during the reporting period, including outside/inside IP addresses, port number, intrusion type, etc.
- Status of customer change requests received and processed during the month
- IDS event summaries and statistics
- Details of Customer contract information and changes
- IDS maintenance activities performed during the month
- Any repetitive incidents or trends noted during the month
- False positive rule sets

In addition to the above reports, ATW provides the ability for the West Virginia Office of Technology POC to run additional reports as needed via the TrustSentry secure web portal.

PROGRAM MANAGEMENT

ATW will assign a program manager to oversee all engagement activities. This person will coordinate and schedule required activities and resources with the West Virginia Office of Technology and will serve as the primary contact for the West Virginia Office of Technology throughout the engagement. The program manager will ensure the quality of all ATW deliverables and will work with the West Virginia Office of Technology to resolve any issues that may arise throughout the course of the project.

Discovery

A representative from West Virginia Office of Technology will be asked to provide information regarding the network topology, internal applications and data stores, Internet and remote access capabilities, WAN configuration, network diagrams, and a written copy of any existing computer or network security policies and procedures or incident response guidelines, and other pertinent information. This information will allow ATW to become familiar with the West Virginia Office of Technology's existing security posture throughout to the engagement.

Kickoff Meeting

The kickoff meeting is typically a short, targeted meeting intended to explain the goals of the engagement to the participants, as well as to describe the development methodology and final products. During the kickoff meeting, ATW will speak with the key IT personnel and set the engagement goals, identify the overall organizational structure, and define the schedule for additional working sessions. The product of the kickoff meeting will be a project schedule including anticipated tasks and completion timeline.

Project Definition and Development

ATW will work with the West Virginia Office of Technology staff to understand their requirements for system isolation and monitoring, and to confirm and update the plan for tuning and escalation procedure integration for the various IDS components. Based on the West Virginia Office of Technology policy requirements, network topology, applications, operating systems, and alerting/reporting requirements, ATW will develop a detailed program plan, and incident reporting procedures. All documents will be reviewed by the West Virginia Office of Technology prior to solution implementation/updating.

Coordination of Project and Testing

All IDS and Scanning project and testing phases are fully coordinated with the client representatives to minimize impacts that may occur as a result of ATW services. While it is solely the client's decision and responsibility to inform other individuals, components, divisions and management, we strongly encourage and recommend full-disclosure of the testing to ALL individuals responsible for the network and related services and devices. Although ATW takes precautions to minimize negative impact on client systems, we do not guarantee against service interruptions due the inherent risk of such testing that could result from un-patched systems, and unique system configurations (i.e., combination of hardware, patch levels, services, third-party software), and other such issues. Thus, we encourage open communications and the establishment of Incident Response procedures in the event of any adverse impact or disruption of network services.

STATEMENT OF WORK

This section details the Scope of Work to be performed under this proposal. The components of this proposal include the following:

- Intrusion Detection Monitoring and Management
- Internal and External Network Vulnerability Scanning

IDS Integration and Tuning

Services Integration

TrustSentry managed security services provide day-to-day operational management of technical security platforms as well as a reporting service for malicious activity and network attacks. While no service provider can stop all attacks, ATW will work with the West Virginia Office of Technology staff to remedy all security problems that are detected.

Incident response is a joint endeavor between the West Virginia Office of Technology and ATW. ATW will work with the West Virginia Office of Technology and its local site administrators to develop specific points of contact for security incident resolution and response. In addition, ATW will work with the West Virginia Office of Technology and its local site administrators to develop integrated escalation procedures and applicable documentation and processes for reporting and responding to security incidents. ATW has a documented set of policies and procedures that it uses internally for day-to-day operations, incident identification and handling. These policies and procedures will be extended where needed to interface with those provided by the West Virginia Office of Technology. ATW will be the focal point for all detected incidents that require immediate action. ATW will bring the appropriate personnel together to work with the West Virginia Office of Technology to perform analysis of security incidents and to develop remedies to security events.

Remedies to security incidents may involve resources that are not managed under the TrustSentry service, such as installing router ACLs, modifying firewall rule sets, or installing system patches. In these cases, ATW will work with the West Virginia Office of Technology and/or its designated contractors to identify a technical or policy solution that the West Virginia Office of Technology's IT staff or management may implement.

Dragon Sensor Tuning

A key phase of any Intrusion Detection System is the tuning of the IDS sensors in order to reduce the occurrence of false positive alarms. This is a function of the location of the sensor, the active services running in the network (e.g., Network Management stations actively pinging hosts), and what services are being protected. Dragon includes customizable signature and alerting capabilities that may be modified to protect specific applications and network components. ATW will work with the client's IT staff to evaluate the sensor output and add, delete, or modify signatures or test settings until a preliminary baseline configuration is installed. ATW will include available virus detection signatures in the State's sensor in order to detect virus activity. This scope of this effort will be fully determined during the Kickoff Meeting. The completion of installation and tuning of the Dragon Sensors will be completed within forty-five (45) days of contract award.

