Request for Proposal #0016531

for

Video Surveillance System and Associated Components

February 28, 2011

RFP 0016531
GENERAL INFORMATION FORM

1. QUESTIONS: All inquiries for information regarding this solicitation should be directed to: John Krallman, Phone: (540) 231-6233, e-mail: john.krallman@vt.edu.

2. DUE DATE: Sealed Proposals will be received until **March 31, 2011 at 3:00 PM**. Failure to submit proposals to the correct location by the designated date and hour will result in disqualification.

3. ADDRESS: Proposals should be mailed or hand delivered to: Virginia Polytechnic Institute and State University (Virginia Tech), Information Technology Acquisitions, 1700 Pratt Drive (0214), Blacksburg, Virginia 24061. Reference the Opening Date and Hour, and RFP Number in the lower left corner of the return envelope or package.

4. **PRE-PROPOSAL CONFERENCE**: See Section IX for information regarding a pre-proposal conference.

5. TYPE OF BUSINESS: (Please check all applicable classifications). If your classification is certified by the Virginia Department of Minority Business Enterprise, provide your certification number: _____. For certification assistance, please visit: http:/www.dmbe.state.va.us/swamcert.html.

____ **Large**

____ **Small business** – An independently owned and operated business which, together with affiliates, has 250 or fewer employees or average annual gross receipts of $10 million or less averaged over the previous three years. Department of Minority Business Enterprise (DMBE) certified women-owned and minority-owned business shall also be considered small business when they have received DMBE small business certification.

____ **Women-owned business** – A business concern that is at least 51% owned by one or more women who are U. S. citizens or legal resident aliens, or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest is owned by one or more women who are citizens of the United States or non-citizens who are in full compliance with the United States immigration law, and both the management and daily business operations are controlled by one or more women who are U. S. citizens or legal resident aliens.

____ **Minority-owned business** – A business concern that is at least 51% owned by one or more minority individuals (see Section 2.2-1401, Code of Virginia) or in the case of a corporation, partnership, or limited liability company or other entity, at least 51% of the equity ownership interest in the corporation, partnership, or limited liability company or other entity is owned by one or more minority individuals and both the management and daily business operations are controlled by one or more minority individuals.

6. 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 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)
(Company name as it appears with your Federal Taxpayer Number)</td><td colspan="2">FEDERAL TAXPAYER NUMBER (ID#)</td></tr>
<tr><td colspan="2">BUSINESS NAME/DBA NAME/TA NAME
(If different than the Full Legal Name)</td><td colspan="2">FEDERAL TAXPAYER NUMBER
(If different than ID# above)</td></tr>
<tr><td colspan="2">BILLING NAME
(Company name as it appears on your invoice)</td><td colspan="2">FEDERAL TAXPAYER NUMBER
(If different than ID# above)</td></tr>
<tr><td colspan="2">PURCHASE ORDER ADDRESS</td><td colspan="2">PAYMENT ADDRESS</td></tr>
<tr><td colspan="2">CONTACT NAME/TITLE (PRINT)</td><td>SIGNATURE (IN INK)</td><td>DATE</td></tr>
<tr><td>E-MAIL ADDRESS</td><td>TELEPHONE NUMBER</td><td>TOLL FREE TELEPHONE NUMBER</td><td>FAX NUMBER TO RECEIVE E-PROCUREMENT ORDERS</td></tr>
</table>

09/10

I. PURPOSE:

The purpose of this Request for Proposal (RFP) is to solicit sealed proposals to establish a contract or contracts through competitive negotiations for an enterprise-wide Internet Protocol-based Video Surveillance System and associated Components to assist in implementing University Policy 5617 related to Safety and Security Camera Acceptable Use Policy (See Attachment D) by Virginia Polytechnic Institute and State University (Virginia Tech), an agency of the Commonwealth of Virginia.

II. CONTRACT PERIOD:

The term of this contract or contracts is for three year(s), or as negotiated. There will be an option for five, one year renewals, or as negotiated.

III. BACKGROUND:

A. University Overview

Founded in 1872 as a land-grant college, Virginia Tech (www.vt.edu) is the most comprehensive university in the Commonwealth of Virginia and is among the top research universities in the nation. Virginia Tech's nine colleges are dedicated to quality, innovation, and results through teaching, research, and outreach activities. At its 2,600 acre main campus located in Blacksburg and other campus centers in Northern Virginia, Southwest Virginia, Hampton Roads, Richmond, Southside, and Roanoke, Virginia Tech enrolls more than 28,000 undergraduate and graduate students from all 50 states and more than 100 countries in 180 academic degree programs.

