
# *Request for Proposal #648689*

For

# Network Intrusion Protection and Detection System

April 5, 2006

RFP
GENERAL INFORMATION FORM

QUESTIONS: All inquiries for information regarding this solicitation should be directed to: Vicky Moore, VCO, Phone: (540) 231-7953, e-mail: vicky.moore@vt.edu.

DUE DATE: Sealed Proposals will be received until **April 20, 2006 at 3:00 PM**. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

ADDRESS: Proposals should be mailed or hand delivered to: Virginia Polytechnic Institute and State University (Virginia Tech), Information Technology Acquisitions Office (0214), 1700 Pratt Drive, Blacksburg, Virginia 24060-6361. Reference the Opening Date and Hour, and RFP Number in the lower left corner of the return envelope or package.

In compliance with this Request For Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

TYPE OF BUSINESS: (Please check all applicable classifications)

____ **Large**.

____ **Small**. A concern, including its affiliates, which is independently owned and operated, is not dominant in the field of operation in which it is contracting and can further qualify under the criteria concerning number of employees, average annual receipts, or other criteria, as prescribed by the United States Small Business Administration.

____ **Minority-Owned**. A business enterprise that is owned and controlled by one or more socially and economically disadvantaged persons. Such disadvantage may arise from cultural, racial, chronic economic circumstances or background or other similar cause. Such persons include, but are not limited to Blacks, Hispanic Americans, Asian Americans, American Indians, Eskimos, and Aleuts.

____ **Women-Owned**. A business enterprise that is at least 51 percent owned by a woman or women who also control and operate it. In this context, "control" means exercising the power to make policy decisions, and "operate" means being actively involved in the day-to-day management.

COMPANY INFORMATION/SIGNATURE: In compliance with this Request For Proposal and to all the conditions imposed therein and hereby incorporated by reference, the undersigned offers and agrees to furnish the goods and services in accordance with the attached signed proposal and as mutually agreed upon by subsequent negotiation.

<table>
<tr><td colspan="2">FULL LEGAL NAME (PRINT)<br>(Company name as it appears with your Federal Taxpayer Number)</td><td colspan="2">FEDERAL TAXPAYER NUMBER (ID#)</td><td>CONTRACTOR'S REGISTRATION</td></tr>
<tr><td colspan="2">BUSINESS NAME/DBA NAME/TA NAME<br>(If different than the Full Legal Name)</td><td colspan="3">FEDERAL TAXPAYER NUMBER<br>(If different than ID# above)</td></tr>
<tr><td colspan="2">BILLING NAME<br>(Company name as it appears on your invoice)</td><td colspan="3">FEDERAL TAXPAYER NUMBER<br>(If different than ID# above)</td></tr>
<tr><td colspan="2">PURCHASE ORDER ADDRESS</td><td colspan="3">PAYMENT ADDRESS</td></tr>
<tr><td colspan="2">CONTACT NAME/TITLE (PRINT)</td><td colspan="2">SIGNATURE (IN INK)</td><td>DATE</td></tr>
<tr><td>E-MAIL ADDRESS</td><td>TELEPHONE NUMBER</td><td colspan="2">TOLL FREE TELEPHONE NUMBER</td><td>FAX NUMBER</td></tr>
</table>

PURPOSE: The purpose of this Request for Proposal (RFP) is to solicit sealed proposals to establish a contract or contracts through competitive negotiations for a Network Intrusion Prevention/Detection System (NIPDS) for the campus network of Virginia Polytechnic Institute and State University (Virginia Tech), an agency of the Commonwealth of Virginia. This NIPDS is being sought to provide a method of passively detecting, categorizing and preventing network attacks directed against systems in the Virginia Tech network.