Installation Documentation

ATW will document for the West Virginia Office of Technology the correct procedure to reinstall the Operating System and the required IDS software for each server. Additionally, ATW will provide with this documentation a CD image of the OS and the IDS software.

IDS Management and Monitoring Service Components

The following sections list the components of the managed service, which will be established and ongoing once the initial deployment has been completed.

Change Control Procedures

ATW maintains a change control and configuration management procedure for ATW's support infrastructure and each West Virginia Office of Technology -specific implementation. All changes that could affect the operation of the West Virginia Office of Technology's systems are coordinated with appropriate West Virginia Office of Technology IT staff. IDS change control is managed by establishing a baseline configuration, and then using a documented change request procedure and validation exchange for all future changes.

ATW establishes an email address for each West Virginia Office of Technology contact that is used to support communication with the West Virginia Office of Technology and their service contractors responsible for administration of their networks. ATW reviews network configuration changes and assesses them with respect to their potential impact to the security posture of the enterprise as well as IDS monitoring. ATW also supports planning and decision meetings for significant changes to the West Virginia Office of Technology's network infrastructure.

Recurring Solution Review

ATW performs monthly analysis including reviews of all security events and reports for the previous month and documents them in the West Virginia Office of Technology's Monthly IDS Report. ATW provides senior security engineering support to review technical documents and participate telephonically in the West Virginia Office of Technology technical meetings pertaining to changes in the West Virginia Office of Technology's network architecture that may affect the ability to monitor security events. ATW also has an experienced staff that is available to perform and support both investigative and criminal forensic activity. This staff is available to review event data and assess its applicability to any related West Virginia Office of Technology investigations that may arise. The ongoing review process typically includes the following components:

- Review prior period security events
- Review prior period security and activity reports
- Review expected technical and operational changes that may change security priorities or ability to monitor security events
- Review IDS forensic data and provide investigative support with respect to IDS for the last period

IDS Maintenance

ATW will maintain and update the IDS including both hardware and software. ATW will update the IDS software and signature sets as needed, whenever new software patches or maintenance updates become available. The West Virginia Office of Technology will be notified of the time and date that any maintenance procedures will be performed. ATW will provide at least 24 hours notice to the State prior to performing any maintenance activities.

With respect to signature updates, ATW will evaluate the applicability of new signature sets to the West Virginia Office of Technology environment. When new signatures are released, or when new threats of exploits are brought to ATW's attention by the IS&C point-of-contact, ATW will begin active monitoring of the new threat or exploit within 24 hours of notification.

Notification and Escalation Procedures

As part of this Intrusion Detection service, both ATW and the West Virginia Office of Technology will generally perform and have responsibility for specific tasks following an incident. This section details those proposed responsibilities and duties.

Phase	AmbironTrustWave	West Virginia Office of Technology
Initial Startup	ATW will provide the facilities, equipment and staff to collect IDS events and work closely with the State to establish effective connectivity to enable monitoring of traffic and detection of incidents	The State will work closely with ATW to ensure that all connections required for effective network traffic monitoring are properly established and operational. WV will provide POC listing, and provide call down instructions for various scenarios.
Initial Detection	ATW will provide the facilities, equipment and staff to collect IDS events and perform all necessary work for initial detection of incidents.	Once the IDS is configured, the West Virginia Office of Technology should not need to be involved in the initial Detection of Incidents.
Verification	ATW Tier 2 staff will verify an incident through the use of documented West Virginia Office of Technology network diagrams, Information generated for the West Virginia Office of Technology network in ATW's knowledgebase, and discussion with the West Virginia Office of Technology (or contracted staff) responsible for operating the West Virginia Office of Technology's Network.	The West Virginia Office of Technology (or contracted staff) will occasionally need to be available to ascertain information related to network.
Stabilization and Assessment	ATW will manage the assessment of incidents and will assist the West Virginia Office of Technology's IT staff in any incident response until which time - the network is stabilized and the incident resolved.	The West Virginia Office of Technology will support ATW in the assessment of the incident and will manage any incident response.

Phase	AmbironTrustWave	West Virginia Office of Technology
Documentation	ATW will provide documentation on all incidents and their assessment.	The West Virginia Office of Technology will provide any required documentation on parts of the network beyond the security incident.
Restoration	ATW will provide expertise as requested by the West Virginia Office of Technology and monitor the restoration of the network.	The West Virginia Office of Technology will be responsible for restoring any necessary computers and network configurations.
Testing	ATW will participate and support in any necessary testing.	The West Virginia Office of Technology will coordinate and lead any necessary testing.
Return to Normal Operations	ATW will resume performing normal IDS operations	The West Virginia Office of Technology will resume normal network operations.