B. Critical Timeliness of Contract(s) Completion

Several projects, critical to university interests are dependent on the completion of contract(s) resulting from this RFP. It is Virginia Tech's intention to award contract(s) resulting from this RFP by April 18, 2011. As a result of this expedited review process, we would ask any offerors to this RFP to be prepared to answer clarification and follow-up questions and be available to provide demonstrations of parts or all of their solutions within 24 hours of request after the closing date of this RFP, in person or on-line.

C. Network Infrastructure

Virginia Tech has an Ethernet-based, Internet Protocol (IP) network system that supports the main campus in Blacksburg. The backbone of the network provides a foundation for Ethernet (802.3) and Wireless (802.11) access through core and, as applicable, distribution switching components capable of supporting a multitude of applications and corresponding service levels. IP Version 4 (IPv4) and IP Version 6 (IPv6) are fully supported in each of the core and distribution components that make up the system foundation. The backbone will support link speeds ranging from 1 Gbps to Nx10 Gbps, with future capabilities for 40 Gbps and 100 Gbps links.

Core and distribution switching components and interconnecting links will be at least 1+1 redundant throughout the backbone and supported by uninterruptible power.

Ethernet access is provided using several generations of Cisco-brand, Ethernet switches, ranging from the Cisco Catalyst 3500 XL to the Cisco Catalyst 3750. Ethernet access switches will utilize 1+1 redundant links to the backbone. Power over Ethernet (PoE) is provided, where needed, using Cisco Catalyst 3750 switches.

Several off-campus locations in the Town of Blacksburg (i.e., leased properties) are integrated into the campus network using either Virginia Tech-provided Single-Pair High-Speed Digital Subscriber Lines (SHDSL) or leased Digital Signal 1 (DS1) facilities.

Internet access is provided to the campus using a pair of Cisco 7600 series routers located adjacent to the primary data center. These routers interconnect the campus with commodity Internet and research networks (e.g., Internet2, National LambdaRail) via leased services and/or leased fiber at speeds ranging from 1 Gbps to 10 Gbps.

IP routing throughout the campus utilizes the Open Shortest Path First (OSPF) protocol. IPv4 and IPv6 are fully supported for production applications on the campus network. At the campus border, Border Gateway Protocol (BGP) is used to provide wide-area IP routing.

D. Current Safety and Security Camera Environment

Virginia Tech currently has approximately 250 cameras in operation managed by 21 separate departments. Most are digital although several are analog or still frame capture. Most capture and store video and maintain storage for varying periods. We have a mix of continuous feed and motion capture cameras with most being stationary, but some remotely controllable. New uses will include monitoring of outdoor areas where people congregate and parking areas. Approximately ten additional locations have been identified for priority camera expansion. Total cameras eventually under management could approach 2500 units.

IV. 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 http://www.eva.virginia.gov/register/vendorreg.htm and **register both with eVA and Ariba**. *This process needs to be completed before Virginia Tech can issue your firm a Purchase Order or contract.* If your firm conducts business from multiple geographic locations, please register these locations in your initial registration.

For registration and technical assistance, reference the eVA website at: eVACustomerCare@dgs.virginia.gov, or call 866-289-7367 or 804-371-2525.

V. CONTRACT PARTICIPATION:

It is the intent of this solicitation and resulting contract to allow for cooperative procurement. Accordingly, any public body, public or private health or educational institutions, or Virginia Tech's affiliated corporations and/or partnerships may access any resulting contract if authorized by the contractor.

Participation in this cooperative procurement is strictly voluntary. If authorized by the Contractor, the resultant contract may be extended to the entities indicated above to purchase at contract prices in accordance with contract terms. The Contractor shall notify Virginia Tech in writing of any such entities 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 entities accessing the Contract. Participating entities shall place their own orders directly with the Contractor and shall fully and independently administer their use of the contract to include contractual disputes, invoicing and payments without direct administration from Virginia Tech. Virginia Tech shall not be held liable for any costs or damages incurred by any other participating entity as a result of any authorization by the Contractor to extend the contract. It is understood and agreed that Virginia Tech is not responsible for the acts or omissions of any entity, and will not be considered in default of the contract no matter the circumstances.

Use of this contract does not preclude any participating entity from using other contracts or competitive processes as the need may be.