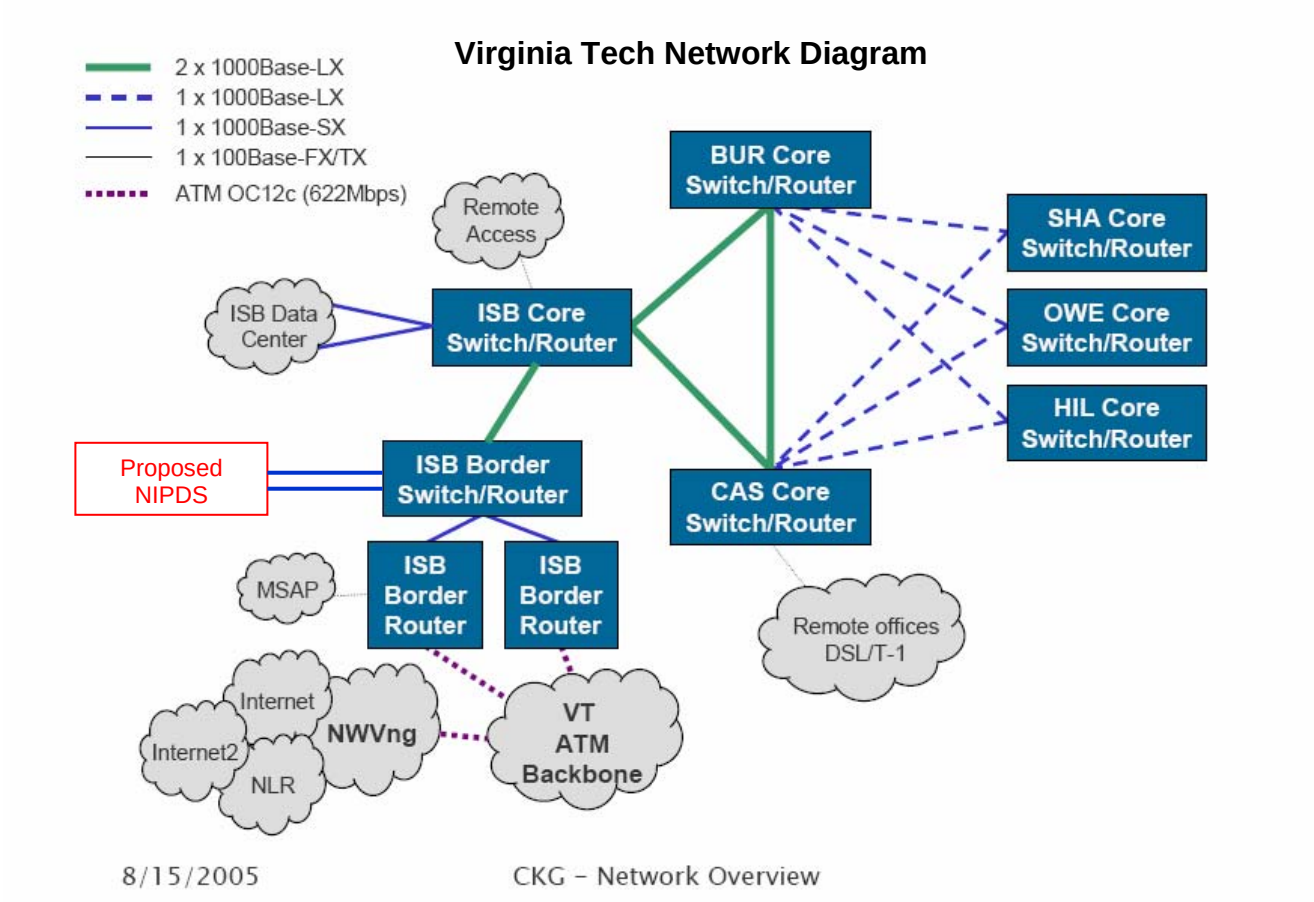
CONTRACT PERIOD: The term of this contract is for two years, or as negotiated. There will be an option for five, one-year renewals, or as negotiated.

I. BACKGROUND: Virginia Tech (VT) is a land-grant institution founded in 1872. It is ranked in the top fifty research universities in the United States, with annual research expenditures of about $170 million. More than 25,000 students pursue 170 degree and post-graduate certificate programs through the University's eight colleges and graduate school. The Virginia Cooperative Extension, operated jointly in the commonwealth by Virginia Tech and Virginia State University, has more than 107 offices and 160 programs. More information about VT can be found at www.vt.edu.

Current Network Environment

VA Tech has been a leader in campus network implementation and management since 1983. Every residence hall room is equipped with 2 Ethernet connections providing full Internet access. Every academic and administrative office and laboratory is connected to the campus network. IP addresses are assigned statically and by using the DHCP protocols. VA Tech's wireless network (WLAN) extends over 98% of the main campus academic and administrative spaces. Wireless access conforms to the IEEE 802/11g standard. Users authenticate to the wireless network in order to connect to the WLAN. VA Tech maintains the network for its remote campus in Northern VA in addition to the main campus in Blacksburg, VA. Some general features about the VA Tech network include:

- 25000 end station network
    - Switched 10Base-T, 100Base-T, 1000Base-T basic Ethernet portal service
    - IPv6 through most of the academic network, 6to4 tunnel available for residence halls
    - Wireless LAN (WLAN) for 98% of campus
        - 802.11 b/g, standard 2.4GHz
        - Blue Socket devices for authenticated access
    - Dial-in modem pool with ~350 56K modems
    - Local network access point provides campus backbone access to local ISPs, Ethernet in local apartment complexes
    - ~13000 telephone, ~5000 cable TV connections on campus
- **Campus core**: 7 core IPv4 routers and 3 core IPv6 routers in partial multi-gigabit Ethernet mesh serving over 250 subnets including approximately 15 remote offices and 8 wireless LAN zones
- **Campus border**: 3 IPv4/v6 routers with 2 ATM OC-12c connections to the Internet and TenGigabit Ethernet services, connected to campus with multi-gigabit Ethernet links. ***NIPDS will be installed at the campus border***.
    - Gigabit Ethernet to Internet2/Abilene
    - Ten Gigabit Ethernet to National Lambda Rail research network




- VA Tech does not have a DMZ network configuration.
    - Only IP routed everywhere
    - No NAT, native IP addresses

## II. CONTRACT PARTICIPATION

Under the authority of the **Code of Virginia 2.2-4304. Cooperative Procurement**, it is the intent of this solicitation and resulting contract(s) to allow for cooperative purchasing by only the Virginia Association of State College and University Purchasing Professionals (VASCUPP) and all other Commonwealth of Virginia public institutions of higher education (to include four-year, two-year and community colleges). Current VASCUPP institutions include: College of William and Mary, University of Virginia, George Mason University, Virginia Military Institute, James Madison University, Old Dominion University, Virginia Tech, Radford University and Virginia Commonwealth University. A list of all other Virginia Public Colleges and Universities is available at http://www.ExploreVirginiaColleges.com/. In addition, the lead-issuing institution may allow local governments, school boards and other agencies serving local governments in their region access to this contract(s).

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor(s), the resultant contract(s) will be extended to the public bodies indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify the lead-issuing institution in writing of any such institutions accessing the contract. No modification of this contract or execution of a separate contract is required to participate. The Contractor will provide semi-annual usage reports for all VASCUPP members and public institutions accessing the Contract. Participating public

bodies shall place their own orders directly with the Contractor(s) and shall fully and independently administer their use of the contract(s) to include contractual disputes, invoicing and payments without direct administration from the lead-issuing institution. The lead-issuing institution shall not be held liable for any costs or damages incurred by any other participating public body as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that the lead-issuing institution is not responsible for the acts or omissions of any VASCUPP member, or public body and will not be considered in default of the Agreement no matter the circumstances.