Web-Portal Access and Reporting

ATW's Managed IDS solution provides real-time access to the Dragon console, as well as daily and monthly reports. Access to the West Virginia Office of Technology Portal is authenticated and encrypted utilizing a Secure Shell (SSH) 3 DES encrypted connection, as well as limited to IP addresses or network blocks within the West Virginia Office of Technology's infrastructure. Information from the West Virginia Office of Technology is partitioned such that no other parties can access the State's data. The information available via the Web Portal includes:

- Daily Event Summary Reports
- Monthly Event Summary Reports
- Trending Reports over variable time periods
- Event Analysis
- Change Request Submission and Status
- Trouble Ticket Submission and Status
- Real-Time Sensor and System Status (up/down)

In addition, the real-time Dragon console will allow the West Virginia Office of Technology to create tailored reports as required by the IS&C staff.

Real-Time IDS Console

Access to the real-time console is provided to the appropriate West Virginia Office of Technology staff as determined in the SLA. This console provides the West Virginia Office of Technology IT staff the same view of events that is available to the ATW Operations staff. The console information includes inbound and outbound connections, detailed source and destination IP information, as well as access to data content and overall network activity.

Reporting

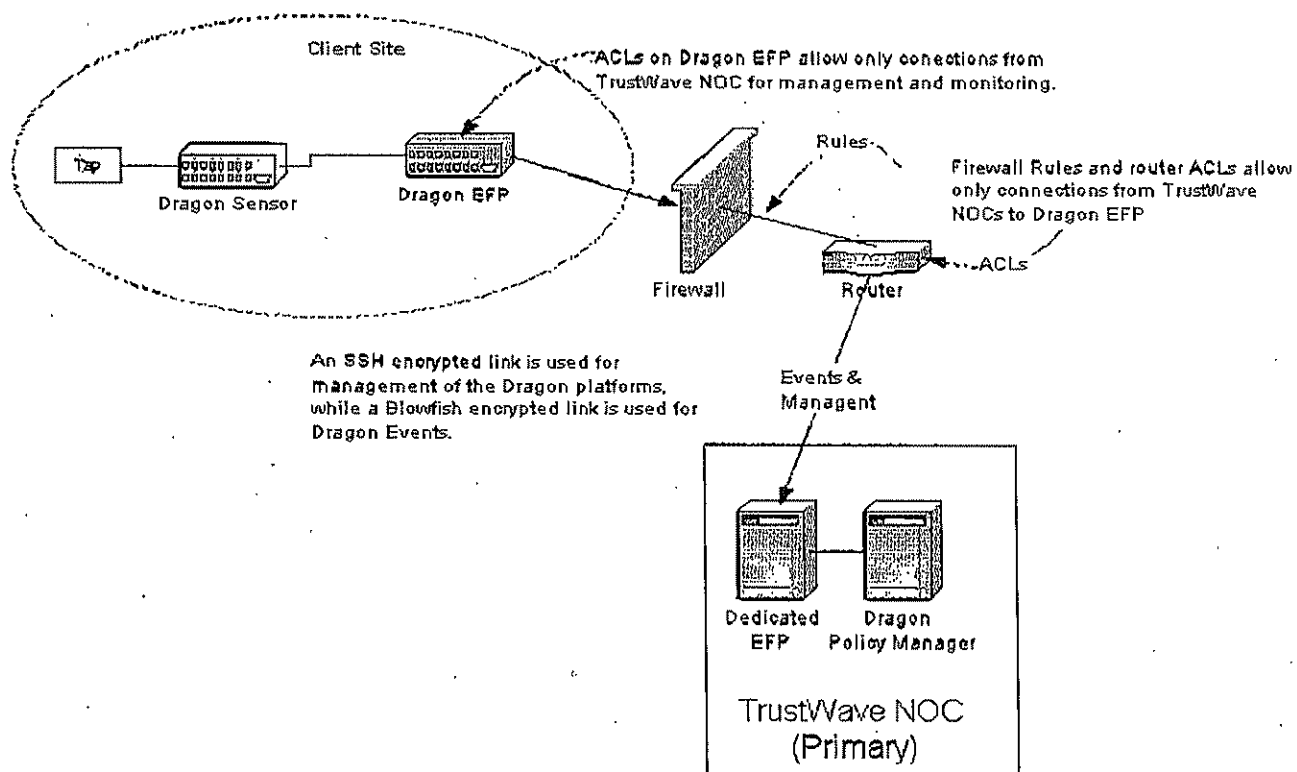
The daily report contains a summary of events, alerts, and incidents for the day. The monthly report includes performance and incident statistics as compiled across the month. These reports are sent to the West Virginia Office of Technology and available on ATW's TrustSentry West Virginia Office of Technology Portal. A sample report is included as an addendum to this proposal; however, the bullets below summarize the report information.