VI. STATEMENT OF NEEDS:

A. Network Capabilities

1. The proposed system must communicate with existing Virginia Tech networks as described in Section III B. Network Infrastructure above.
2. Describe the capabilities of the proposed solution to provide power over Ethernet.
3. Describe the capabilities of the system to support IP and IPv6 including:
   a. DHCP for IP configuration
   b. Stateless address autoconfiguration (SLAAC) or static configuration for IPv6
   c. DHCP/Stateless DHCP for IPv6
   d. The ability to operate on an IPv6-only network
4. Describe the capabilities of the system to provide packet filtering for IP and IPv6.
5. Describe the extent to which your proposal could make use of the university-provided 802.11 wireless infrastructure for network connectivity, including 802.1x authentication.
6. Describe how Virginia Tech system administrators will access any and all system components.
7. Describe how the proposed solution will enable stored or real-time video to be sent to a network database or viewed remotely on a secure personal computer.
8. Describe how the proposed solution will be able to store surveillance records from multiple locations for 30 days, and then erase or write over data older than 30 days utilizing a central storage repository.
9. Describe how the proposed system implements a “litigation” or “investigative” hold on selected video footage for an indefinite period of time.
10. Describe the features and capabilities of the proposed solution that will allow it to interface with existing access control and fire alarms via an open Application Programming Interface (API) and Software Development Kit (SDK).
11. Describe how the proposed solution will prevent data loss or the interruption of data collection should one of the storage nodes fail
12. The proposed system should be capable of daily backup. The backup should consist of two copies, one copy of which Virginia Tech will store offsite. System recovery procedures shall be well documented and kept up-to-date in order to allow Virginia Tech to test, ensure the system is functional, and that applications and data can be restored from backups.
13. Describe how the proposed system will provide redundancy in server and storage components.

B. Security Capabilities

1. Describe the security features and capabilities of the proposed solution.
2. Complete and attach the Virginia Tech Information Technology Security Office’s technology procurement questionnaire (Attachment C).
3. Describe how the proposed system will provide HTTPS for system configuration, SSL client authentication and support user installation of the server certificate chain.
4. Indicate whether the proposed solution is capable of encrypting all control and image transfer with either SSL or SSH and describe how.
5. Describe how control and image transfer will be encrypted.
6. Describe how the proposed system will provide access control, including different access levels and / or accounts for routine image fetching and administrative access.
7. Describe how the system manages and supports multiple users simultaneously accessing the same data, including access to live camera data from multiple disparate locations.
8. Describe how the system will authenticate surveillance records as original.
9. Describe the features and capabilities of the proposed system that will enable remote access via the Virginia Tech Virtual Private Network (VPN) for real time viewing from surveillance cameras or use of surveillance records.
10. Describe what access controls or technologies the system can employ to prevent misuse of data, such as unauthorized disclosure of video records to third parties.

C. Operating Standards

1. The proposed system must be broad enough to address all university locations as described in University Policy and Procedures No. 5617 (Attachment D).
2. Indicate whether the proposed solution will include an API for camera operation and image transfer available to the public and unencumbered by license and provide details.

3. Indicate whether cameras in the proposed solution can be fully configurable via a web browser with standard JavaScript and list the minimum versions required.
4. Indicate whether cameras in the proposed solution can be fully configurable via a web browser with Java.
5. Can configuration data from all components be exported and imported via plain ASCII text or XML? If so, please describe how.
6. The proposed system must provide for "five nines" (99.999%) reliability for uptime of video monitoring, storage and archival review functions, in a manner equivalent to the normal production mode.
7. The proposed system must monitor self-health and report failures of cameras and other edge peripherals to operations staff.

D. Technical Capabilities

1. The proposed system must address the use of security cameras as well as other video monitoring and recording systems. (See Attachment D)
2. To the extent possible, the proposed system should protect existing investments in legacy camera systems.
3. Describe the functional capabilities of the proposed system to simultaneously collect video including the maximum number of simultaneous digital and analog cameras, maximum number of frames per second, highest resolution, etc.
4. Describe the scalability characteristics of the proposed solution.
5. Describe how the proposed system will support access by multiple campus groups and accommodate different levels of users.
6. Describe the management characteristics of the proposed solution including:
    a. Search functions by camera, time and date or frame number
    b. Display capabilities of the system during active alarms
    c. Viewing of synchronized video from multiple cameras on a single monitor
    d. Operator selection of the camera or cameras to appear on the monitors and display format options.
    e. Real time review of video from multiple locations, and in some cases, simultaneous access to the same video feed.
    f. Procedures to export images and archive for legal purposes.
7. Describe how the proposed system will incorporate existing cameras, including both fixed and Pan Tilt Zoom (PTZ) cameras.
8. Describe the system's capability to copy video footage or single video frames from a stored surveillance recording on to a standard magnetic medium for viewing on a personal computer. Describe the playback controls available to users.
9. Describe the system's ability to incorporate the use of maps and other GIS data.
10. Describe the system's ability to capture audio.
11. Describe the system's ability to operate outdoors under low-light conditions or where lighting conditions will fluctuate.
12. Describe the system's ability to operate in inclement weather and temperature conditions ranging from 0-105 degrees Fahrenheit.
13. Describe how the proposed solution will support the future use of video analytics.
14. Describe the system's ability to operate during a power failure.