Use of this contract(s) does not preclude any participating public body from using other contracts or competitive processes as required by law.

III. EVA BUSINESS-TO-GOVERNMENT ELECTRONIC PROCUREMENT SYSTEM:

The eVA Internet electronic procurement solution streamlines and automates government purchasing activities within the Commonwealth of Virginia. Virginia Tech, and other state agencies and institutions, have been directed by the Governor to maximize the use of this system in the procurement of goods and services. We are, therefore, requesting that your firm register as a trading partner within the eVA system.

There are registration fees and transaction fees involved with the use of eVA. These fees must be considered in the provision of quotes, bids and price proposals offered to Virginia Tech. Failure to register within the eVA system may result in the quote, bid or proposal from your firm being rejected and the award made to another vendor who is registered in the eVA system.

Registration in the eVA system is accomplished on-line. Your firm must provide the necessary information. Please visit the eVA website portal at www.eva.state.va.us and complete the Ariba Commerce Services Network registration. *This process needs to be completed before Virginia Tech can issue your firm a Purchase Order or contract.* If your company conducts business from multiple geographic locations, please register these locations in your initial registration.

For registration and technical assistance, reference the eVA website at: http://evaregishelp.dgs.state.va.us, or call 866-289-7367.

IV. STATEMENT OF NEEDS:

Overview

VA Tech has been installing components of its Network Defense-in-Depth strategy since 2003. The installation of a Network Intrusion Detection/Prevention System is the next step in this strategy. The NIPDS will provide a method of passively detecting, categorizing and preventing network attacks against its network infrastructure.

In general, NIPDS have 4 major components: the detection technology used by the system; the intrusion response, reporting and forensic analysis technology; the configuration and management component; and the base unit security measures designed to protect the system itself from attack. The *detection technology* typically describes the method and breadth of attack detection. The ability of the unit to process packets without dropping them or impairing the normal packet flow within the network is another important piece of this component. Accuracy of detection reduces the ability of the unit to provide “false positives” and hopefully, fewer “false negatives”. Good detection technologies allow the user to customize and design new detection filters. The *intrusion response, reporting and forensic technology (IRRFT)* allows the end use to present effective reports detailing specific information about an attack or class of attacks. It allows the end user to measure the types and effectiveness of the NIPDS countermeasures. A good IRRFT also has the ability to do event correlation and analysis. *NIPDS installation, configuration and management* should reflect ease of unit installation coupled with the ability to scale the configuration appropriately. Vendor support and policy, signature and response customization are important components. Finally, *base unit security* describes the ability of the NIPDS to withstand attacks aimed at it. The system’s ability to resist flooding, DoS, malformed packet attacks increase its effectiveness. In addition, it should provide minimal information about the unit itself to an external scanner.

**A. Detection Technology**

**1. REQUIRED (Provide sufficient detail to indicate how your system will meet these minimum requirements)**

a) Must analyze network traffic in real time (line speed)

b) Must provide the ability to selectively block, replace and alert when suspicious activity is detected.
   i) Must do stateful inspection, i.e., tracking connection states
   ii) Must be able to do fragmented IP packet reassembly even if packets are sent out of order or with overlapping fragment offsets
   iii) Must correctly reassemble TCP segments that are sent out of order or with overlapping data.
   iv) System must track which packets belong to which session.

c) Must perform stateful protocol analysis for the most common application protocols. Examples include:
   i) TCP, UDP, ICMP, WWW, DNS, P2P
   ii) Traffic normalization techniques to prevent evasion and insertion techniques
   iii) Protocol decodes
   iv) TCP state verification

d) Must detect the following attacks in real-time to allow automated responses
   i) Must block and log network, application, service-level attacks dynamically
      (1) Examples: worms, Trojan horse, spyware, port scans, DoD, DDoS, server exploits, viruses
   ii) Must be able to detect protocol violations
   iii) Must provide transport layer tools to detect port scans, IP stack fingerprinting, TCP protocol anomaly or evasion attacks
   iv) Must detect spoofing attacks (IP, ICMP, etc.)

e) Must provide alert notification of these events

f) Must be able to detect IPv6 attacks.

**2) ADDITIONAL INFORMATION (Describe how your proposed solution will perform the actions listed in this section)**

a) The four possible IPS states are shown below. Describe how your system handles the 4 states shown in this table.

| | **BLOCK** | **NO BLOCK** |
|---|---|---|
| **ALERT** | ***1.*** | ***2.*** |
| **NO ALERT** | ***3.*** | ***4.*** |

b) Does your system detect all exploits available from products such as Core Impact, Immunity Sec Canvas? Which exploits or attacks generated by these toolkits did your system fail to detect or block?

c) Does your system detect individual exploit code?

d) Is your system able to detect unsolicited traffic (stateless attacks)? If so, how?

e) Does your system detect vulnerability exploitation? If so, how?

f) Describe which exploits or attacks launched from Metasploit v1.0-2.5 are not detected (generated an alert) or blocked by your system. Include which version of Metasploit caused the failure.

g) Describe which attacks generated by the Fragrouter and Toast tools are blocked by your system. Which of these attacks generated an alert?

h) Is your system capable of doing full 7 layer protocol analysis? Please provide an example of this analysis.

i) Does your system perform a combination of heuristic and signature analysis?

j) Does your system allow users to dynamically create their own signatures to add to the signature database?
   i) Does the user have to contact you to have a filter or signature added to your system?
   ii) If so, how long does it take to actually install and activate the filter or signature?