A list of incidents which occurred during the reporting period, including source and destination addresses, service type, and attack classification level and type

- Change request status
- IDS event summaries, trends and statistics
- Customer contact information and changes
- IDS maintenance activities performed during the month
- False positives noted during the reporting period

Event Reporting and Management Architecture

The sensor and server reporting hierarchy is shown in the diagram below. The EFPs at the West Virginia Office of Technology sites receive and aggregate events from Dragon Sensors and then forward them to a dedicated EFP at the ATW Network Operations Centers (NOCs). The ATW EFPs process the events and provide alerting and analysis functions as well.



The West Virginia Office of Technology site has a management architecture as shown in the diagram above. All network sensors are connected to the monitored segments utilizing network interface cards that are configured without IP addresses, which prevent the sensors from being 'seen.' In addition, the monitoring interface of the sensors does not utilize a TCP/IP stack. Sensor will be attached to the network utilizing Shomiti taps, which will further hide the presence network sensors. ATW will assist the State in the installation and configuration of the tap.

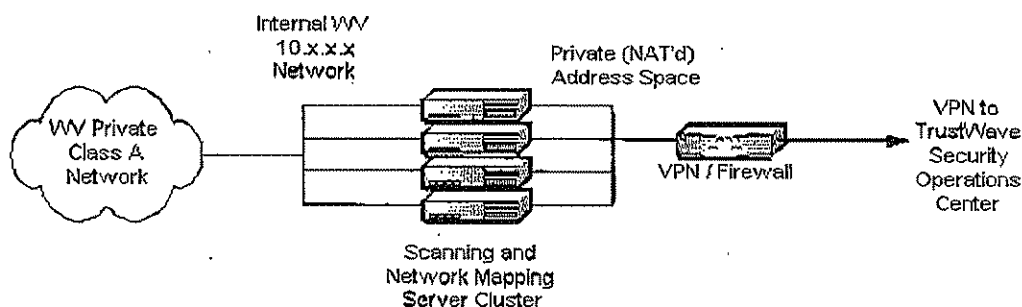
The management interface of the Dragon Sensors is connected via a separate LAN segment to the Dragon Event Flow Processor (EFP). This segment utilizes a private addressing scheme. The 'Public' side of the EFP is connected to the public DMZ segment of the existing West Virginia Office of Technology firewall. The firewall ruleset will be configured to allow only the necessary connections from ATW's NOCs. In addition, Access Control Lists (ACLs) on the Dragon EFP will be set to disallow any connections except those from ATW.

The Dragon EFP and Sensor operating systems will be managed using a Secure Shell (SSH) 3DES encrypted connection, which will be configured to allow only connections from the ATW NOCs. Dragon events will be reported from the local EFP to the NOC EFP using the native Blowfish and/or AES encryption protocols within Dragon.

By utilizing encryption, firewall and VPN rules, operating system level ACLs and application-level ACLs, the management and event reporting links will be protected by multiple layers of security. Depending upon the type of switching equipment in use at the West Virginia Office of Technology site, additional VLAN ACLs can be set to further protect the management interface of the Dragon EFP. These safeguards will ensure that only ATW and the West Virginia Office of Technology can access the sensor network, and that third parties will not be able to see or interact with the West Virginia Office of Technology data or traffic.

Network Vulnerability Scanning

ATW will conduct automated vulnerability scanning of the West Virginia Office of Technology external and internal network address space. This scanning will be conducted using ATW's TrustKeeper scanning tool. The external scans will utilize the TrustKeeper scanning infrastructure at ATW's Security Operations Center (SOC). Scanning of the private address space will require an onsite presence, and because the West Virginia Office of Technology has asked for up to 54 Network scans, ATW proposes utilizing the currently deployed TrustKeeper scanning system at the West Virginia Office of Technology site. This cluster has been configured as shown in the diagram below.



A secure VPN connection via the Internet to ATW's Security Operations Center (SOC) will be used to administer and control the TrustKeeper scanner. The VPN will be set up to connect only with the ATW SOC, and to block any attempts at unauthorized access. In addition, a Secure Shell (SSH) encrypted connection will be tunneled through the VPN in order to provide an additional layer of encryption, authentication, and security.

A secondary connection to the West Virginia Office of Technology private network will allow TrustKeeper to scan the address space quickly and efficiently, and will remove the need for an onsite ATW presence to conduct scans. This will allow ATW to conduct scans on-demand, with a short turnaround time once the scan has been requested by West Virginia Office of Technology personnel.

TrustKeeper Scan Parameters and Connections

A representative from the West Virginia Office of Technology will be asked to provide some limited information regarding the type of network, which may include Internet capabilities, network diagrams, and other pertinent information. This information will allow ATW to understand the West Virginia Office of Technology existing security posture and network. TrustWave will work with the West Virginia Office of Technology to coordinate updating of the onsite equipment, establish points-of-contact and schedule the various phases of this activity.

TrustWave will next conduct a kickoff meeting with the West Virginia Office of Technology IT staff. The kickoff meeting is typically a short, targeted meeting intended to set the overall goals of the engagement and establish a schedule and Points-of-Contact. The product of the kickoff meeting will be a jointly agreed upon project schedule including anticipated scan tasks and a completion timeline.