E. Account Management

1. Through expert consultation, the successful offeror must be able to assist the users of both new and existing camera systems with the design and implementation of the proposed system, so they may be in compliance with University Policy No. 5617 (Attachment D).
2. The successful offeror must be able to provide technical assistance to Information Technology and users regarding placement, type, connectivity and operation of cameras in both indoor and outdoor locations.
3. As the pilot project for the enterprise solution, the successful offeror must design and implement the first installation of the full safety and security system for Virginia Tech Parking Services at the Perry Street Parking Deck immediately upon award.
4. Describe the upgrade path from the completion of the parking deck pilot project to deployment of other university locations.
5. Provide detailed warranty information for all equipment in the proposed solution.
6. Describe the on-site support available to resolve a system failure. Provide a detailed description of maintenance options available for the proposed solution.

7. Provide a detailed description of the end user training included in the proposal to prepare Virginia Tech to use and administer the proposed solution, and to fully realize the utility of the proposed solution

F. Cost

1. Provide complete pricing information for an enterprise-wide safety and security camera system.
2. Provide itemized pricing information that includes all hardware, software, licensing, training and professional services, including annual maintenance and support.

VII. 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. One (1) **original and** seven (7) **copies** of each proposal must be submitted to:

   Virginia Tech
   Information Technology Acquisitions (0214)
   1700 Pratt Drive
   Blacksburg, VA 24061

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

   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. Proposals which are substantially incomplete or lack key information may be rejected by Virginia Tech 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, subletter, 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 subletter should be repeated at the top of the next page. The proposal should contain a table of contents which cross references the RFP requirements. Information which the offeror desires to present that does not fall within any of the requirements of the RFP should be inserted at 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.

   e. Ownership of all data, material and documentation originated and prepared for Virginia Tech pursuant to the 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 is 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.

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 detailed as possible so that Virginia Tech may properly evaluate your capabilities to provide the required goods and services. 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. Responses to the Statement of Needs as noted in Section VI formatted as noted above in Paragraph VII.A.2

3. The return of Attachment C filled out as required.

4. Four (4) recent references, either educational or governmental, for whom you have provided the type of goods and services described herein. Include the date(s) the goods and services were furnished, the client name, address and the name and phone number of the individual Virginia Tech has your permission to contact.

5. Demonstrate economic viability by providing a copy of your most recent annual report, public filing, or equivalent. Other financial statements may be requested as necessary, such as supplementary financial statements and any quarterly financial statements prepared since the period reported in the annual report. Supplementary financial statements should include, at a minimum, a consolidated balance sheet and income statement.

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

7. Small, Women-owned and Minority-owned Business (SWAM) Utilization:

   If your business can not be classified as SWAM, describe your plan for utilizing SWAM subcontractors if awarded a contract. Describe your ability to provide reporting on SWAM subcontracting spend when requested. If your firm or any business that you plan to subcontract with can be classified as SWAM, but has not been certified by the Virginia Department of Minority Business Enterprise (DMBE), it is expected that the certification process will be initiated no later than the time of the award. If your firm is currently certified, you agree to maintain your certification for the life of the contract. For assistance with SWAM certification, visit the DMBE website at www.dmbe.virginia.gov. Any questions relating to SWAM businesses or SWAM subcontracting opportunities can be directed to Mark Cartwright, the University's Assistant Director for Supplier Diversity, at 540-231-3333 or mcartwright@vt.edu.

VIII. SELECTION CRITERIA AND AWARD:

A. Selection Criteria

Proposals will be evaluated by Virginia Tech using the following:

Criteria	Maximum Point Value
1. Network Capabilities	
2. Security Capabilities	
3. Operating Standards	
4. Technical Capabilities	
5. Account Management	
6. Cost	
7. SWAM Utilization	
Total	100

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 then 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 which, 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. Should Virginia Tech determine in writing and in its sole discretion that only one offeror has made the best proposal, a contract may be negotiated and awarded to that offeror. The award document will be a contract incorporating by reference all the requirements, terms and conditions of this solicitation and the Contractor's proposal as negotiated. See Attachment B for sample contract form.

IX. OPTIONAL PRE-PROPOSAL CONFERENCE:

An optional pre-proposal conference will be held on **March 10, 2011 at 1:30 P.M**. in Room 115 of Research Building 14. The purpose of this conference is to allow potential Offerors an opportunity to present questions and obtain clarification relative to any facet of this solicitation.

While attendance at this conference will not be a prerequisite to submitting a proposal, offerors who intend to submit a proposal are encouraged to attend. For those attending, a site visit of the Perry Street Parking Deck, which will be the first implementation under the system, will follow the conference (see Account Management, VI.E.3.). An email to John Krallman with your company name and the number of people planning to attend will help with our planning.