k) Does your system provide kernel level protection, i.e., detecting and stopping malicious system and API calls?

l) Does your system scale to multi-10gigabit Ethernet campus backbone? If so, describe how.

m) Can your system handle the following network traffic levels with peak traffic levels up to three times these values? Describe what network interfaces are needed to meet these levels.
   i) Line rate: 1Gbits/second full duplex
   ii) Flow instantiation rate of 10000 flows/second

**B. Intrusion Response, Reporting and Forensic Technology (IRRFT)**

**1. REQUIRED (Provide sufficient detail to indicate how your system will meet these minimum requirements)**

a) Must provide the following response features
   i) email alerts, pager messages, syslog or eventlog messages
   ii) Real-time alert messages on central IDS monitor console

b) Must provide customizable workflows to view event

c) Must provide in-depth backtracking in realtime or batch more from the central console. Backtrack features must include:
   i) DNS name resolution
   ii) NETBIOS name resolution
   iii) IP addresses
   iv) MAC addresses

d) Must be capable of logging suspicious complete TCP sessions starting with the packet that triggered the alert.

e) Must provide in-depth drill down capabilities. Drill-down information must include:
   i) Source, destination IP addresses
   ii) IP header data including flags and options
   iii) Protocol type (TCP/UDP/ICMP….)
   iv) Numeric source, destination ports or ICMP type/code information
   v) TCP header data including flags, options, sequence numbers
   vi) Protocol decodes as far as possible
   vii) Payload data

f) GUI must provide interactive searching and analysis of data from event databases for forensic analysis. The following search and comparison criteria for data retrieval must be provided:
   i) Time range or exact time of the event
   ii) Event Name
   iii) Source, destination IP addresses
   iv) Protocol (TCP/UDP/ICMP…)
   v) Source, destination ports
   vi) Alert priority

2) **ADDITIONAL INFORMATION (Describe how your proposed solution will perform the actions listed in this section)**

a) Does your system stop attacks automatically using TCP RST or active blocking?

b) Does your system log stateless connections?
   i) Does your system log a predefined number of packets with the same IP src/dst addresses, UDP src/dst ports?

c) Does your system provide the analysts with the ability to interactively block attacks by TCP RST and/or ACL updates?

d) Does your system slow down attacks by manipulation of TCP or IP information? Please provide an example of this.

e) Does your system allow countermeasures to be activated or deactivated on a per-rule basis? Please provide an example of this.

f) Explain how your system's monitoring console GUI allows individual events to be selected and analyzed during periods of high activity.

g) Can your system interface with other infrastructure components such as routers, firewalls, switches? If so, which ones and how do they interface?

h) Do you provide alerts via SNMP traps?

i) Does your system provide file integrity checking tools or an interface for Tripwire or similar tools to ensure the integrity of the NIDPS system files?

j) Does your product provide customizable workflow to view the following event information? Please provide a sample workflow report.
   i) Event type
   ii) Time threshold
   iii) Source and destination IP addresses
   iv) Service ports

k) Please provide examples of printable reports showing all levels of available detail. Report formats can be:
   i) Charts/graphs
   ii) # of attacks vs. type of attacks
   iii) # of attacks vs. priority/severity
   iv) Timestamp vs. # of attacks
   v) Trending analysis reports
      (1) Event names
      (2) Detailed event descriptions
      (3) IP address data
      (4) TCP/UDP port numbers or ICMP type/codes

**C. NIDPS Installation, Configuration and Management**

**1. REQUIRED (Provide sufficient detail to indicate how your system will meet these minimum requirements)**

a) Must have intuitive graphical user interface (GUI) for management of all devices related to the NIPDS

b) Must allow centralized reinstallation, configuration and updating of all NIDPS components

c) Must be able to manage multiple IDS/IPS sensors from a single management console and have the ability to group these sensors into logical entities

d) Must have a set of predefined security policies that can be easily customized by a local administrator

e) Must have a set of predefined alert filters that can be customized by a local administrator

f) Must be possible to define custom signatures and filters
   i) Must allow definition of source and destination IP addresses, address ranges, ports, port ranges
   ii) Must allow definition of protocols, for example, IP, TCP, UDP, ICMP, etc.
   iii) Must allow definition of any combination of IP header, TCP header, ICMP header flags and options.
   iv) Must allow definition of the payload data to be searched in either hex or ascii formats
   v) Must allow definition of the starting point for the payload search (offset) and search depth

g) Must store alerts, header data, payload data in a central event database

**2) ADDITIONAL INFORMATION (Describe how your proposed solution will perform the actions listed in this section)**

a) Does your system have a command line user interface that allows scripting?

b) Does your system have the capability of using an alert filter to exclude certain events from being displayed but still detected? For example, events filtered at one console could be displayed on another console elsewhere. Describe how this capability works.

c) Explain how your system is able to integrate alert data with 3rd party IDS databases such as central syslog server , DShield (www.dshield.org or http://dshield.cirt.vt.edu) and Remedy trouble ticket system

d) Can your system manage all of its components over IPv6?

e) Does your system allow unattended setup of a unit? Does it provide the means to predefine setup and configuration of the device using vendor or customer supplied templates?

f) Does your system allow automated download of signatures and software updates from the vendor via the management GUI? Describe how this process works.

g) Explain how your system allows definition of policy groups or security domains by local administrators.

h) Explain how signature library and policy are distributed on a per host basis. How often does this happen?

i) Is the system capable of supporting multiple management consoles for splitting/grouping tasks between multiple analysts and for redundancy?

j) Does your system support a hierarchical architectural design thereby providing flexible deployment and scalability?

k) What is your system's log archive policy? A log archive policy stores alert data which contains full packet information for a predefined time. This information is reduced for long term storage and analysis. At a minimum the reduced format should contain the following items:
   i) Data and time
   ii) Event name
   iii) Protocol name – IP/TCP/UDP/ICMP…..
   iv) Source and destination IP address and port information
   v) Type codes

l) Does your system's management GUI include tools for database administration and maintenance? If so, what are they?

m) What platforms do you support for your management console/agents? Are the consoles provided as part of the package?