Once the kickoff meeting has been completed, TrustWave will test the TrustKeeper system, as well as a VPN device to administer and control the system. ATW will conduct security testing of the VPN

connection, as well as operational testing of the TrustKeeper cluster, to ensure the security and functionality of the system.

TrustKeeper Operation

The following paragraphs detail the tools and techniques utilized by ATW's TrustKeeper tool.

Host Mapping

TrustKeeper begins host mapping by conducting broad-stroke reconnaissance of individual hosts on the target network, creating port listings of individual hosts with generic port scanners such as **nmap** and **strobe**. Methods used include such techniques as FIN scanning, SYN-only scans, NULL scans and negative probes. TrustKeeper also utilizes reconnaissance techniques such as pathological IP and TCP fragmentation and one-hop-short port probes. Such tools can distinguish between the responses received from the target hosts and those received from network access control devices such as firewalls. Once the TrustKeeper establishes a rough list of open ports for each host, it conducts TCP fingerprinting to ascertain the operating system of each target, utilizing such tools as **queso** and **nmap** to facilitate these activities.

It is often possible to directly query the target systems for information about their configuration. TrustKeeper will query the **netstat** and **systat** services on target hosts, and retrieve SNMP information with tools such as **snmpwalk** and **AMDSNMP**. TrustKeeper then gathers specific information about servers that support NetBIOS using **qtip** (a homegrown tool that ATW has made available as freeware). TrustKeeper may also obtain information about accounts and active users via **finger**, as well as gather RPC and NFS information with **rpcinfo**, **rpcscan**, and **showmount**.

Vulnerability Identification

Once the reconnaissance phase has been completed, TrustKeeper begins to identify specific vulnerabilities in the network and host configurations as well as custom and commercial application weaknesses. TrustKeeper utilizes a database containing over 3500 vulnerabilities ranging from software bugs to default configuration weaknesses to administrative error. TrustKeeper automated scans search for unlikely or ostentatious vulnerabilities in a rapid fashion. TrustKeeper determines if systems and servers are subject to vulnerabilities that could cause West Virginia Office of Technology Information Systems to be compromised. More than just a network scanner, TrustKeeper also incorporates special technology that allows custom-developed applications to be scanned for a variety of vulnerabilities. TrustKeeper compares potential vulnerability results against an internally maintained vulnerability database whose contents are an amalgamation from public information resources such as Bugtraq, Technotronic and Packetstorm, as well as from less public and more up-to-date resources. The following list is an example of the vulnerability classifications investigated during this phase:

Administrative Error	Application Errors	Authentication mechanism subversion
Insufficient system hardening	Shell escape character insertion in user-supplied data	Intelligent brute-force password cracking
Extraneous services	Batch SQL queries	Replay attacks
Operating System Weaknesses	JavaScript embedded in user-supplied data	Session Hijacking
Insufficient credential checking	Software Bugs	Session ID guessing
Privilege impersonating	Buffer Overflows	Network Layer Weaknesses

Known or blank passwords	Race Conditions	Source address spoofing
Vendor Backdoors	Incomplete or insufficient trust relationship exploitation	Network stream hijacking
Kernel module/driver installation		Overlapped fragmentation reassembly

Reporting

Once the assessment has been completed, TrustKeeper delivers a concise, easy to understand report detailing its findings. Included in this report are the results of the reconnaissance phases, the complete catalog of Internet services listed by server, as well as a complete report of any identified threats, vulnerabilities or potential vulnerabilities. This report includes clear, easy to understand recommendations to help the West Virginia Office of Technology eliminate or mitigate the risks to systems, and provide links to additional materials to help West Virginia Office of Technology better understand the specific vulnerabilities. Wherever possible, the report recommends specific security patches or procedural changes that may be required. Any vulnerability that TrustKeeper uncovers is ranked according to severity: High, Medium, Low, or Informational, to help prioritize which vulnerabilities should be addressed first.

COST PROPOSAL, PREREQUISITES AND CONTACT INFORMATION

Cost Proposal

A detailed cost proposal has been provided as an addendum to this RFQ response. The cost proposal is located within the sealed envelope as requested and includes the following line items:

- Monitoring, Analysis and Reporting**
- Occasional Network Scans:**
 - **Class A Scan (16,777,216 IP Addresses)**
 - **Class B Scan (65,536 IP Addresses)**
 - **Class C Scan (256 IP Addresses)**

Costs are all inclusive of remote services described. No travel or other expenses are anticipated or expected for this engagement.