Bring a copy of this solicitation with you. Any changes resulting from this conference will be issued in a written addendum to this solicitation.

It is strongly recommended that you obtain a Virginia Tech parking permit for display on your vehicle prior to attending the conference. While a parking permit is not necessary at 1770 Forecast Drive, the site of the conference, a permit is required elsewhere on campus. Parking permits are available from the Virginia Tech Parking Services Department located at 455 Tech Center Drive, phone: (540) 231-3200, e-mail: parking@vt.edu.

The format of the conference is to summarize background and procedural information, ask if there are follow-up questions to any Questions & Answers documents already posted to our department website (http://www.ita.vt.edu/VSSAC_RFP.html), receive any new questions, and close. Note that we do not plan to provide answers to questions immediately. For accuracy we plan to respond in writing in a document entitled Questions & Answers Pre-Proposal Conference that will be posted within a few days as an addendum to the RFP on the RFP website, http://www.ita.vt.edu/VSSAC_RFP.html. Please contact John Krallman if any questions arise. Follow-on questions will be accepted until 5:00 P.M., March 24, 2011. Answers will be posted as Addenda at the RFP website.

X. INVOICES:

Invoices for goods or services provided under any contract resulting from this solicitation shall be submitted to:

Virginia Polytechnic Institute and State University
Accounts Payable
201 Southgate Center
Blacksburg, VA 24061

XI. METHOD OF PAYMENT:

Virginia Tech will authorize payment to the contractor as negotiated in any resulting contract from the aforementioned Request for Proposal.

Payment can be expedited through the use of a ghost card payment system. For more information on this program please refer to Virginia Tech's Purchasing website: http://www.purch.vt.edu/Department/WellsOne.html

XII. ADDENDUM:

Any **ADDENDUM** issued for this solicitation may be accessed at http://www.ita.vt.edu/VSSAC_RFP.html. Since a paper copy of the addendum will not be mailed to you, we encourage you to check the web site regularly.

XIII. CONTRACT ADMINISTRATION:

A. Richard Hach, Associate Director, Network Administration, Network Infrastructure and Services, at Virginia Tech or his/her 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 Purchasing Department through a written amendment to the contract.

XIV. TERMS AND CONDITIONS:

This solicitation and any resulting contract/purchase order shall be governed by the attached terms and conditions.

XV. ATTACHMENTS:

Attachment A – Terms and Conditions
Attachment B – Standard Contract Form
Attachment C – Security Questions for Technology Based Procurements
Attachment D – University Policy 5617 - Safety and Security Camera Acceptable Use Policy

TERMS AND CONDITIONS

RFP General Terms and Conditions

http:/www.purch.vt.edu/html.docs/terms/GTC_RFP_100110.pdf

Special Terms and Conditions

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

3. **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, the resulting contract may be terminated by either party, without penalty, after the initial 12 months of the contract period upon 60 days written notice to the other party. Any contract cancellation notice shall not relieve the Contractor of the obligation to deliver and/or perform on all outstanding orders issued prior to the effective date of cancellation.

4. **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.

5. **INSURANCE**:
   By signing and submitting a proposal under this solicitation, the Offeror certifies that if awarded the contract, it will have the following insurance coverage at the time the work commences. Additionally, it will maintain these during the entire term of the contract and that all insurance coverage will be provided by insurance companies authorized to sell insurance in Virginia by the Virginia State Corporation Commission.
   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.

6. **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: Nancy Sterling
Information Technology Acquisitions (0214)
1700 Pratt Dr.
Blacksburg, VA 24061

7. **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.

8. **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 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.

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

10. **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.

11. **RENEWAL OF CONTRACT**: This contract may be renewed by Virginia Tech upon written agreement of both parties for five successive one year periods, or as negotiated under the terms of the current contract, and at a reasonable time (approximately 90 days) prior to the expiration.

12. **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.

13. **RIGHT TO SELECT PROJECT PERSONNEL:** The University has the right to interview and select all of the Contractor's personnel that will provide services under the Agreement.

14. **RIGHT TO REMOVE PROJECT PERSONNEL:** The University has the right to remove any of the selected Contractor's personnel that will provide services under the Agreement.

15. **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.

16. **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.

17. **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).

18. **SEVERAL LIABILITY**: Virginia Tech will be severally liable to the extent of its purchases made against any contract resulting from this solicitation. Applicable entities described herein will be severally liable to the extent of their purchases made against any contract resulting from this solicitation.

19. **WARRANTIES:**
    A. Vendor warrants that all services provided to Customer shall conform to and be performed in accordance with Vendor's proposal and that Vendor's services shall not infringe any third-party intellectual property rights
    B. The Contractor agrees that the goods and services furnished under any award resulting from this solicitation shall be covered by the most favorable commercial warranties the contractor gives any customer for such goods and services and that the rights and remedies provided therein are in addition to and do not limit those available to Virginia Tech by any other clause of this solicitation. A copy of this warranty must be furnished with the proposal.