**D. NIPDS Base Unit Security**

**1) REQUIRED (Provide sufficient detail to indicate how your system will meet these minimum requirements)**

a) Communication between IDS components (sensors, middle tier, management console) must be encrypted.

b) Must be stealthy unless configured manually and intentionally and must use at least one of the following techniques
   i) Configure network interface card (NIC) without any IP address
   ii) Disabling TCP/IP for the NIC
   iii) Unbinding the NIC completely from the IP stack

c) Must drop blocked packets silently without letting the attacker know what happened.

d) Must not interfere with transmission of legitimate packets.

e) TCP RST packets must be able to spoof IP addresses, TCP sequence numbers and MAC addresses.

2) **ADDITIONAL REQUIREMENTS (Describe how your proposed solution will perform the actions listed in this section)**

a) Describe the authentication mechanisms used by your system.

b) Explain how your system is not susceptible to attacks generated by the Snort testing tool, "snot".

c) Can your system be configured to fail either open or closed depending on the analyst's selection? Describe how this is done.

d) Does your system provide minimal clues about the system type, version of the IDS code installed via explicit (banner titles) or implicit (unique behavior patterns) when the system itself is scanned? If so, what information does it provide?

e) Does your system block only packets that are identified as part of the attack?

**E. Costs**

Please use the spreadsheet shown in Attachment D to list the costs for all items included in the proposal. Add any additional fields as needed. All proposals must include vendor name, vendor model, system options of all NIPDS equipment proposed by the vendor as a solution.

V. REQUIREMENTS – General

A. Public Inspection - Ownership of all data, material and documentation originated and prepared for Virginia Tech pursuant to this RFP shall belong exclusively to Virginia Tech and be subject to public inspection in accordance with the Virginia Freedom of Information Act. Trade secrets or proprietary information submitted by an Offeror shall not be subject to public disclosure under the Virginia Freedom of Information Act. However, to prevent disclosure the Offeror must invoke the protections of Section 2.2-4342F of the Code of Virginia, in writing, either before or at the time the data or other materials are submitted. The written request must specifically identify the data or other materials to be protected and state the reasons why protection is necessary. The proprietary or trade secret material 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 may result in rejection of the proposal.

VI. PROPOSAL PREPARATION AND SUBMISSION

A. General Requirements:

1. **RFP Response**: In order to be considered for selection, Offerors must submit a complete response to this RFP. 1 **original and** 4 **copies** of each proposal must be submitted to:

Virginia Tech
Information Technology Acquisitions (0214)
1700 Pratt Drive
Blacksburg, VA 24060-6361

**Reference the Opening Date and Hour, and RFP Number in the lower left hand corner of the return envelope or package**.

In addition, please supply an electronic copy of the proposal in a generally used format(s) on CD or DVD media.

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

2. **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 Virginia Tech requiring prompt submission of missing information and/or giving a lowered evaluation of the proposal. Virginia Tech may reject proposals, which are substantially incomplete or lack key information, at its discretion. 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 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 that cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at an appropriate place or be attached at the end of the proposal and designated as additional material. Proposals that are not organized in this manner risk elimination from consideration if the evaluators are unable to find where the RFP requirements are specifically addressed.

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

3. Oral Presentation: Offerors who submit a proposal in response to this RFP may be required to give an oral presentation of their proposal to Virginia Tech. This will provide an opportunity for the Offeror to clarify or elaborate on the proposal but will in no way change the original proposal. Virginia Tech will schedule the time and location of these presentations. Oral presentations are an option of Virginia Tech and may not be conducted. Therefore, proposals should be complete.

B. Specific Requirements: Proposals should be as thorough and sufficiently detailed so that Virginia Tech may properly evaluate your capabilities to provide the required good. Offerors are required to submit the following information/items as a complete proposal:

   1. The return of the General Information Form and addenda, if any, signed and filled out as required.

   2. Offeror Information
      a. Company profile
         (a) Concisely describe the company, including its history, origin, and any affiliation to other corporate entities.
         (b) If the company is currently for sale or involved in any transactions to expand or to be acquired by another organization, please explain.
         (c) Describe the company's involvement with software development organizations and standards organizations.
         (d) Describe the company's strategy for keeping up with industry trends and developments in software development and maintenance.
         (e) Describe the procedure for developing new features, including how customer input is taken, evaluated, and weighed.

      b. Strategic partnerships/test sites - List any partnerships with third-party contractors, including a brief description of the services they provide.

c. Annual reports and financial data - Submit the company's three (3) most recently audited financial statements. Provide the most recent annual report to governing boards or shareholders.

d. Company contacts - Provide a list of your key organizational personnel directly involved in the support of this contract should the contract be awarded to you, with their backgrounds and credentials. Identify the number (by skill set) and location (by skill set) of personnel supporting the contract (should it be awarded to you)

e. Users groups - Provide contact information for users groups, including website or listserv addresses. Provide the URL for any website that provides information on the company, press releases, and product information that is relevant to this proposal.

f. Customers.
   (a) Describe the company's experience in providing and supporting hardware and software.
   (b) Provide a list of at least 5 customers who are currently using your software, hardware and/or services.
   (c) Provide the names and contact information of any customers who have switched to another vendor and or product within the last three years.