Prerequisites and Contact Information

This Agreement was developed based on the following dependencies and assumptions, which if not accurate or adhered to, may require a change in the scope of services. Any change in services and fees will be mutually agreed to in writing by both parties. The dependencies and assumptions include:

1. ATW shall not begin to provide the Services as described in this Statement of Work (SOW) until Client has returned this signed SOW and a Purchase Order (PO) for the total amount of the Services selected (full contract amount).
2. Client's Primary Contact (PC), as identified below or their designee must be available to ATW during the entire engagement. The representative must have sufficient authority to schedule testing and address any issues that may arise.
3. Client will provide ATW with sufficient information to evaluate compliance for all project requirements. Client is solely responsible for providing access to and coordinating any required interviews or testing with Client's third parties or service providers.
4. If needed, Client will provide resources and information as requested to enable ATW's consultants to sufficiently develop documentation consistent with the West Virginia Office of Technology Information Security Policy requirements. This will include access to personnel who can provide information related to the business operations, organizational structure, network architecture, security controls, disaster recovery and general daily operational processes and procedures.
5. During testing, the configuration of Client's network will be kept as stable as possible (i.e., no new systems or configuration changes). If changes are required, then Client shall inform ATW, and a mutually acceptable testing schedule shall be agreed upon.

Contact West Virginia Office of Technology

Name: _____

Title: _____

Phone/Fax: _____

E-mail Address: _____

Billing Address: _____

TERMS AND CONDITIONS

1. **IP Addresses, URL and Domain Names.** State of West Virginia represents and warrants that State of West Virginia has full right, power, and authority to consent to have the TrustKeeper service scan for vulnerabilities the IP address and/or URL and/or domain names identified to AmbironTrustWave (ATW) by Client for scanning, whether electronically or by any other means, whether during initial enrollment or thereafter. Without limiting any other remedy that ATW may have, State of West Virginia agrees to indemnify and hold ATW and its affiliates harmless from and against all liabilities, losses, damages, costs and expenses, including without limitation reasonable attorney's fees and costs incurred by ATW resulting from State of West Virginia's breach of this provision. Client acknowledges and understands that accessing and scanning IP addresses and penetration testing involves inherent risks, including, without limitation, risks related to system or network performance and availability, and data corruption or loss.
2. **Applicable Laws and Restrictions.** State of West Virginia's use of the TrustKeeper portal, reports, and scanning solution is subject to the following restrictions: (a) State of West Virginia may use the TrustKeeper services and portal only to scan IP addresses, URLs and domain names owned by and registered to State of West Virginia; (b) the TrustKeeper services, portal and reports may only be used for the stated purposes in this Agreement for State of West Virginia's internal business purposes in accordance with all applicable laws (including any export control laws); and, (c) Client shall limit access to the TrustKeeper portal to only those employees and/or contractors who have executed a written confidentiality agreement with Client and only to those who have a requirement for such access on a "need to know" basis.
3. **Warranty.** ATW warrants to State of West Virginia that all Services shall be performed by employees or contractors of ATW in a professional and workmanlike manner. Each party warrants that (i) it has the full right and power to conduct its business; (ii) that this Agreement has been duly authorized, executed and delivered, and constitutes a valid and binding Agreement in accordance with the terms herein; and (iii) neither the execution or consummation of the services contemplated shall result in the breach or default of any other agreement, charter provision or bylaw, order, law, rule or regulation.
4. **LIMITATION OF LIABILITY AND DISCLAIMER OF WARRANTY.**
 - a. ATW SHALL NOT BE LIABLE TO State of West Virginia FOR (1) ANY ACTS OR OMISSIONS WHICH ARE NOT THE RESULT OF ATW'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, (2) ANY AMOUNTS IN EXCESS OF ANY FEES PAID TO ATW BY CLIENT HEREUNDER, (3) ANY OUTAGES OR SLOW DOWNS OF PERFORMANCE FOOD GROUP'S COMPUTER SYSTEMS RESULTING FROM THE PERFORMANCE OF ANY SERVICES, UNLESS SUCH OUTAGES OR SLOW DOWNS ARE THE RESULT OF ATW'S GROSS NEGLIGENCE, RECKLESSNESS OR WILLFUL MISCONDUCT, OR (4) ANY LOSSES, COSTS, DAMAGES OR EXPENSES INCURRED BY CLIENT RESULTING FROM THE PERFORMANCE OF ANY TEST, UNLESS SUCH ARE THE RESULT OF ATW'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT.
 - b. THIS AGREEMENT IS A SERVICE AGREEMENT, AND EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, ATW DISCLAIMS ALL OTHER REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES REGARDING QUALITY, SUITABILITY, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE (IRRESPECTIVE OF ANY COURSE OF DEALING, CUSTOM OR USAGE OF TRADE) OF ANY SERVICES OR ANY GOODS OR SERVICES PROVIDED INCIDENTAL TO THE SERVICES PROVIDED UNDER THIS AGREEMENT.
 - c. IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY SPECIAL, INDIRECT, EXEMPLARY, INCIDENTAL, OR CONSEQUENTIAL LOSSES OR DAMAGES, INCLUDING LOST PROFITS WHETHER FORESEEABLE OR NOT, WHETHER OCCASIONED BY ANY FAILURE TO PERFORM OR THE BREACH OF ANY REPRESENTATION, WARRANTY, COVENANT OR OTHER OBLIGATION FOR ANY CAUSE WHATSOEVER.
5. **Indemnification.** Each party shall indemnify and hold harmless the other party and its Affiliates and their respective officers, directors, employees, partners, agents, successors and assigns from, and shall defend the other against, any costs, liabilities, damages or expenses (including reasonable attorneys' fees) arising out of or relating to (i) any third party claim that the services, software, or any work performed by either party, or their agents, consultants or contractors under this Agreement infringes the proprietary rights of any third party; (ii) an act or omission by either party and/or their employees and agents relating to any laws or regulations for a protected class or category of persons, and sexual discrimination or harassment; (iii) claims for personal injuries, death or damage to tangible personal or real property to the extent caused by acts or omissions as a result of gross negligence, recklessness or willful misconduct of the party or its Affiliates, contractors or agents; and (iv) claims or suits attributable to breaches of the other party's express representations and warranties contained in the Agreement.
6. **Proprietary Rights.** State of West Virginia acknowledges and agrees that, as between ATW and State of West Virginia, all right, title and interest in and to the TrustKeeper portal and its contents, the TrustKeeper Scanning Solution and any part thereof, including, without limitation, all patents, copyrights, trade secrets and all other intellectual property rights therein and thereto, and all copies thereof, in whatever form, including any written documentation shall at all times be and