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 _____ 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 by Virginia Tech in accordance with the contract documents.

CONTRACT DOCUMENT: The contract documents shall consist of this signed contract, Request For Proposal Number _____ dated _____, 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:_____	

Virginia Tech Security Questions for Technology-Based Procurements

If purchased, Virginia Tech reserves the right to conduct an IT security assessment on the product(s), system(s) and/or service(s) once delivered to validate the answers to the questions below.

If evaluation copies or instances are available for testing, they should be provided to the IT Security Office prior to purchase. Nicolas Pachis (npachis@vt.edu) or Randy Marchany (randy.marchany@vt.edu) may be contacted in the IT Security Office.

In the space following each question, please provide a Yes, No or a "no answer" (N/A), and add any appropriate comments. If the answer is No or N/A, please provide comments indicating how this question/concern is addressed elsewhere or why it is not applicable.

1. Does your product(s), system(s) and or service(s) protect against the SANS Top 20 security vulnerabilities http://www.sans.org/top20?

2. Does your product(s), system(s) and or service(s) protect against the OWASP http://www.owasp.org/index.php/OWASP_Top_Ten_Project?

3. What specific encryption algorithms are employed for your product(s), system(s) and/or service(s)?

4. Is all sensitive data (i.e. Social Security Numbers, Credit Card Numbers, Health Information, etc) encrypted in transit and at rest? If not, please explain? (NOTE: Please see the Sensitive Information page at http://www.security.vt.edu/sensitiveinfo.html for specifics).

5. Is login information such as user name and password encrypted during transmission from the client to the server? NOTE: Base-64 encoding is not acceptable.

6. Are operating systems (e.g. Windows or Linux), programming and scripting languages (e.g. Java or PHP), web servers (e.g. Apache or IIS), database servers (e.g.. Oracle or MySQL), application servers, etc. always promptly patched and current with security updates? If not, please explain.

7. Is all access, including administrative accounts, controlled and logged (i.e. firewalls, file system permissions, ACLs, database table permissions, packet logs, etc.)? If not, please explain.

8. Does your product(s), system(s) and/or service(s) prevent the use of shared credentials or accounts including administrative accounts?

9. Describe how your product(s), system(s) and/or service(s) authenticates and authorizes users?

10. Does your product(s) and/or system(s) facilitate compliance with Federal and State laws, such as FERPA, HIPPA and PCI?

11. Does your company alert customers to vulnerabilities and security issues in a timely fashion? If so, please describe your process.

For hosted services, in addition to questions above

1. Are intrusion detection technologies and firewalls utilized on the hosted system(s)?

2. Describe how your facility is physically secured?

3. Does your network or facility undergo vulnerability scanning and penetration testing?

4. Do your employees hold Information Technology Security certifications and/or secure coding certifications? If so, please describe them.

Virginia Polytechnic Institute and State University **No. 5617 Rev.: 0**
Policy and Procedures **Date: March 1, 2010**

Subject: Safety and Security Camera Acceptable Use Policy

1. Purpose

Virginia Tech is committed to enhancing the quality of life of the campus community by integrating the best practices of safety and security with technology. A critical component of a comprehensive security plan is the utilization of a security and safety camera systems. The surveillance of public areas is intended to deter crime and assist in protecting the safety and property of the Virginia Tech community. This policy addresses the university's safety and security needs while respecting and preserving individual privacy.

To ensure the protection of individual privacy rights in accordance with the university's core values and state and federal laws, this policy is adopted to formalize procedures for the installation of surveillance equipment and the handling, viewing, retention, dissemination, and destruction of surveillance records. The purpose of this policy is to regulate the use of camera systems used to observe and record public areas for the purposes of safety and security. The existence of this policy does not imply or guarantee that cameras will be monitored in real time 24 hours a day, seven days a week.

2. Policy

The Virginia Tech Police Department (VTPD) has the authority to select, coordinate, operate, manage, and monitor all campus security surveillance systems pursuant to this policy. All departments using camera surveillance are responsible for implementing and complying with this policy in their respective operations.

All existing uses of security camera systems shall be brought into compliance with this policy within 12 months of the approval of the policy. Unapproved or nonconforming devices will be removed.

A university Surveillance Oversight Committee (SOC) is an operational committee established by the Vice President for Administrative Services to oversee implementation of this policy. Proposed policy revisions will be reviewed by the SOC and the University Safety and Security Policy Committee.

2.1 Responsibilities

VTPD, in conjunction with Information Technology and the Office of Emergency Management (OEM), is responsible for realization and assimilation of the policy.