3. Responses to the requirements as noted in Section IX formatted as noted above in Paragraph VI.A.2.

4. Any other supporting information as noted in Paragraph VI.A.2.c.

5. Any proposed exceptions to the RFP terms and conditions.

## VII. SELECTION CRITERIA AND AWARD

A. Selection Criteria: Proposals will be evaluated by Virginia Tech using the following:

1. Detection technology used by the system
2. Intrusion Response, Reporting and forensic analysis
3. Installation, configuration and management of NIPDS
4. Unit Security
5. Vendor Qualifications, Experience and Financial Stability
6. Cost

B. Award: 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 Proposal, including price, if so stated in the Request for Proposal. 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, Virginia Tech shall select the offeror who, in its opinion, has made the best proposal, and shall award the contract to that offeror. Virginia Tech may cancel this Request for Proposal or reject proposals at any time prior to an award, and is not required to furnish a statement of the reason why a particular proposal was not deemed to be the most advantageous. (Section 2.2-4359(D.), Code of Virginia.) Should Virginia Tech 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 this solicitation and the Contractor's proposal as negotiated. See Attachment C for sample contract form.

OPTIONAL PRE-PROPOSAL CONFERENCE: No pre-proposal conference will be held due to the quick turnaround of this RFP however we suggest that you read through this RFP and submit your questions to nipds-rfp@vt.edu. All questions and answers will be posted on our website: http://ccpurch.vt.edu/NIPDS-RFP. Questions will be accepted through **Thursday, April 13, 2006 at 5:00 p.m.**

## VIII. CONTRACT ADMINISTRATION

A. Randy Marchany, Director of the Information Technology Security Lab at Virginia Tech or his designee, shall be identified as the Contract Administrator and shall use all powers under the contract to enforce its faithful performance.

B. The Contract Administrator, or his/her designee, shall determine the amount, quantity, acceptability, fitness of all aspects of the services and shall decide all other questions in connection with the services. The Contract Administrator, or his/her designee, shall not have authority to approve changes in the services which alter the concept or which call for an extension of time for this contract. Any modifications made must be authorized by the Virginia Tech Information Technology Acquisitions Office through a written amendment to the contract.

## IX. ATTACHMENTS:

Attachment A- Special Terms and Conditions
Attachment B- General Terms and Conditions
Attachment C - Standard Contract Form
Attachment D – Proposal Pricing Spreadsheet

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

2. CANCELLATION OF CONTRACT: Virginia Tech 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, either party, without penalty, may terminate the resulting contract 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.

3. CONTRACT DOCUMENTS: The contract entered into by the parties shall consist of the Request for Proposal including all modifications thereof, the proposal submitted by the Contractor, the written results of negotiations, the Commonwealth Standard Contract Form, all of which shall be referred to collectively as the Contract Documents.

4. DELIVERY POINT: Except when otherwise specified herein, all items shall be F.O.B. delivered any point within the Commonwealth of Virginia as directed by ordering department, institution or agency of the Commonwealth or Public bodies of the Commonwealth as defined in Section 2.2-4301 of the Virginia Public Procurement Act.

5. IDENTIFICATION OF PROPOSAL ENVELOPE: If a special envelope is not furnished, or if return in the special envelope is not possible, the signed proposal should be returned in a separate envelope or package, sealed and addressed as follows:

   VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
   Information Technology Acquisitions (0214)
   1700 Pratt Drive
   Blacksburg, VA 24060-6361

   Reference the opening date and hour, and RFP Number in the lower left corner of the envelope or package. If a proposal not contained in the special envelope is mailed, the Offeror takes the risk that the envelope, even if marked as described above, may be inadvertently opened and the information compromised which may cause the proposal to be disqualified. No other correspondence or other proposals should be placed in the envelope. Proposals may be hand delivered to the Virginia Tech Information Technology Acquisitions Office.

6. INDEPENDENT CONTRACTOR: The contractor shall not be an employee of Virginia Tech, but shall be an independent contractor. Nothing in this agreement shall be construed as authority for the contractor to make commitments, which shall bind Virginia Tech or to otherwise act on behalf of Virginia Tech, except as Virginia Tech may expressly authorize in writing.

7. INSURANCE: By signing and submitting a proposal under this solicitation, the Offeror certifies that if awarded the contract, it will have the following insurance coverages at the time the work commences. Additionally, it will maintain these during the entire term of the contract and that all insurance coverages will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission. During the period of the contract, Virginia Tech reserves the right to require the Contractor to furnish certificates of insurance for the coverage required.

   INSURANCE COVERAGES AND LIMITS REQUIRED:
   A. Worker's Compensation - Statutory requirements and benefits.
   B. Employers Liability - $100,000.00
   C. General Liability - $500,000.00 combined single limit. Virginia Tech and the Commonwealth of Virginia shall be named as an additional insured with respect to goods/services being procured. This coverage is to include Premises/Operations Liability, Products and Completed Operations Coverage, Independent Contractor's Liability, Owner's and Contractor's Protective Liability and Personal Injury Liability.
   D. Automobile Liability - $500,000.00

E. Builders Risk – For all renovation and new construction projects under $100,000 Virginia Tech will provide All Risk – Builders Risk Insurance. For all renovation contracts, and new construction from $100,000 up to $500,000 the contractor will be required to provide All Risk – Builders Risk Insurance in the amount of the contract and name Virginia Tech as additional insured. All insurance verifications of insurance will be through a valid insurance certificate.