remain solely with ATW. State of West Virginia shall not be an owner or licensee of the TrustKeeper portal and related software.

7. **Term.** This Agreement shall be for a term of three years (Initial Term) commencing on the date of execution by both parties, and subject to earlier termination as provided in this Agreement. Following the Initial Term, this Agreement shall automatically renew, with such amendments as to which the parties shall agree, for additional one (1) year periods unless either party provides written notice to the other party, at least ninety (90) days prior to the conclusion of the then-current term, of its intention not to renew.
8. **Termination for Cause.** Either party may terminate this Agreement for Cause (a) upon the expiration of thirty (30) calendar days following detailed written notice to the other party of its material breach of any of its material obligations under this Agreement, provided that the other party has not remedied such breach during the notice period, or (b) immediately upon written notice to the other party if a petition in bankruptcy is filed by or against the other party and is not withdrawn within 60 days or the other party makes an assignment for the benefit of its creditors or an arrangement pursuant to any bankruptcy law, or if the other party discontinues its business or a receiver is appointed for its business.
9. **Effect of Termination; Survival.** If Client terminates this Agreement for any reason, State of West Virginia agrees to pay ATW within 30 days for all services performed by ATW up to the date of cancellation that have not previously been paid for by State of West Virginia. Additionally, if Client terminates this Agreement other than for cause, then State of West Virginia shall pay to ATW, as a cancellation fee and not as a penalty, an amount equal to the sum of the monthly service charges for the remainder of this agreement. The provisions of this section 9, sections 1, 2, 4, 5, 6, 10, 16, 19 and 20 shall survive any expiration or termination of this Agreement.
10. **Confidentiality and Authorized Disclosure.** ATW and State of West Virginia hereby confirm that the provisions of a mutual non-disclosure agreement between ATW and State of West Virginia, if executed, shall be in full force and effect and apply to all information furnished by either party in connection the services. In addition, Client authorizes ATW to release all Client reports to the Client's merchant acquiring bank, if applicable, and the payment card association for reporting PCI compliance.
11. **Dependencies.** Client acknowledges that the provision of services is dependent upon the performance of Client, and its affiliates, and that ATW shall not be liable for its failure to perform to the extent such failure is due to (i) a failure by Client or any third party retained by, or under the control of, Client to provide data or materials that Client or such third party is required to provide to ATW or required by ATW to perform the services under this Agreement, (ii) a failure by Client to timely and accurately perform its responsibilities as set forth in this Agreement, or (iii) a failure by Client to obtain consents, approvals or access for ATW.
12. **Force Majeure.** Neither party shall be liable for any default or delay in the performance of its obligations hereunder (except for payments) if and to the extent such default or delay is caused, directly or indirectly, by acts of God, governmental acts, accidents, wars, terrorism, riots or civil unrest, fires, storms, earthquakes, floods or elements of nature, or any other similar cause beyond the reasonable control of such party, provided such default or delay could not have been prevented by reasonable precautions and cannot reasonably be circumvented by the non-performing party through the use of commercially reasonable alternative sources, workaround plans or other means.
13. **Entire Agreement and Amendments.** This Agreement, together with an executed mutual non-disclosure agreement, if any, constitutes the entire Agreement among the parties pertaining to the subject matter hereof and supersedes all prior and contemporaneous, oral and written, agreements and understandings pertaining thereto. Any amendment to this Agreement must be in writing, mutually agreed upon and duly executed. The waiver or failure of either party to exercise any right provided for in this Agreement shall not be deemed a waiver of any further or future right under this Agreement.
14. **Assignment.** Neither party may assign, delegate nor otherwise transfer the rights or obligations associated with this Agreement, in whole or in part, without the prior written consent of the other party; provided however, no written consent shall be required to assign this Agreement to any parent or the wholly owned subsidiary of the party. Subject to the foregoing, this Agreement will bind and inure to the benefit of the parties, their respective successors and permitted assigns.
15. **Counterparts.** This Agreement may be executed in two or more counterparts, each of which when so executed will be deemed original, and all of which together will constitute one and the same instrument.
16. **Trademarks and Logo.** Client shall not have any rights to use ATW's trademarks, service marks or logos for any other purpose without the prior written approval of ATW's legal department.
17. **Severability.** Any term or provision of this Agreement that is or becomes invalid or unenforceable shall be ineffective to the extent of such invalidity or unenforceability without rendering invalid or unenforceable the remaining terms or provisions of this Agreement.
18. **Governing Law; Consent to Jurisdiction; Venue.** This Agreement shall be governed by and construed in accordance with the laws of the State of Delaware, without giving effect to conflict of law principles. Each party hereto hereby agrees that any proceeding relating to this Agreement and the transactions contemplated hereby shall be brought solely in the

