Alaska Railroad Corporation
327 W. Ship Creek Avenue, Anchorage, AK 99501
P.O. Box 107500, Anchorage, AK 99510-7500
Telephone 907.265.2593 Facsimile 907.265.2439

December 24, 2015

REQUEST FOR PROPOSAL

#15-63-204437

Security Incident and Event Management Software/Hardware, Implementation, Training, and Integration Services

Response Required

This form must be completed and returned to ensure receipt of future addenda or additional information. Please email this form to goemerg@akrr.com All addenda will be forwarded to the contract name and number listed below.

Company _____

Address _____

_____

Contact _____

Phone _____ Fax_____

Email _____

www.alaskarailroad.com

Alaska Railroad Corporation
327 W. Ship Creek Avenue, Anchorage, AK 99501
P.O. Box 107500, Anchorage, AK 99510-7500
Telephone 907.265.2481 Facsimile 907.265.2439

December 24, 2015

REQUEST FOR PROPOSALS

#15-63-204437

The Alaska Railroad Corporation (ARRC) is soliciting proposals from interested concerns for the following:

Security Incident and Event Management Software/Hardware, implementation, Training, and Integration Services

Sealed offers in **original and five (5) copies** will be received until **3:00 pm local time, January 22nd**. The envelope used for the submittal of your offer shall be plainly marked with the following information:

1. Offeror's name.
2. Offer number 15-63-204437
3. Date and time scheduled for the receipt of offers.
4. Sealed Offer: Security Incident and Event Management Software (SIEM)

PRE-BID/ Conference: A Pre-Bid Conference and is scheduled for **January 6, 2016 at 10:00 AM Alaska Standard Time** via telephone conference line @ 907-265-2348. A bidder's failure to participate will in no way relieve the bidder of the responsibility of performing the work in strict compliance with the true intent and meaning of the terms, conditions and specifications of this RFP.

The Alaska Railroad may award a contract resulting from this solicitation to the responsible offeror whose offer conforming to this solicitation will be most advantageous to the Alaska Railroad. The Alaska Railroad may reject any or all offers if such actions is in the best interest of Alaska Railroad, and waive informalities and minor irregularities in offers received.

ARRC may award a contract on the basis of initial proposals without discussions. Therefore, each initial proposal should contain the offeror's best terms from a cost or price and technical standpoint. Any contract resulting from this solicitation shall incorporate the General Terms and Conditions contained in this solicitation package.

This Request for Proposal is not to be construed as a commitment of any kind nor does it commit the Alaska Railroad to pay any costs incurred in the submission of an offer or for any other costs incurred prior to the execution of a formal contract.

Proposals received after the time and date set forth above shall be rejected. All proposals submitted in response to this solicitation must be signed by an individual with the legal authority to submit the offer on behalf of the company.

The Alaska Railroad is a member of Green Star (http://www.greenstarinc.org/). ARRC earned an initial Green Star Award in 1994 and a Green Star Air Quality Award in 2007. The Alaska Railroad considers Green Star membership to be a positive business attribute, and regards a Green Star award as a tangible sign of an organization's commitment to environmental stewardship and continual improvement within its operations.

Please direct all responses to this solicitation and/or questions concerning this Request for Proposal to Greg C. Goemer, Alaska Railroad Corporation, 327 W. Ship Creek Avenue, Anchorage, AK 99501 or email to goemerg@akrr.com.

Best Regards,

Greg Goemer
Sr. Contract Administrator

SOLICITATION INDEX

ATTACHMENTS:

1. **Sizing**
2. **SIEM Requirements Document**
3. **Functional Responses sheet**
4. **NIST SP 800-82 (Revision 2) guidance document**

SECTION A

BACKGROUND INFORMATION

The Alaska Railroad Corporation (ARRC) is a full-service freight and passenger railroad linking ports and communities throughout South-central and Interior Alaska to the state's major metropolitan centers, Anchorage and Fairbanks. Although owned by the State of Alaska, it is incorporated and run as a private business. ARRC receives no operating funds from the State, and its employees are not State employees.

ARRC employs approximately 620 year-round, with another 125 seasonal employees. Ensuring our technology is protected, threats identified, and employees have the knowledge and skills they need to do their jobs correctly and safely is critical to our operational sustainability. In order to help ARRC provide a modern view of the vulnerabilities, attack vectors and responses, we are purchasing a SIEM, implementation, training, monitoring assistance, and periodic reviews of our security architecture.

ARRC has hundreds of devices, networks, users, external interactions (EDI), and Positive Train Control (PTC) in the form of the mandated Interoperable – Electronic Train Management System (I – ETMS). Our systems need a unifying technology platform to assist with understanding, monitoring, improving, hardening, and maintaining our security infrastructure. We are looking for a technology partner who can provide a SIEM solution, assist in the implementation of Hardware/Software, and provide services, training and periodic reviews of our security incidents and events.

Cybersecurity Solutions may be:

- Cloud based or terrestrial (Offsite or onsite)
- Hardware, Software or virtual

Cybersecurity Solutions must be:

- Easily implemented, maintained and upgraded
- Capable of taking inputs from the many technological sources across the Railroad
- Automatically update attack signatures, methods and techniques
- Include free online instruction for users (if applicable)
- Include in-depth administrator courses available via web
- Provide dashboard and web based monitoring capabilities

To operate our technology platforms safely and effectively, as well as meet our regulatory requirements, ARRC will select a firm and product that has a demonstrated ability to assist firms to meet the following Guideline and requirements:

- PCI-DSS
- NIST SP 800-53
- NIST SP 800-82

SECTION B

SCOPE OF SERVICES

The Alaska Railroad Corporation (ARRC) is seeking proposals from Cybersecurity Firms who can provide a unifying technology platform to assist with understanding, monitoring, improving, hardening, and maintaining our security infrastructure. We are looking for a technology partner who can provide a SIEM solution, assist in the implementation of Hardware/Software, and provide services, training and periodic reviews of our security incidents and events.

MINIMUM QUALIFICATIONS TO BE CONSIDERED RESPONSIVE:

- A technology platform that will provide event and log management based on our sizing document (Attachment 1)
- A technology platform that will allow a review of attacks at the IP session level (review of a series of packets that establish an attack)
- The ability to track events over a period of years
- The ability to review specifics of attacks and situations based on IP connections for weeks
- Implementation services sufficient to bring up a dashboard of reports and critical systems, services and architecture status
- Training services sufficient to prepare the administrator to train others in the operation of the system.
- Monitoring assistance services (6 months). Limited consulting on the true meaning of incidents, appropriate response, configuration techniques, reporting tools, alerting configuration, storage and maintenance tasks.

These services and the product will ensure our platforms are providing the needed benefits.

The product must provide capabilities based on:

- Technical requirements document (Attachment 2)
- Functional Responses document (Attachment 3)
- NIST 53 and 82 Guidance (Attachment 4)

SECTION C

PROPOSAL FORMAT AND CONTENT

Alaska Railroad Corporation (ARRC) is requesting proposals from interested firms qualified to perform the work described in the Scope of Services. This is intended to be an unbiased evaluation. ARRC reserves the right to determine that proposed services will meet ARRC requirements. ARRC reserves the right to withdraw this RFP, reject any and all proposals, advertise for new proposals, or accomplish the work by other means including issuing only some of the tasks defined in the Scope of Services above, that ARRC in its sole discretion, determines to be in its best interest. ARRC may request additional information from any firm to make a proposal responsive to this RFP or otherwise obtain clarification or additional information that ARRC, in its sole discretion, deems necessary to analyze and compare proposals. Proposals must be complete as to the requested information.