The contractor agrees to be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from the payment of all sums of money by reason of any claim against them arising out of any and all occurrences resulting in bodily or mental injury or property damage that may happen to occur in connection with and during the performance of the contract, including but not limited to claims under the Worker's Compensation Act. The contractor agrees that it will, at all times, after the completion of the work, be responsible for, indemnify, defend and hold harmless Virginia Tech, its officers, agents and employees from all liabilities resulting from bodily or mental injury or property damage directly or indirectly arising out of the performance or nonperformance of the contract.

8. MINORITY BUSINESS, WOMEN-OWNED BUSINESSES SUBCONTRACTING AND REPORTING: Where it is practicable for any portion of the awarded contract to be subcontracted to other suppliers, the contractor is encouraged to offer such business to minority and/or women-owned businesses. Names of firms may be available from the buyer and/or from the Division of Purchases and Supply. When such business has been subcontracted to these firms and upon completion of the contract, the contractor agrees to furnish the purchasing office the following information: name of firm, phone number, total dollar amount subcontracted and type of product/service provided.

9. 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 a equivalence is not available. Installation of hardware, software, or peripheral devices used for nonvisual access is not required when the Technology is being used exclusively by individuals who are not blind or visually impaired, but applications programs and underlying operating systems (including the format of the data) used for the manipulation and presentation of information shall permit the installation and effective use of nonvisual access software and peripheral devices. If requested, the Contractor must provide a detailed explanation of how compliance with the foregoing nonvisual access standards is achieved and a validation of concept demonstration. The requirements of this Paragraph shall be construed to achieve full compliance with the Information Technology Access Act, §§2.1-807 through 2.1-811 of the Code of Virginia.

10. PROPOSAL ACCEPTANCE PERIOD: Any proposal received in response to this solicitation shall be valid for 120 days. At the end of the 120 days the proposal may be withdrawn at the written request of the Offeror. If the proposal is not withdrawn at that time it remains in effect until an award is made or the solicitation is cancelled.

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

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

13. QUANTITIES: Quantities set forth in this solicitation are estimates only, and the Contractor shall supply at proposal prices actual quantities as ordered, regardless of whether such total quantities are more or less than those shown.

14. RENEWAL OF CONTRACT: This contract may be renewed by Virginia Tech upon written agreement of both parties for up to five successive one year periods only under the terms and conditions of the original contract except as stated in A and B below. Price increases may be negotiated only at the time of renewal. Written notice of Virginia Tech's intention to renew shall be given (approximately 90 days) prior to the expiration date of each contract period.
    A. If Virginia Tech elects to exercise the option to renew the contract for an additional one-year period, the contract price(s) for the additional year shall not exceed the contract prices 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.
    B. If during any subsequent renewal period Virginia Tech 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 for the Consumer Price Index of the United States Bureau of Labor Statistics for the latest twelve months for which statistics are available.

15. SEVERAL LIABILITY: Virginia Tech will be severally liable to the extent of its purchases made against any contract resulting from this solicitation. Applicable departments, institutions, agencies and Public Bodies of the Commonwealth of Virginia will be severally liable to the extent of their purchases made against any contract resulting from this solicitation.

16. WORK SITE DAMAGES: Any damage to existing utilities, equipment or finished surfaces resulting from the performance of this contract shall be repaired to the Owner's satisfaction at the Contractor's expense.

17. COMMUNICATIONS: Communications regarding this Request for Proposals (RFP) shall be formal from the date of issue for this RFP, until either a Contractor has been selected or the Information Technology Acquisitions Office rejects all proposals. Formal communications will be directed to the Information Technology Acquisitions Office. Informal communications including but not limited to, request for information, comments or speculations regarding this RFP to any University employee other than an Information Technology Acquisitions Office representative may result in the offending Offeror’s proposal being rejected.

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

19. ADVERTISING: In the event a contract is awarded for supplies, equipment, or services resulting from this solicitation, no indication of such sales or services to Virginia Tech will be used in product literature or advertising without the prior written consent of Virginia Tech. The Contractor shall not state in any of the advertising or product literature that the Commonwealth of Virginia or any agency or institution of the Commonwealth has purchased or uses its products or services.

20. CERTIFICATION TESTING AND ACCEPTANCE: The system specified in the contract shall be considered ready for production testing upon receipt of documentation from the Contractor that a successful system audit or diagnostic test was performed at the site demonstrating that the system meets the minimum design/performance capabilities stipulated by the contract. The system shall be deemed ready for production certification testing on the day following receipt of this documentation. Virginia Tech shall provide written confirmation of its acceptance following successful completion of the production certification test. System (software and/or hardware) payment will be authorized after the successful completion and certification test(s).

21. NOTICES: Any notices to be given by either party to the other pursuant to any contract resulting from this solicitation shall be in writing, hand delivered or mailed to the address of the respective party at the following address

If to Contractor: Address Shown On RFP Cover Page
Attention: Name of Person Signing RFP

If to Virginia Tech:

Virginia Polytechnic Institute and State University
Attn: John D. Krallman
Information Technology Acquisitions (0214)
1700 Pratt Dr,
Blacksburg, VA 24061

RFP GENERAL TERMS AND CONDITIONS

See http://www.purch.vt.edu/html.docs/terms/gtc_rfp_030906.pdf

**ATTACHMENT C**

**Standard Contract form for reference only**
**Offerors do not need to fill in this form**

COMMONWEALTH OF VIRGINIA
STANDARD CONTRACT

Contract Number:_____

This contract entered into this ____ day of _____ 20___, by _____, hereinafter called the "Contractor" and Commonwealth of Virginia, Virginia Polytechnic Institute and State University called "Virginia Tech".

WITNESSETH that the Contractor and Virginia Tech, in consideration of the mutual covenants, promises and agreements herein contained, agrees as follows:

SCOPE OF CONTRACT: The Contractor shall provide the Library Management System to Virginia Tech as set forth in the Contract Documents.