state or federal court located in Delaware. Each party hereto hereby consents to personal jurisdiction in any such action brought in any such state or federal court, consents to service of process by registered mail made upon such party, waives any objection to venue in any such state or federal court and any claim that any such state or federal court is an inconvenient forum.

- 19. **Third-Party Beneficiaries.** Nothing herein expressed or implied is intended to or shall be construed to confer upon or give any person or entity, other than the parties hereto and their respective successors and permitted assigns, any rights or remedies under or by reason of this Agreement.
- 20. **Non-Solicitation.** During the term and for a period of one (1) year thereafter, State of West Virginia shall not, directly or indirectly solicit, hire, attempt to solicit or hire, or participate in any attempt to solicit or hire any person who was an employee of ATW or any of its Affiliates.
- 21. **Notice.** Except as otherwise provided in this Agreement, all notices, consents, or approvals required by this Agreement shall be (i) in writing sent by certified or registered mail, postage prepaid, or by facsimile or electronic mail (confirmed by certified or registered mail) to:

AmbironTrustWave
 c/o TrustWave Holdings, Inc.
 PO Box 4815, Annapolis, MD 21403
 Attention: Legal Department
 Fax: (410) 571-8493

State of West Virginia:

 Fax: _____

or (ii) in any other manner mutually agreed upon by the Parties. Notices shall be deemed effective on the date of mailings.

{SIGNATURE PAGE FOLLOWS}

SIGNATURES

IN WITNESS WHEREOF, the Parties below have executed this agreement as of the date indicated below.

AmbironTrustWave: As a duly elected officer authorized to enter into Agreements and contracts on behalf of AmbironTrustWave, I hereby provide and accept this Agreement for the designated services and term as accepted by Client, as written this day this 22nd day of AUGUST, 2006.

Signature: Joseph L. Patanella

Print Name: JOSEPH L. PATANELLA

Title: PRESIDENT

Effective Date: 8/23/2006

West Virginia Office of Technology: As a duly elected officer authorized to enter into agreements and contracts on behalf of Client, I hereby accept this Agreement for the designated services and term as initialed below, as written this ____ day of _____, 2006.

Signature: _____

Print Name: _____

Title: _____

Date: _____

Ssealed Bid Enclosed

RFQ No. 15C60023
Buyer: Krista Farrell
Bid Opening Date: August 23, 2006
Bid Opening Time: 1:30 PM

Mail To:

|||||
PURCHASING DIVISION
2019 WASHINGTON STREET EAST
P O BOX 50130
CHARLESTON WV 25305-0130

015

West Virginia Office of Technology
Intrusion Detection RFQ ISCG0023

I.

COST PROPOSAL

Provide the cost of the monitoring solution that fully meets the technical specifications contained in this RFQ:

The successful vendor will provide the following support on a 7 x 24 x 365 basis for up to a three year contract duration.

1) Monitoring,
Analyses, Reporting

\$ 17,280⁰⁰ per year * / \$ 1,440 per month*

Occasional Network Scans:

(As described in specification 5 and 6)

Unit Price *

1) Class A scan
(16,777,216 host addresses)

22,000⁰⁰ per scan

2) Class B scan
(65,536 host addresses)

8,000⁰⁰ per scan

3) Class C scan
(~~265~~ host addresses)
256

750⁰⁰ per scan

*Cost must be all inclusive and no separate reimbursement of any travel or other expenses will be paid.

Note: This contract may be cancelled with 30 days notice at the option of the Office of Technology. This provision is required in order to allow the State to implement a more comprehensive IDS/IPS strategy at its discretion, without penalty or breach of contract.