SELECTION PROCESS AND EVALUATION CRITERIA

The selection of a contractor (or contractors) to perform the requested services will be made by the Selection Committee which will evaluate the proposals in accordance with the evaluation criteria specified herein. Proposals will be evaluated on the basis of advantages and disadvantages to ARRC using the criteria described in this section. Please note, however, that a serious deficiency in any one criterion may be grounds for rejection and that the listing of cost as an evaluation factor does not require ARRC to select the firm that submits the lowest cost. ARRC shall have the right to obtain, from any and all sources, information concerning a Proposer, which is deemed pertinent to the RFP, and to consider such information in the evaluation of the Proposer's Proposal.

ARRC reserves the right to select the top ranked firm based solely on the scoring of the written proposals and to enter directly into negotiations with said firm. However, at its sole discretion, ARRC may require the highest ranked firms to make an additional presentation to the evaluation committee. The selected firms will have an opportunity to summarize the information provided in their written proposals, expand on their capabilities, experience and proposed approach and work plan and answer questions from the selection committee. Scores obtained in the initial phase will not carry over to the presentation phase. Upon completion of the presentations, the evaluation committee will review the material presented and determine a ranking order for the firms interviewed.

Failure to follow this format in a proposal or failure to include complete information as requested will result in a lower score and may result in rejection of the proposal. At a minimum your proposal shall address the following in order to be considered responsive

EVALUATION CRITERIA

DESCRIPTION	WEIGHT
Qualifications of the Firm	**15%**
Proposed Key Personnel	**15%**

Functional Requirements	**30%**
Implementation and Approach	**15%**
Cost Proposal	**25 %**
Total Score	**100**

Qualifications of the Firm – Attachment 4 and **15%**

1. Please give an overview / profile of your company including a brief history and a profile of your key management staff.
2. What are your company's key success factors and what differentiates you from your competition?
3. Please indicate if your Company has been profitable in your last 4 years of business.
4. What awards or certifications (if any) has your company received?
5. How many scheduled releases in past two years?
6. Does your company own full rights to the application and source code?
7. Does your company perform its own implementation and systems integration or do you outsource?
8. Do you require Clients to upgrade? If yes, what is your average time frame to upgrade? If no, do you provide support for older versions?
9. Please provide three (3) government sector or transportation client references that are using your software.

Proposed Key Personnel – Attachment 4 and **15%**

1. Discuss the availability of key personnel for this engagement.
2. Include resumes and work experience of the key personnel to be assigned to the work effort, clearly describing their qualifications and experience. Information about these individuals should include three clients where they are performing tasks and functions comparable to those outlined in the Scope of Services for a client with similar scope and complexity.
3. ARRC reserves the right to terminate the contract at any point after award if the approved personnel become unavailable, are reassigned or otherwise removed from the project by the firm, or the qualifications are generally found to be inadequate.

4. All personnel reassignments will be approved by ARRC in writing.

5. Disclose any actual or appearance of conflict of interest.

Functional Requirements – Attachments 2 and 3 **30%**

1. Extent to which the proposed solution meets the RFP's functional requirements

2. Compliance with the RFP's technical requirements

3. Extent of modifications required to meet requirements

4. Ease of Use

Implementation and Approach **15%**

1. Describe your project approach

2. Describe your project plan and schedule

3. Describe your project management

4. Outline your current workload and your ability to perform required work within VRS schedules

5. Describe your system training

Cost Proposal: **25%**

Provide a detailed description on how your firm is to be remunerated for the services requested to include:

1. Provide the hourly rates of the key individuals who will be responsible for the performance of the services and maintenance.

The cost/fee matrix covering the following:

2. SIEM – Costs including setup, hw/sw - (Attachment 1)

3. Netflow costs – including setup, hw/sw – (Attachment 1)

4. Cost of storage additions (If any) –

5. Implementation Costs – Installation, setup, configuration, initial reporting (base level), event identification, event response, mitigation, backup, archive, restore, HA –

6. Implementation services sufficient to bring up a dashboard of critical systems, services and architecture status –

7. Training services sufficient to prepare the administrator to train others in the operation of the system. –

8. Monitoring assistance services (6 months) -

9. Yearly maintenance fees starting after year one.

Other direct costs (ODC) on contracts incurred shall be billed at cost. Any travel and travel related expenses shall be billed at cost with coach airfare only, no first class or business class. Lodging and meal expenses must be reasonable. ARRC will not pay for alcohol, valet parking or other expenses it considers to be exorbitant.

For purposes of determining low cost, the costs shall be totaled in the aggregate. The Firm with the lowest cost in the aggregate shall receive a score of 25 the other offers following suit shall be calculated on a percentage basis and ranked accordingly

Contract Award

Once the committee has established a ranking, ARRC will begin negotiations with the highest ranked firm. If an agreement cannot be reached on contract terms, negotiations will be terminated, and negotiations will be conducted with the next highest ranked firm, until an agreement is reached, or until ARRC exercises its right to cancel the solicitation.

Proposers may be disqualified, and their Proposals rejected, for any reason deemed appropriate by ARRC including, but not limited to, the following:

(a) Evidence of collusion between a Proposer and any other Proposer(s).

(c) Evidence that the Proposer may not be financially able to complete the work required by the Scope of Work in a satisfactory manner.

(d) If Proposer has failed to complete one or more public contracts in the past, or an unsatisfactory performance record on prior projects.

(e) If Proposer has been convicted of a crime arising from previous public contracts.

(f) If Proposer is not authorized to perform work in the State of Alaska.

SECTION D

PROPOSAL INFORMATION, CONDITIONS & INSTRUCTIONS

1. Pre-Submission Proposal Inquires

Proposers shall promptly notify ARRC of any ambiguity, inconsistency, conflict, or error which they may discover upon examination of the solicitation documents. Verbal inquiries regarding this RFP are not permitted. All inquiries must be made in writing and received at ARRC's offices prior to January 11, 2016 and the written inquiries must be submitted as follows:

Greg Goemer
Alaska Railroad Corporation
327 W. Ship Creek Ave.,
Anchorage, Alaska 99501
Email Goemerg@akrr.com

ARRC will respond to all or part of the written inquiries received through the issuance of a written Addendum to the RFP, if in the opinion of ARRC, such information is deemed necessary to submit proposals or if the lack of it would be prejudicial to other prospective proposers. Oral and all other non-written responses, interpretations and clarifications shall not be legally effective or binding. Any Proposer who attempts to use or uses any means or method other than those set forth above to communicate with ARRC or any director, officer, employee or agent thereof, regarding this RFP shall be subject to disqualification.

2. Proposal Submission Deadline

Sealed proposals must be received by ARRC no later than 3:00 p.m., local time, on January 22, 2016 at:

Alaska Railroad Corporation
Purchasing Department
327 W. Ship Creek Avenue,
Anchorage, AK 99501

One (1) original and five (5) copies of each proposal must be submitted. The sealed envelope or package used in submitting a proposal shall be clearly marked with the following information:

1. Proposer's Name
2. RFP number 15-63-204437
3. Date and Time Scheduled for Receipt of Proposals
4. Sealed Proposal: Security Incident and Event Management (SIEM)

Proposals received after the time and date set forth above shall be rejected. All proposals submitted in response to this solicitation must be signed by an individual with the legal authority to submit the offer on behalf of the company.

3. Proposal Open and Subject to Acceptance

All proposals shall remain open and subject to acceptance by ARRC for ninety (90) days after the deadline for proposal submission.

4. Proposal Opening

Proposals will be opened privately at ARRC's convenience on or after the proposal due date.