PERIOD OF CONTRACT: From _____ through _____.

COMPENSATION AND METHOD OF PAYMENT: The Contractor shall be paid in accordance with the contract documents.

CONTRACT DOCUMENT: The contract documents shall consist of this signed contract, Request For Proposal Number 501757 dated February 22, 2006, together with all written modifications thereof and the proposal submitted by the Contractor dated _____ and the Contractor's letter dated _____, all of which contract documents are incorporated herein.

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

| Contractor: | Virginia Tech |
|---|---|
| By:_____ | By: _____ |
| Title:_____ | |

Vendor: _____
Date:_____

# Attachment D
# Hardware Costs

## Initial Hardware Costs

**NIDPS Detection Units (itemize all peripherals and cables)**

| Manufacturer | Product Code | Item Description | List Unit Price | VT Net Unit Price | Quantity | Total | Explanatory Comments |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**NIDPS Management Units (itemize all peripherals and cables)**

| Manufacturer | Product Code | Item Description | List Unit Price | VT Net Unit Price | Quantity | Total | Explanatory Comments |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Other Hardware (describe purpose under explanatory comments)**

| Manufacturer | Product Code | Item Description | List Unit Price | VT Net Unit Price | Quantity | Total | Explanatory Comments |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Shipping**

| List Unit Price | VT Net Unit Price | Quantity | Total | Explanatory Comments |
|---|---|---|---|---|
| | | | | |
| | | | | |

**Test Database (List cost of a full-sized test instance of your system)**

| Manufacturer | Product Code | Item Description | List Unit Price | VT Net Unit Price | Quantity | Total | Explanatory Comments |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

Note: Add additional rows and explanatory comments as needed
Provide additional detail at the bottom as necessary to explain your pricing, including any discounts.

Vendor: _____
Date:_____

# Attachment D
# Hardware Costs

## Hardware Maintenance Costs

### NIDPS Detection Units

| Manufacturer | Product Code | Item Description | Maintenance | | | Explanatory Comments |
|---|---|---|---|---|---|---|
| | | | 1st year | 2nd year | Optional 1-5 year | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

### NIDPS Management Units

| Manufacturer | Product Code | Item Description | Maintenance | | | Explanatory Comments |
|---|---|---|---|---|---|---|
| | | | 1st year | 2nd year | Optional 1-5 year | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

### Other Hardware

| Manufacturer | Product Code | Item Description | Maintenance | | | Explanatory Comments |
|---|---|---|---|---|---|---|
| | | | 1st year | 2nd year | Optional 1-5 year | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

### Test Database

| Manufacturer | Product Code | Item Description | Maintenance | | | Explanatory Comments |
|---|---|---|---|---|---|---|
| | | | 1st year | 2nd year | Optional 1-5 year | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

Vendor: _____
Date: _____

# Attachment D
# Software Costs

**NIDPS System Software (include signature & software updates)**

| Manufacturer | Product Code | Item Description | List Unit Costs | VT Net Unit Price | # of Single Licenses | # of Concurrent Licenses | Total | Maintenance 1st year | Maintenance 2nd year | Maintenance Optional 1-5 year | Explanatory Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

**NIDPS Application Software (include signature & software updates)**

**List each Module and options that can be priced separately.**
**Also list any discounts for comprehensive purchases with components included.**

| | Manufacturer | Product Code | Item Description | List Unit Costs | VT Net Unit Price | # of Single Licenses | # of Concurrent Licenses | Total | Maintenance 1st year | Maintenance 2nd year | Maintenance Optional 1-5 year | Explanatory Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Module A** | | | | | | | | | | | | |
| **Module B** | | | | | | | | | | | | |
| **etc.** | | | | | | | | | | | | |
| | | | | | | | | | | | | |

**Required Third Party Software (itemize)**

| Manufacturer | Product Code | Item Description | List Unit Costs | VT Net Unit Price | # of Single Licenses | # of Concurrent Licenses | Total | Maintenance 1st year | Maintenance 2nd year | Maintenance Optional 1-5 year | Explanatory Comments |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

Vendor: _____
Date: _____

# Attachment D
# Software Costs

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | |

**Suggested Third Party Software (itemize)**

| | | | | | | | | Maintenance | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Manufacturer** | **Product Code** | **Item Description** | **List Unit Costs** | **VT Net Unit Price** | **# of Single Licenses** | **# of Concurrent Licenses** | **Total** | **1st year** | **2nd year** | **Optional 1-5 year** | **Explanatory Comments** |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |

Note: Add additional rows and explanatory comments as needed
Provide additional detail at the bottom as necessary to explain your pricing, including any discounts.

Vendor: _____
Date: _____

# Attachment D
# Services Costs

**Customization**

**(List expected customizations based on information presented in the RFP and experience with installations of similar size and complexity)**

| Hourly Rate | Expected Number of Hours | Total | Explanatory Comments |
|---|---|---|---|
| | | | |
| | | | |

**System Installation (List basic services provided and optional assistance available)**

| Hourly Rate | Expected Number of Hours | Total | Explanatory Comments |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Maintenance (Provide maintenance costs based on 24/7 coverage. Separately list any optional add ons or enhancements.)**

| Hourly Rate | Expected Number of Hours | Total | Explanatory Comments |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Training (List training packages)**

| Hourly Rate | Expected Number of Hours | Total | Explanatory Comments |
|---|---|---|---|
| | | | |
| | | | |
| | | | |

**Documentation**

Note: Add additional rows and explanatory comments as needed
Provide additional detail at the bottom as necessary to explain your pricing, including any discounts.