Information Technology and VTPD are responsible for advising departments on appropriate applications of surveillance technologies and for providing technical assistance to departments preparing proposals for the purchase and installation of security camera systems.

VTPD and Information Technology shall monitor developments in the law and in security industry practices and technology to ensure that camera surveillance is consistent with the best practices and complies with all Federal and State laws.

VTPD and Information Technology will review proposals and recommendations for camera installations and review specific camera locations to determine that the perimeter of view of fixed location cameras conforms to this policy. Proposals for the installation of surveillance cameras shall be reviewed by the Chief of Police or designee. Recommendations shall be forwarded to the SOC.

VTPD will review any complaints regarding the utilization of surveillance camera systems and determine whether this policy is being followed. Appeals of a decision made by the Chief of Police will be made to and reviewed by the SOC which will make a recommendation to the Vice President for Administrative Services who will render a decision. An appeal of the Vice President for Administrative Services decision may be taken to the University President who is the final arbiter.

2.1.1 Responsibilities of Surveillance Oversight Committee (SOC)

The SOC will be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by the Chief of Police. The SOC shall propose to the Vice President for Administrative Services appropriate changes to this policy as needed.

The SOC shall be comprised of five members;

- The Virginia Tech Chief of Police or designee, Chair of the SOC
- Chief Information Officer or designee
- Vice President for Student Affairs or designee
- Associate Vice President for Facilities or designee
- Virginia Tech Director of Emergency Management or designee

2.1.2 Responsibilities of University Relations and General Counsel

University Relations will review all external requests to release records obtained through security camera surveillance. University Relations will seek consultation and advice from the General Counsel related to these requests prior to the release of any records.

2.2 Scope

This policy applies to all personnel, departments, and colleges of Virginia Tech in the use of security cameras and their video monitoring and recording systems. Security cameras may be installed in situations and places where the security and safety of either property or persons would be enhanced. Cameras will be limited to uses that do not violate the reasonable expectation of privacy as defined by law. Where appropriate, the cameras may be placed campus-wide, inside and outside buildings. Although the physical cameras may be identical, the functions of these cameras fall into three main categories:

A. **Property Protection:** Where the main intent is to capture video and store it on a remote device so that if property is reported stolen or damaged, the video may show the perpetrator. Examples: an unstaffed computer lab, an unstaffed science lab, or a parking lot.

B. **Personal Safety:** Where the main intent is to capture video and store it on a remote device so that if a person is assaulted, the video may show the perpetrator. Examples: a public walkway, or a parking lot.

C. **Extended Responsibility:** Where the main intent is to have the live video stream in one area monitored by a staff member in close proximity. In this case video may or may not be recorded. Example: a computer lab with multiple rooms and only one staff.

2.3 General Principles

Information obtained from the cameras shall be used exclusively for law and/or policy enforcement, including, where appropriate, student judicial functions. Information must be handled with an appropriate level of security to protect against unauthorized access, alteration, or disclosure in accordance with Policy 7105, Policy for Protecting University Information in Digital Form (.http://www.policies.vt.edu/7105.pdf)

All appropriate measures must be taken to protect an individual's right to privacy and hold university information securely through its creation, storage, transmission, use, and deletion.

All camera installations are subject to federal and state laws.

Departments requesting security cameras will be required to follow the procedures outlined in this policy.

2.3.1 Placement of Cameras

The locations where cameras are installed may be restricted access sites such as a departmental computer lab; however, these locations are not places where a person has a reasonable expectation of privacy. Cameras will be located so that personal privacy is maximized.

No audio shall be recorded except in areas where no one is routinely permitted. Requests to utilize audio surveillance that does not comply with this requirement will be evaluated on a case by case basis by the SOC.

Camera positions and views of residential housing shall be limited. The view of a residential housing facility must not violate the standard of a reasonable expectation of privacy.

Unless the camera is being used for criminal surveillance, monitoring by security cameras in the following locations is prohibited:

- Student dormitory rooms in the residence halls,
- Bathrooms,
- Locker rooms,
- Offices,
- Classrooms not used as a lab.

The installation of “dummy” cameras that do not operate is prohibited.

Unless being used for criminal surveillance all video camera installations should be visible.

2.3.2 Access and Monitoring

All recording or monitoring of activities of individuals or groups by university security cameras will be conducted in a manner consistent with university policies, state and federal laws, and will not be based on the subjects’ personal characteristics, including age, color, disability, gender, national origin, race, religion, sexual orientation, or other protected characteristic. Furthermore, all recording or monitoring will be conducted in a professional, ethical, and legal manner. All personnel with access to university security cameras should be trained in the effective, legal, and ethical use of monitoring equipment.