5. Reserved Rights

In addition to other rights in this RFP, ARRC reserves, holds and may exercise at its sole discretion, the following rights and options:

(a) To supplement, amend, or otherwise modify or cancel this RFP with or without substitution of another RFP.
(b) To issue additional or subsequent solicitations for proposals.
(c) To conduct investigations of the Proposers and their proposals.
(d) To clarify the information provided pursuant to this RFP.
(e) To request additional evidence or documentation to support the information included in any proposal.
(f) To reject any and all proposals, or parts thereof, and/or to waive any informality or informalities in any of the proposals or the proposal process for the RFP, if such rejection or waiver is deemed in the best interest of ARRC.
(g) To award a contract or contracts resulting from this solicitation to the responsible Proposer whose proposal conforming to this solicitation will be most advantageous to ARRC.
(h) To negotiate any rate/fee offered by a Proposer. ARRC shall have the sole right to make the final rate/fee offer during contract negotiations. If the selected Proposer does not accept ARRC's final offer, ARRC may, in its sole discretion, reject the proposal and start negotiations with the next highest ranked Proposer.
(i) If an award is made and, prior to entering into a contract, subsequent information indicates that such award was not in the best interest of ARRC, ARRC may rescind the award without prior notice to proposers and either award to another proposer or reject all proposals or cancel the RFP.
(k) To terminate the contractor at any point in the evaluation process or after award if the approved personnel become unavailable, are switched off project by the firm, or the qualifications are generally found to be inadequate. All personnel reassignments to and from the project will be approved by ARRC.

6. Proposal Costs

Each Proposer shall be solely responsible for all costs and expenses associated with the preparation and/or submission of its proposal, and ARRC shall have no responsibility or liability whatsoever for any such costs and expenses. Neither ARRC nor any of its directors, officers, employees or authorized agents shall be liable for any claims or damages resulting from the solicitation or collection of proposals. By submitting a proposal, Proposer expressly waives (i) any claim(s) for such costs and expenses, and (ii) any other related claims or damages.

7. Taxes

Pursuant to AS 42.40.910, ARRC is exempt from all forms of state or local sales, property and other taxes. Accordingly, any Proposer who submits a proposal shall not include any such tax in any of its proposal prices or in any calculation thereof.

8. Proposal Format

Interested firms shall submit one (1) original proposal and five(5) copies, containing a statement of qualifications and a concise narrative that fully addresses each evaluation criteria. Proposals shall have a maximum of thirty (30) pages, exclusive of resumes and exhibits. A signed cover letter of a maximum two (2) pages should introduce the proposed firm, summarize the main qualifications of the firm, and include any other information the Contractor deems will emphasize the Contractor's ability to successfully perform the services required and demonstrate why selection of Contractor would be advantageous to ARRC. A limited number of larger (11x17) sheets are acceptable for graphics or charts. The page limit excludes cover sheets, cover letter, table of contents, forms required by ARRC, resumes or other attachments required herein.

9. Capacity to Perform

Any Proposer considered for award as a result of this solicitation may be required to make assurance to the Contract Administrator concerning the Proposer's capacity and capability to perform. Previous contracts of a like nature, financial solvency, and other information may be requested of the considered Proposer. Failure to provide assurances requested in a timely manner may be cause for rejection of the Proposal.

10. Purchase Obligation

ARRC and responding firms expressly acknowledge and agree that ARRC has made no express or implied promises to expend any dollar amounts with respect to the services addressed by this RFP. By submitting a proposal in response to this RFP, each firm acknowledges and agrees that the provisions of this RFP, and/or any communication, statement, act or omission by representatives of ARRC (including consultants) in the selection process, shall not vest any right, privilege, or right of action in any Proposer.

11. Exceptions to Terms, Conditions and Specifications

Any contract resulting from this solicitation shall incorporate the General Terms and Conditions contained in this solicitation package. Each Proposer shall indicate all exceptions to terms, conditions, and specifications of this solicitation individually in its proposal. Exceptions received or placed after the proposal submission date will be considered as counter offers and as such will render the entire proposal non-responsive.

12. Public Information

All submitted proposals will be considered confidential until notice of intent to award is issued. After notice of intent to award is issued, all proposals will become public information.

13. Conflict of Interest

Disclose any information that may pose an actual conflict of interest in providing these services or give the appearance of a conflict of interest.

APPENDIX F

QUESTIONNAIRE
(Revised 2-27-06)

Note: Failure to provide the information requested in this questionnaire may be cause for rejection of your proposal or offer on the grounds of non-responsiveness and/or non-responsibility.

Solicitation Number _____

Business Name: _____

Street Address: _____

Mailing Address if Different: _____

City:_____ State: _____Mailing Zip:_____

Telephone: _____ Fax:_____ E-Mail: _____

Date Firm Established: _____

How many years has the business been under the above name? _____

Previous business name(s) if any:_____

Federal Tax ID Number: _____

Business License Number: _____

Bid Acceptance Period _____Days. (Bids providing less than ninety-day (90) calendar days for acceptance may be considered non-responsive and may be rejected.)

Discount for prompt pay _____% _____ days.

List any variations from or exceptions to the Terms, Conditions or Specifications of the Solicitation

_____

_____

_____

Continued on the next page

Are you acting as a broker or the primary supplier in this transaction?

☐ Broker

☐ Primary Supplier

Business Information (Please check all that apply):

☐ The business is Individual
☐ The business is a Partnership
☐ The business is a Non-Profit
☐ The business is a Joint-Venture
☐ The business is a Corporation incorporated under the laws of the State of _____
☐ The business is full-time
☐ The business is part-time
☐ The business is not a certified Disadvantaged Business (DBE)
☐ Business is a certified DBE
☐ DBE was certified by State DOTPF
☐ DBE was certified by the Municipality of Anchorage
☐ Business is an 8(a)/WBE/MBE and is certified by SBA
☐ Business was certified by _____

☐ DBE Certification # is _____

Firms Annual Gross Receipts:

☐ <$500,000
☐ $500,000 - $999,999
☐ $1,000,000 - $4,999,999
☐ $5,000,000 - $9,999,999
☐ $10,000,000 - $16,999,999
☐ >$17,000,000

Completed by: _____ Title: _____

Signature: _____

Date:_____

SECTION G

GENERAL TERMS AND CONDITIONS
(Professional Service Contracts)
(Revised 3/4/08)

The following terms and conditions supersede the terms and conditions on the reverse side of ARRC's purchase order to the extent that they are inconsistent therewith and shall be deemed to have the same force and effect as though expressly stated in any such purchase order into which this document is incorporated.

1. Definitions.

"ARRC" shall mean the Alaska Railroad Corporation.

"Contractor" shall mean the person or entity entering into the contract to perform the work or services specified therein for ARRC.

"Contract" shall mean these General Terms and Conditions, the contract form to which they are annexed, and all other terms, conditions, schedules, appendices or other documents attached to the contract form or incorporated by reference therein.

"Services" shall mean any work, direction of work, technical information, technical consulting or other services, including but not limited to design services, analytical services, consulting services, construction management services, engineering services, quality assurance and other specialized services furnished by Contractor to ARRC under the contract.

2. Inspection and Reports. ARRC may inspect all of the Contractor's facilities and activities under this contract in accordance with the provisions of ARRC Procurement Rule 1600.9. The Contractor shall make progress and other reports in the manner and at the times ARRC reasonably requires.

3. Claims. Any claim by Contractor for additional compensation or equitable adjustment arising under this contract which is not disposed of by mutual agreement must be made by Contractor in accordance with the time limits and procedures specified in sections 1800.12 et seq. of ARRC's Procurement Rules, which by this reference are hereby incorporated herein.

4. Nondiscrimination.

4.1 The Contractor may not discriminate against any employee or applicant for employment because of race, religion, color, national origin, ancestry, physical or mental handicap, sex, marital status, change in marital status, pregnancy or parenthood when the reasonable demands of the positions do not require distinction on the basis of age, physical handicap, sex, marital status, changes in marital status, pregnancy, or parenthood. To the extent required by law, the Contractor shall take affirmative action to insure that the applicants are considered for employment and that employees are treated during employment without unlawful regard to their race, color, religion, national origin, ancestry, physical or mental handicap, age, sex, marital status, changes in marital status, pregnancy or parenthood. This action must include, but need not be limited to, the following: employment, upgrading, demotion, transfer, recruitment or recruitment advertising, layoff or termination, rates of pay or other forms of compensation, and selection for training including apprenticeship. The Contractor shall post

in conspicuous places, available to employees and applicants for employment, notices setting out the provisions of this paragraph.

4.2 The Contractor shall cooperate fully with ARRC efforts which seek to deal with the problem of unlawful discrimination, and with all other ARRC efforts to guarantee fair employment practices under this contract, and promptly comply with all requests and directions from the State Commission for Human Rights or any of its officers or agents relating to prevention of discriminatory employment practices.

4.3 Full cooperation in Paragraph 4.2 includes, but is not limited to, being a witness in any proceeding involving questions of unlawful discrimination if that is requested by any official or agency of the State of Alaska; permitting employees of the Contractor to be witnesses or complainants in any proceeding involving questions of unlawful discrimination, if that is requested by any official or agency of the State of Alaska; participating in meetings; submitting periodic reports on the equal employment aspects of present and future employment; assisting inspection of the Contractor's facilities; and promptly complying with all State directives considered essential by any office or agency of the State of Alaska to insure compliance with all federal and state laws, regulations, and policies pertaining to the prevention of discriminatory employment practices.

4.4 Failure to perform under this section constitutes a material breach of the contract.

5. Cancellation/Termination.

5.1 ARRC may, for its sole convenience, cancel this contract in whole or in part, at any time by giving written notice of its intention to do so. In the event of such cancellation, Contractor shall be entitled to receive payment in accordance with the payment provisions of this contract for services rendered or charges incurred prior to the effective date of termination. Contractor shall not be paid for any work done after receipt of a notice of cancellation or for any costs incurred by Contractor's suppliers or subcontractors which Contractor could reasonably have avoided. In no event shall ARRC be liable for unabsorbed overhead or anticipatory profit on unperformed services.

5.2 In addition to ARRC’s right to cancel this contract for its convenience, ARRC may, by written notice of default to Contractor, terminate the contract in whole or in part in the following circumstances:

(1) The Contractor refuses or fails to perform its obligations under the contract, or fails to make progress so as to significantly endanger timely completion or performance of the contract in accordance with its terms, and Contractor does not cure such default within a period of ten (10) days after receipt of written notice of default from ARRC or within such additional cure period as ARRC may authorize; or

(2) Reasonable grounds for insecurity arise with respect to Contractor’s expected performance and Contractor fails to furnish adequate assurance of due performance (including assurance of performance in accordance with the time requirements of the contract) within ten (10) days after receipt of a written request by ARRC for adequate assurance; or

(3) Contractor becomes insolvent or makes an assignment for the benefit of creditors or commits an act of bankruptcy or files or has filed against it a petition in bankruptcy or reorganization proceedings.

5.3 Upon receipt of a notice of cancellation or termination, Contractor shall immediately discontinue all service and it shall immediately cause any of its suppliers or subcontractors to cease such work unless the notice directs otherwise and deliver immediately to ARRC all reports, plans, drawings, specifications, data, summaries or other material and information, whether completed or in process, accumulated by Contractor in performance of the contract. In the event of termination for default, Contractor shall not be entitled to receive any further payment until the work is finished. If the unpaid balance of the amount to be paid on this contract exceeds the expense of finishing the work, compensation for additional managerial and administrative services and such other costs and damages as ARRC may suffer as a result of Contractor's default, such excess shall be paid to Contractor. If such expense, compensation, costs and damages shall exceed such unpaid balance, Contractor shall be liable for and shall pay the differences to ARRC. The rights and remedies of ARRC provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law.

6. No Assignment or Delegation. The Contractor may not assign, subcontract or delegate this contract, or any part of it, or any right to any of the money to be paid under it, except with the prior written consent of ARRC. The hiring or use of outside services, subcontractors or consultants in connection with the work shall not be permitted without the prior written approval of ARRC. No such approval shall relieve Contractor from any of its obligations or liabilities under this contract.

7. Independent Contractor. The Contractor's relationship to ARRC in performing this contract is that of an independent contractor and nothing herein shall be construed as creating an employer/employee relationship, partnership, joint venture or other business group or concerted action. The personnel performing services under this contract shall at all times be under Contractor's exclusive direction and control and shall be employees of the Contractor, and not of ARRC.

8. Payment of Taxes. As a condition of performance of this contract, the Contractor shall pay all federal, state, and local taxes incurred by the Contractor and shall require their payment by any subcontractor or any other persons in the performance of this contract. Satisfactory performance of this paragraph is a condition precedent to payment by ARRC under this contract.

9. Ownership of Work Product. Except for items that have preexisting copyrights, all exhibits, drawings, plans, specifications, notes, reports, data, recommendations, artwork, memoranda and any other information prepared or furnished by Contractor to ARRC in the performance of this contract (collectively "Work Product") shall become the property of ARRC and may be used by ARRC for any other purpose without additional compensation to the Contractor. Contractor hereby grants ARRC an irrevocable, perpetual, royalty-free, fully assignable license (with full sublicense rights) to use all proprietary and confidential information and other intellectual property that may be incorporated into any of Contractor's Work Product for ARRC. Should ARRC elect to reuse said Work Product, ARRC shall indemnify, hold harmless and defend Contractor and its subcontractors against any damages or liabilities arising from said reuse. When Work Product produced by the Contractor and its Subcontractors under this Contract are reused by ARRC, the Contractor's and Subcontractor's signatures, professional seals, and dates shall be removed. If such Work Product requires professional signature and seal, it will be signed, sealed, and dated by the professional who is in direct supervisory control and responsible for the new project for which such Work Product is being reused.

Contractor hereby represents and warrants to and for the benefit of ARRC and its successors and assigns that no part of its work product for ARRC will infringe any patent rights or copyrights or utilize any proprietary, confidential or trade secret information or other intellectual property for which Contractor does not have the unqualified right to grant ARRC the license and sublicensing rights referred to above. Contractor shall defend, indemnify and hold harmless ARRC, its successors and assigns, and their respective representatives, agents and employees from and against, any and all claims, defenses, obligations and liabilities which they may have or acquire under or with respect to any patent, copyright, trade secret, proprietary or confidential information, or any other form of intellectual property that may be asserted by Contractor or any other person which arises out of, results from or is based upon the manufacture, use or sale by ARRC or any of its successors or assigns of any of Contractor's work product for ARRC. ARRC shall have the right to select its legal counsel and control its defense in any litigation resulting from any such claim.

10. Governing Law. This contract, and all questions concerning the capacity of the parties, execution, validity (or invalidity) and performance of this contract, shall be interpreted, construed and enforced in all respects in accordance with the laws of the State of Alaska.

11. Alaska Executive Branch Ethics Act Requirements. No officer or employee of the State of Alaska or of the ARRC and no director of the ARRC or legislator of the state shall be admitted to any share or part of this contract or to any benefit that may arise therefrom. Contractor shall exercise reasonable care and diligence to prevent any actions or conditions which could be a violation of Alaska Statute 39.52 et seq. Contractor shall not make or receive any payments, gifts, favors, entertainment, trips, secret commissions, or hidden gratuities for the purpose of securing preferential treatment or action from or to any party. This obligation will apply to the activities of Contractor’s employees and agents in their relations with ARRC employees, their families, vendors, subcontractors, and third parties arising from this contract and in accomplishing work hereunder. Certain gratuities may be given or accepted if:

(1) There is no violation of any law or generally accepted ethical standards;

(2) The gratuity is given as a courtesy for a courtesy received and does not result in any preferential treatment or action;

(3) The gratuity is of limited value (less than$150) and could not be construed as a bribe, payoff or deal; and

(4) Public disclosure would not embarrass ARRC.