With the exception of **Extended Responsibility** cameras, university security cameras are not monitored continuously under normal operating conditions, but may be monitored for legitimate safety and security purposes that include but are not limited to the following: high risk areas, restricted access areas/locations, in response to an alarm, special events, and specific investigations authorized by the Chief of Police or designee.

For **Property Protection** and **Personal Safety** cameras, access to live video or recorded video from cameras shall be limited to persons authorized by the Chief of Police or designee. For Extended Responsibility cameras, the live video can be monitored by the staff person: however, any video recorded must comply with the recording storage and retention requirements of this policy.

When an incident is reported, the personnel responsible for the area in question may request to the Police Chief to review the images from the camera. As circumstances require, the Police Chief may authorize others to review images. A record log will be kept of all instances of access to and use of recorded material. Nothing in this section is intended to limit the authority of the Virginia Tech Police Department (VTPD) in law enforcement activities.

2.3.3 Appropriate Use and Confidentiality

Personnel are prohibited from using or disseminating information acquired from University security cameras except for official purposes. All information and/or observations made in the use of security cameras are considered confidential and can only be used for official university and law enforcement purposes upon the approval of the Chief of Police or designee. Personnel are expected to know and follow University Policy 7000, Acceptable Use and Administration of Computer and Communication Systems and the Acceptable Use of Information Systems at Virginia Tech (www.policies.vt.edu/7000.pdf).

2.3.4 Use of Cameras for Criminal Investigations

The use of mobile or hidden video equipment may be used in criminal investigations by VTPD. Covert video equipment may also be used for non-criminal investigations of specific instances which may be a significant risk to public safety, security and property as authorized by the Chief of Police or designee.

2.3.5 Exceptions

This policy does not apply to cameras used for academic purposes. Cameras that are used for research would be governed by other policies involving human subjects and are therefore excluded from this policy.

This policy does not address the use of Webcams for general use by the University (e.g., on the Official Virginia Tech Website). This policy also does not apply to the use of video equipment for the recording of public performances or events, interviews, or other use for broadcast or educational purposes. Examples of such excluded activities would include

videotaping of athletic events for post game review, videotaping of concerts, plays, and lectures, or videotaped interviews of persons. Automated teller machines (ATMs), which may utilize cameras, are exempt from this policy.

3. Procedures

Departments requesting security cameras will be required to follow the procedures outlined in this policy.

3.1 Installation

Individual colleges, departments, programs, or campus organizations installing video surveillance equipment shall submit a written request to their appropriate dean or vice president describing the proposed location of surveillance devices, justifying the proposed installation, providing a cost estimate, and identifying the funding source or sources for purchase and ongoing maintenance.

- The vice president or dean will review the request and recommend it to the Chief of Police, if appropriate.
- The Chief of Police or designee will review all proposals from deans and vice presidents. Upon completion of review of the project, the Chief of Police will forward the proposal to the SOC with a recommendation.
- The SOC will be responsible for reviewing and approving or denying all proposals for security camera equipment recommended by the Chief of Police.

Communication Network Services shall oversee the installation of all approved security camera systems with the assistance of VTPD, the Office of Information Technology and Facilities, as required.

Purchasing (HokieMart) will not accept, approve, or process any order for security camera systems without the approval of the SOC.

3.2 Training

Camera control operators shall be trained in the technical, legal, and ethical parameters of appropriate camera use. Camera control operators shall receive a copy of this policy and provide written acknowledgement that they have read and understood its contents.

3.3 Operation

Video surveillance will be conducted in a manner consistent with all existing university policies.

Camera control operators shall monitor based on suspicious behavior, not individual characteristics.

Camera control operators shall **not** view private rooms or areas through windows.

All operators and supervisors involved in video surveillance will perform their duties in accordance with this policy.

3.4 Storage and Retention of Recordings

No attempt shall be made to alter any part of any surveillance recording. Surveillance centers and monitors will be configured to prevent camera operators from tampering with or duplicating recorded information.

Surveillance records shall not be stored by individual departments. All surveillance records shall be stored in a secure university centralized location for a period of 30 days and will then promptly be erased or written over, unless retained as part of a criminal investigation or court proceedings (criminal or civil), or other bona fide use as approved by the Chief of Police. Individual departments shall not store video surveillance recordings.

A log shall be maintained of all instances of access to or use of surveillance records. The log shall include the date and identification of the person or persons to whom access was granted.

4. Definitions

5. References

Policy 7000, Acceptable Use and Administration of Computer and Communication Systems
http://www.policies.vt.edu/7000.pdf

Policy 7105, Policy for Protecting University Information in Digital Form
http://www.policies.vt.edu/7105.pdf

6. Approval and Revisions

Approved March 1, 2010 by Vice President for Administrative Services, Sherwood G. Wilson.

Safety and Security Camera Acceptable Use Policy