ARRC may cancel this contract without penalty or obligation in the event Contractor or its employees violate the provisions of this section.

12. Non-Disclosure of Confidential Information. Contractor acknowledges and agrees that for and during the entire term of this contract, any information, data, figures, projections, estimates, reports and the like received, obtained or generated by Contractor pursuant to the performance of this contract shall be considered and kept as the private, confidential and privileged records of ARRC and will not be divulged to any person, firm, corporation, regulatory agency or any other entity except upon the prior written consent of ARRC. Furthermore, upon termination of this contract, Contractor agrees that it will continue to treat as private, privileged and confidential any information, data, figures, projections, estimates, reports and the like

received, obtained or generated by Contractor during the term of the contract and will not release any such information to any person, firm, corporation, regulatory agency or any other entity, either by statement, deposition or as a witness except upon the express written authority of ARRC. ARRC shall be entitled to an injunction by any competent court to enjoin and restrain the unauthorized disclosure of such information.

Contractor's agreement of non-disclosure as specified in this section applies except to the extent required for (1) performance of services under this contract; (2) compliance with professional standards of conduct for preservation of the public safety, health, and welfare (so long as Contractor has given ARRC prior notice of the potential hazard and ARRC has had a reasonable opportunity to correct the hazard prior to disclosure); (3) compliance with a court order or subpoena directed against Contractor (so long as Contractor has given ARRC prior notice of such and ARRC has had an opportunity to contest the same in a court of law); or (4) Contractor's defense against claims arising from performance of services under this contract.

13. Covenant Against Contingent Fees. Contractor warrants that it has not employed or retained any company or person, other than a bona fide employee working solely for Contractor, to solicit or secure this contract, and that it has not paid or agreed to pay any person, company, individual, or firm any commission, gift, percentage, fee, contingent upon or resulting from the award or making of this contract. For the breach or violation of this warranty, ARRC may terminate this contract without liability and, at its discretion, deduct from the contract price or otherwise recover the full amount of the commission, percentage, gift, or fee.

14. Standard of Performance. Contractor shall perform its services with care, skill and diligence in accordance with normally accepted industry standards and shall be responsible for the professional quality, technical accuracy, completeness, and coordination of all reports, designs, drawings, plans, information, specifications and other items and services furnished under this Contract. Contractor shall comply with all applicable federal, state and local laws and ordinances, codes, and regulations in performing its services. If any failure to meet the foregoing standard of performance appears within one (1) year after the services are accepted by ARRC, Contractor shall, at a minimum, re-perform the work at no cost to ARRC and shall reimburse ARRC for any additional costs that may be incurred by ARRC or any of its contractors or subcontractors as a result of such substandard work. If Contractor should fail to re-perform the work, or if ARRC determines that Contractor will be unable to correct substandard services before the time specified for completion of the project, if any, ARRC may correct such unsatisfactory work itself or by the use of third parties and charge Contractor for the costs thereof. The rights and remedies provided for in this section are in addition to any other remedies provided by law.

15. Warranty. In the event Contractor supplies equipment, goods, materials or other supplies in addition to services under this contract, Contractor warrants that said items: (a) shall be of good quality and free from all defects and deficiencies in workmanship, material and design; (b) shall be fit, suitable and operate successfully for their intended purpose; (c) shall be new; (d) shall be free from all liens, claims, demands, encumbrances and other defects in title; and (e) shall conform to the specifications, if any, stated in the contract. Contractor shall honor all guarantees and warranties offered by the manufacturer of the equipment, goods, materials or other supplies provided under this contract. The rights and remedies provided for in this section are in addition to any other remedies provided by law.

16. Indemnification. Contractor shall defend, indemnify and hold ARRC harmless from and against all claims and actions asserted by a third party (or parties) and related damages, losses

and expenses, including attorney's fees, arising out of or resulting from the services performed or neglected to be performed by Contractor or anyone acting under its direction or control or in its behalf in the course of its performance under this contract and caused by any error, omission or negligent act, provided that Contractor's aforesaid indemnity and hold harmless agreement shall not be applicable to any liability based upon the independent negligence of ARRC. If there is a claim of, or liability for, the joint negligent error or omission of the Contractor and the independent negligence of ARRC, the indemnification and hold harmless obligation shall be apportioned on a comparative fault basis. The term "independent negligence" is negligence other than ARRC's selection, administration, monitoring, or controlling contractor and in approving or accepting Contractor's work.

17. Insurance. Without limiting Contractor's indemnification, it is agreed that Contractor shall purchase at its own expense and maintain in force at all times during the performance of services under this contract the following policies of insurance. Where specific limits are shown, it is understood that they shall be the minimum acceptable limits. If the Contractor's policy contains higher limits, ARRC shall be entitled to coverage to the extent of such higher limits. Certificates of Insurance must be furnished to the ARRC contracting officer prior to beginning work and must provide for a 30-day prior notice of cancellation, non-renewal or material change. Failure to furnish satisfactory evidence of insurance or lapse of the policy is a material breach and grounds for termination of the Contractor's services.

17.1 Workers' Compensation Insurance: The Contractor shall provide and maintain, for all employees of the Contractor engaged in work under this contract, worker's compensation insurance as required by applicable law. The Contractor shall be responsible for worker's compensation insurance for any subcontractor who directly or indirectly provides services under this contract. This coverage must include statutory coverage for states in which employees are engaging in work and employer's liability protection not less than $100,000 per person, $100,000 per occurrence. Where applicable, coverage for all federal acts (i.e. U.S.L. & H. and Jones Acts) must also be included.

17.2 Comprehensive (Commercial) General Liability Insurance: With coverage limits not less than $1,000,000 combined single limit per occurrence and annual aggregates where generally applicable and shall include premises-operations, independent contractors, products/completed operations, broad form property damage, blanket contractual and personal injury endorsements. Said policy shall name ARRC as an additional insured and contain a waiver of subrogation against ARRC and its employees.

17.3 Comprehensive Automobile Liability Insurance: Covering all owned, hired and non-owned vehicles with coverage limits not less than $100,000 per person/$300,000 per occurrence bodily injury and $50,000 property damage. Said policy shall name ARRC as an additional insured and contain a waiver of subrogation against ARRC and its employees.

17.4 Professional Liability (E&O) Insurance: Covering all errors, omissions or negligent acts of the Contractor, its subcontractor or anyone directly or indirectly employed by them, made in the performance of this contract which result in financial loss to ARRC. Limits required are per the following schedule:

Contract Amount	Minimum Required Limits
Under $100,000	$ 500,000 per Occurrence/Annual Aggregate
$100,000-$499,999	$1,000,000 per Occurrence/Annual Aggregate

$500,000-$999,999	$2,000,000 per Occurrence/Annual Aggregate
Over $1,000,000	Negotiable-Refer to Risk Management

18. ARRC's Rights Not Waived by Payment. No payment made by ARRC shall be considered as acceptance of satisfactory performance of Contractor's obligations under this contract. Nor shall any payment be construed as acceptance of substandard or defective work or as relieving Contractor from its full responsibility under the contract.

19. Nonwaiver. A party's failure or delay to insist upon strict performance of any of the provisions of this contract, to exercise any rights or remedies provided by this contract or by law, or to notify the other party of any breach of or default under this contract shall not release or relieve the breaching or defaulting party from any of its obligations or warranties under this contract and shall not be deemed a waiver of any right to insist upon strict performance of this contract or any of the rights or remedies as to any subject matter contained herein; nor shall any purported oral modification or rescission of this contract operate as a waiver of any of the provisions of this contract. The rights and remedies set forth in any provision of this Agreement are in addition to any other rights or remedies afforded the nonbreaching or nondefaulting party by any other provisions of this contract, or by law.

20. Savings Clause. If any one or more of the provisions contained in the contract shall, for any reason, be held to be invalid, illegal or unenforceable in any respect, such invalidity, illegality or unenforceability shall not affect any other provisions of this contract, but this contract shall be construed as if such invalid, illegal or unenforceable provision had never been contained herein.

21. Headings. The headings of sections and paragraphs of this contract are for convenience of reference only and are not intended to restrict, affect, or be of any weight in the interpretation or construction of the provisions of such sections or paragraphs.

22. Forum Selection. The parties shall not commence or prosecute any suit, proceeding or claim to enforce the provisions of the contract, to recover damages for breach or default under the contract, or otherwise arising under or by reason of the contract, other than in the courts of the State of Alaska for the Third Judicial District at Anchorage. The parties hereby irrevocably consent to the jurisdiction of said courts.

23. Conflict of Interest. Contractor shall act to prevent any actions or conditions which could result in a conflict with ARRC's best interests. This obligation shall apply to the activities of Contractor's employees and agents in their relationships with ARRC's employees, their families, vendors, subcontractors and third parties accomplishing work under this contract.

24. Publicity. Contractor shall not release any information for publication or advertising purposes relative to this contract or to the material, equipment and/or services furnished under this contract without the prior written consent of the ARRC.

25. Audit. ARRC has the right to audit at reasonable times the accounts and books of the Contractor in accordance with the provisions of ARRC Procurement Rule 1600.10.

26. Internal Controls and Record Keeping. Contractor shall keep full and accurate records and accounts of all of its activities in connection with this contract, including, without limitation, reasonable substantiation of all expenses incurred and all property acquired hereunder.

27. Force Majeure. Neither ARRC nor Contractor shall be responsible for failure to perform the terms of this contract when performance is prevented by force majeure, provided that: (1) notice and reasonably detailed particulars are given to the other party and (2) the cause of such failure or omission is remedied so far as possible with reasonable dispatch. The term "force majeure" shall mean acts of God, earthquakes, fire, flood, war, civil disturbances, governmentally imposed rules, regulations or other causes whatsoever, whether similar or dissimilar to the causes herein enumerated, which is not within the reasonable control of either party and which through the exercise of due diligence, a party is unable to foresee or overcome. In no event shall force majeure include normal or reasonably foreseeable or reasonably avoidable operational delays.

28. Permits and Licenses. The Contractor shall, at its own expense, obtain all necessary permits, licenses, certifications and any other similar authorizations required or which may become required by the government of the United States or any state or by any political subdivision of the United States or of any state except where laws, rules or regulations expressly require the ARRC to obtain the same.

29. Environmental Protection. When performing all obligations under the contract, Contractor shall comply with all specific instructions of ARRC with regard to environmental concerns, regardless of whether such instructions are based upon specific law, regulation or order of any governmental authority.

30. Set Off. If ARRC has any claim against the Contractor related or unrelated to this contract, it may set off the amount of such claim against any amount due or becoming due under this contract.

31. Observance of Rules. The contractor's personnel performing work or services hereunder on ARRC's premises shall observe all fire prevention, security, and safety rules in force at the site of the work.

32. No Third-Party Beneficiary Rights. No provision of this contract shall in any way inure to the benefit of any third parties (including the public at large) so as to constitute any such person a third-party beneficiary of the contract or of any one or more of the terms hereof, or otherwise give rise to any cause of action in any person not a party hereto.

33. Entire Agreement. This contract represents the entire and integrated agreement between ARRC and the Contractor and supersedes all prior negotiations, representations, or agreements, either written or oral. This contract may be amended only by a written instrument signed by both ARRC and the Contractor.

34. Key Personnel Changes. Contractor shall secure prior written approval from ARRC for any changes of key personnel assigned to perform services under this contract. ARRC reserves the right to reject any of Contractor's employees whose qualifications and/or experience in ARRC's good faith and reasonable judgment do not meet the standards necessary for the performance of the services required under this contract.

ATTACHMENET #1

Events & Storage

Device Type	Quantity
Windows Active Directory Servers	4
Windows IIS and Exchange Servers	3
Windows General Purpose Servers	140
UNIX and Linux Servers	2
DNS and DHCP Servers	5
Antivirus Servers	4
Database Servers	18
Proxy Servers	2
Large Firewalls	3
Small Firewalls	2
IDS, IPS, and DAM	3
VPNs	10
Access Points, Routers and Switches	120

Flows

Device Type	Quantity
Total Workstations on Network	400
Total Servers on Network	180

NetFlow

Type & Bandwidth	
Number of Internet Connections	2
Total Bandwidth of Internet Connection	30Mb
Typical Bandwidth between any Remote Sites	1Gb

Additional Log Sources

Device Type	Quantity
IBM i	12
DS4700 SAN	5
V7000 SAN	1
HP SAN	15
Wireless	50
SCADA	150

PTC related Log Source Sites and Equipment

Device Type	Quantity
Cisco Switches / Routers (May need to be captured at ASA location in main facilities)	111
IP Phone/IP Radio (May need to be captured at ASA location in main facilities)	111
Battery Backups (May need to be captured at ASA location in main facilities)	111

Selection Criteria for a SIEM Solution

REQUIREMENTS

This section details the unique features and functionality that should be considered when evaluating competitive Security Intelligence offerings. Each unique feature and/or functionality is associated with an ID number for reference. All requirements will be categorized by three 'levels' of requirements. These are:

The solution **[]**

Must

> Requirements identified as '**MUST**' will carry the heaviest weight in evaluation. The solution MUST display the ability to address this requirement to be considered.

Should

> Requirements identified as '**SHOULD**' will carry a medium weight in evaluation. The solution SHOULD demonstrate the ability to address all or part of the requirement.

May

> Requirements identified as '**MAY**' will carry the lowest weight in evaluation. The solution MAY demonstrate the ability to address all or part of the requirement.

Responses to requirements listed within this section should pertain to currently shipping product only. If a feature requirement is met in a future release, please indicate as 'Roadmap' in the response section and discuss this capability in that portion of the document.

(Note: All responses in this template have been defined as a "**must**" category. The template can be adjusted to reflect an organization's unique requirements)

PLATFORM CONSIDERATIONS

It is important to ensure that the chosen solution meets both immediate tactical requirements (i.e. log management to meet specific compliance requirements) and longer term strategic requirements, which will vary by organization but may include: security information and event management (SIEM), network activity monitoring, advanced threat detection, vulnerability monitoring, and/or risk management, among other things.

The following proposal defines requirements for the selection of Security Intelligence Solution. It has been broken into multiple logically connected sections. Please respond on how the solution being considered meets each of the following requirements.

1. ADMINISTRATION & CONFIGURATION

Administration and configuration functions are an integral part of any security or network intelligence solution. From installation to ongoing maintenance the solution should present the ability to be easily managed and configured.

The following are the administration and configuration requirements of the system:

#	Requirement		Response	
1.1	The Security Intelligence solution **must** provide central management of all components and administrative functions from a single web based user interface. Please describe how your solution meets this requirement.			
1.2	The administrator **must** be able to define role base access to the system by device, device group or network range. This includes being able restrict a users access to information to only those systems from a specific group of devices or network range. Please describe how your solution meets this requirement.			
1.3	The administrator **must** be able to define role based access to various functional areas of the solution. This includes being able			

	to restrict a users access to specific functions of the solution that is not within the scope of a users role including, but not limited to, administration, reporting, event filtering, correlation, and/or dashboard viewing. Please describe how your solution meets this requirement.			
1.4	The solution **must** support auto discovery of assets that are being protected or monitored. Please describe how your solution meets this requirement.			
1.5	The solution **should** support automated classification of assets that are being protected Please describe how your solution meets this requirement.			
1.6	The solution **must** support the detachment of selected dashboards from the UI for use in SOC or NOC deployments. Please describe how your solution meets this requirement.			
1.7	The vendor of the Security Intelligence solution **should** provide and foster community oriented information and experience sharing among users of the security intelligence solution. Describe your companies approach to this requirement.			
1.8	The solution **should** support the ability to modify communications ports between components. Please describe how your solution meets this requirement.			
1.9	The solution **must** provide an open API, ODBC or other method for access to data stored within the information database(s). Please describe how your solution			

	meets this requirement.			
1.10	The solution **must** provide the ability to encrypt communications between components. Please describe how your solution meets this requirement.			
1.11	The solution **must** integrate with 3rd party directory systems as an authentication method. How does your solution integrate with a LDAP or AD solution for access provisioning to the SIEM system?			

2. OPERATIONAL REQUIREMENTS

This section details the operational requirements of the solution. This section details the requirements from the perspective of 'day-to-day' operations.

The following sections detail the requirements for the operational aspects of the solution:

#	Requirement		Response	
2.1	The solution **must** enable a phased role out of log management and security intelligence functions. Introduction of more analysis capabilities should minimize the need for additional system components and be enabled through license key upgrades. Please describe how your solution meets this requirement.			
2.2	The solution **may** provide a framework for future expansion and integration with other 3rd part solutions. Please describe how your solution meets this requirement.			
2.3	The solution **must** demonstrate 'ease of use'. Ease of use is critical to the successful deployment and on-going use of the solution. Describe the ease of			

	use considerations and implementations within the solution.			
2.4	The solution **must** support the automatic update of configuration information with minimal user intervention. For example, security taxonomy updates, vendor rule updates, device support, etc. Describe how the solution provides this functionality and detail the features that are updated.			
2.5	The solution **must** support a web-based GUI for management, analysis and reporting. Please describe how your solution meets this requirement.			
2.6	The solution **should** support high availability requirements in an embedded fashion and without the need for additional 3rd party software. Please explain meets this requirement to provide 24x7 availability and fault tolerance?			
2.7	The solution **must** ensure all distributed system components continue to operate when any other part of the system fails or loses connectivity. (i.e., management console goes off-line all separate collectors still continue to capture logs). Please describe how your solution meets this requirement.			
2.8	The solution **should** have an automated backup/recovery process. Please describe how your solution meets this requirement.			
2.9	The solution **must** automate internal health checks and notify the user when problems arise.			

	Please describe how your solution meets this requirement.			
2.10	The solution **should** provide the ability to deliver multiple dashboards that can be customized to meet the specific requirements of different users of the system. Please describe how your solution meets this requirement.			
2.11	The solution **must** deliver sample dashboards out of the box (i.e. for threat management, compliance management, etc.). Please describe how your solution meets this requirement.			
2.12	The solution **should** deliver customizable dashboard widgets that can present relevant security information to the users of the system (i.e. event views, network activity views, incident views, etc.). Please describe how your solution meets this requirement.			
2.13	The solution **must** maintain an externally accessible store or database of all assets discovered on the network. This asset data should include important information about the asset as learned by the information collected (i.e. system attributes, network attributes, vulnerability state, etc.). The database must provide the ability to edit attributes when they cannot be learned (i.e. department, location, etc.). The user must be able to search this database. Please describe how your solution meets this requirement.			

3. ARCHITECTURAL REQUIREMENTS

Overall solution architecture is a key consideration in the selection of a security or network intelligence solution.

The following are the architectural requirements of the system:

#	Requirement		Response	
3.1	The solution **must** enable deployments as software and/or appliance. Please describe how your solution meets this requirement.			
3.2	The solution **must** integrate with other security and network intelligence solutions. Describe the level of integration and solutions supported.			
3.3	The Security Intelligence solution **must** allow for customization to meet our unique requirements. Please describe how your solution meets this requirement.			
3.4	The solution **must** easily expand to support additional demand. How does your solution scale to increase demand placed on the solution as the organization adds more devices, locations, applications, etc? Please describe the impact to each of the proposed components of your solution (i.e. appliances, storage, management consoles, etc.)			
3.5	The solution **should** support a distributed database for event and network activity collection such that all information can be access from a single UI. Please describe how your solution meets this requirement.			
3.6	The solution **should** ensure the integrity of the information collected. What mechanisms			

	does the solution provide to meet this requirement?			
3.7	The solution **must** provide intuitive mechanisms for troubleshooting such as proactive notifications, command line utilities etc.			
3.8	The solution **may** support a distributed model for correlation such that counters, sequences, identity lookups, etc… are shared across all collectors. (i.e., look for 25 login failures from the same user name followed by a single successful login for that same user name, where events seen by a single collector do not exceed the threshold of 25, but across multiple collectors would exceed the threshold). Please describe how your solution meets this requirement.			
3.9	The solution **should** support user extended taxonomy of events and fields. The user must be able to add their own unique event names (i.e., the ability to add in new fields that are not part of the vendors out of the box schema such as a failed called “SpecialID from my Custom Application”). Please describe how your solution meets this requirement.			
3.10	The solution **must** allow for custom defined tagging of events. Please describe how your solution meets this requirement.			
3.11	The solution **should** provide transparent retrieval, aggregation, sorting, filtering and analysis of data across all distributed components. Please describe how your solution meets this requirement.			

4. LOG MANAGEMENT REQUIREMENTS

Log management functions are an integral part of any security or network intelligence solution.

The following are the log management requirements of the system:

LOG COLLECTION, RETENTION, AND PROCESSING

#	Requirement		Response	
4.1	The solution **must** have a log collection and archive architecture that supports both short-term (online) and long-term (offline) event storage. How does your solution manage, store, and archive the log data?			
4.2	The solution **may** support log archives on 3rd party storage. Please describe how your solution meets this requirement.			
4.3	The solution **should** provide capabilities for efficient storage and compression of collected data. Please describe how your solution meets this requirement.			
4.4	The solution **must** support industry log collection methods (syslog, WMI, JDBC, SNMP, Checkpoint LEA, etc.)? Please describe what collection methods are available in your solution.			
4.5	The solution **should** provide agent-less collection of event logs whenever possible. Does your solution rely on agent technology? If so, please describe how this is used to collect and aggregate event data?			
4.6	The solution **may** provide the ability to distribute both event storage and processing across the entire Log Management/SIEM			

	deployment. Explain how your architecture will support this requirement.			
4.7	The solution **should** support long-term access to detailed security event and, if available, network flow data. The system **should** be able to provide access to at least x month's worth of detailed information. Describe how the system provides access to this information.			

5. LOG NORMALIZATION & CATEGORIZATION

#	Requirement		Response	
5.1	The solution **must** normalize common event fields (i.e. usernames, IP addresses, hostnames, and log source device, etc.) from disparate devices across a multi-vendor network. Please describe how normalization is performed and the standard event fields that are normalized out-of-the-box.			
5.2	The solution **may** provide a common taxonomy of events. Please describe how this is provided by the solution the standard event categories that are provided out-of-the-box.			
5.3	The solution **must** provide the ability to store/retain both normalized and the original raw format of the event log for forensic purposes. Please describe how this requirement is met by the solution.			
5.4	The solution **may** provide the ability to normalize and aggregate event fields that are not represented by the out-of-the-box			

	normalized fields. Please describe how this requirement is met by the solution.			
5.5	The solution **should** support/normalize event time stamps across multiple time zones. Describe you this requirement is met by the solution.			

6. EVENT FILTERING & ANALYSIS

#	Requirement		Response	
6.1	The solution **must** provide near-real-time analysis of events. Please describe how this requirement is met by the solution.			
6.2	The solution **must** provide long term trend analysis of events. Please describe how this requirement is met by the solution.			
6.3	The solution **must** provide the ability to aggregate and analyze events based on a user specified filter. Please describe how this requirement is met by the solution.			
6.4	The solution **should** provide more advanced event drill down when required. Please describe how this requirement is met by the solution.			
6.5	The solution **should** provide a real-time streaming view that supports full filtering capabilities. Please describe how this requirement is met by the solution.			
6.6	The solution **must** provide alerting based on observed anomalies and behavioral changes in network and security events. Please describe how this requirement is			

	met by the solution.			
6.7	The solution **must** support and maintain a history of user authentication activity on a per asset basis. Please describe how your solution meets this requirement.			

7. REPORTING

#	Requirement		Response	
7.1	The solution **should** provide reporting on all items available for management via the GUI. Describe how the solution provides the ability to configure reports.			
7.2	The solution **should** provide configurable reporting engine for customized report creation or 3rd party reporting integration. Please describe how your solution meets this requirement.			
7.3	The solution **must** support the ability to schedule reports. Describe the mechanisms and frequency at which reports can be scheduled.			
7.4	The solution **should** provide templates for the easy creation and delivery of reports at multiple levels ranging from operations to business issues. Please describe the process for creating reports and the number of available reports.			
7.5	The solution **should** provide 'canned' out-of-the-box reports for typical business and operational issues. Describe the reports and report types available.			

7.6	The solution **should** provide 'canned' out-of-the-box reports for specific compliance regulations (PCI, SOX, FISMA) and control frameworks including (NIST, CoBIT, ISO). Please describe how your solution meets this requirement.			
7.7	The solution **must** provide a 'Dashboard' for quick visualization of security and network information. Please describe the components available in the dashboard and the frequency at which this information refreshes.			
7.8	The solution **must** support the automated distribution of reports. Describe the mechanisms used to distribute reports.			
7.9	The solution **must** support the capability to provide historical trend reports. Please describe how your solution meets this requirement.			
7.10	The solution **must** support the ability to centrally deliver vulnerability reports. Please describe how your solution meets this requirement.			
7.11	The solution **may** support the ability to centrally deliver asset reports. Please describe how your solution meets this requirement.			

8. SIEM REQUIREMENTS

From simple correlation to comprehensive network activity monitoring to advanced threat detection and response the solution should present the ability to leverage all data collected to its fullest potential.

The following are the SIEM requirements of the system:

9. CORRELATION AND ALERTING

#	Requirement		Response	
9.1	The solution **must** provide alerting based on observed security threats from monitored devices. Please describe how your solution meets this requirement.			
9.2	The solution **must** provide the ability to correlate information across potentially disparate devices. Please describe how your solution meets this requirement.			
9.3	The solution **must** provide alerting based on observed anomalies and behavioral changes in network activity (flow) data. Describe any pre-packaged alerts and method for adding user-defined anomaly and behavior alerts.			
9.4	The solution **must** provide alerting based upon established policy. (e.g., IM traffic is not allowed.) Describe the solutions ability to alert on policy violations.			
9.5	The solution **may** support weighted alerts to allow for prioritization. Weights must be assignable based on multiple characteristics such as asset type, protocol, application, etc. Describe how the solution supports weighted alerts and the structure of assigning weights.			
9.6	The solution **should** provide the ability to transmit alerts using multiple protocols and mechanisms to other management solutions			
9.7	The solution **should** provide UI based wizard and capabilities to minimize false positives and			

	deliver accurate results. Please describe how your solution meets this requirement.			
9.8	The solution **must** limit the presentation of multiple similar alerts. Describe the solutions ability to minimize duplicate alarms.			
9.9	The solution **must** support the ability to take action upon receiving an alert. For example, the solution should support the ability to initiate a script or send an email message. Please describe how your solution meets this requirement.			
9.10	The solution **must** support the ability to correlate against 3rd party security data feeds (i.e. geographic mapping, known botnet channels, known hostile networks, etc.). These 3rd party data feeds should be updated automatically by the solution. Please describe how your solution meets this requirement.			
9.11	The solution **may** support the ability to correlate against 3rd party vulnerability scan results. Please describe how your solution meets this requirement.			
9.12	The solution **should** monitor and alert when there is a disruption in log collection from a device. In other words, if logs are not seen from a server in X minutes then generate an alert. Please describe how your solution meets this requirement.			
9.13	The solution **may** provide an out of the box mechanism to discover and classify assets by system type (i.e. mail servers vs. data base			

	servers) to minimize false positives associated with poor asset classification. Please describe how your solution meets this requirement.			
9.14	The solution **may** support correlation for a missing sequence. Example service stopped not followed by the service restarting within 10 minutes. Please describe how your solution meets this requirement.			
9.15	The solution **should** support correlation for additive values over time. For example, alert when any SRC IP sends more than 1GB of data to a single port on a single DST IP in a one hour period of time. Please describe how your solution meets this requirement.			
9.16	The solution **should** provide a mechanism, to optimize rule tuning, which allows for the grouping of similar input values of a correlation rule that can be used by multiple rules. This grouping mechanism should allow for both static groups and groups that are dynamically created by other correlation rules. For example, the user of the system can define a group of banned ports/protocols that should be used across multiple correlation rules that monitor for inappropriate network activity. Please describe how your solution meets this requirement.			

10. NETWORK ACTIVITY MONITORING

#	Requirement		Response	
10.1	The solution **should** display visual traffic profiles in terms of bytes,			

	packet rates and number of hosts communicating. These displays **should** be available for applications, ports, protocols, threats and each monitoring point in the network. All of these views **must** support network location specific view such that they can present information from a single location, the entire network or any other defined grouping of hosts. Please describe how your solution meets this requirement.			
10.2	The solution **should** support application definition beyond protocol and port. The system **should** support the identification of applications using ports other than the well-known, and applications tunneling themselves on other ports (e.g., HTTP as transport for MS-Instant Messenger should be detected as Instant messenger - not HTTP). Please describe how your solution meets this requirement.			
10.3	The solution **must** detect "zero-day" events. Describe how the solution detects and displays this information.			
10.4	The solution **should** dynamically learn behavioral norms and expose changes as they occur. Detail the methods used by the solution and the method by which anomalies are displayed.			
10.5	The solution **must** detect denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Describe how the solution detects and displays this information.			
10.6	The solution **must** detect and present views of traffic pertaining to observed threats in the network.			

	Describe the types of threats and visualizations for this information in the Security Intelligence system.			
10.7	The solution **should** profile traffic by TCP and UDP port. Please describe how your solution meets this requirement.			
10.8	The solution **should** support traffic profiling associated with logical network design (e.g., Subnet/CIDR). Please describe how your solution meets this requirement.			
10.9	The solution **must** identify network traffic from potentially risky applications (e.g. file sharing, peer-to-peer, etc.). Please describe how your solution meets this requirement.			
10.10	The solution **may** display traffic profiles in terms of packet rate. This capability **should** be available for simple TCP analysis (TCP Flags, etc) but rate-based information may be presented for other profiles (e.g., applications). Please describe how your solution meets this requirement.			
10.11	The solution **may** profile and present information in multiple timeframes. Profiles **should** be available for week, day and hour. Describe the maximum and minimum timeframes available for profiling and analysis.			
10.12	The solution **may** be able to profile communication originating from or destined to the internet by Geographic regions in real-time. Describe how this is accomplished.			

10.13	The solution **must** create clearly independent and differentiated profiles from local traffic vs traffic originating or destined for the internet. Please describe how your solution meets this requirement.			
10.14	The solution **should** allow the user to create custom profiles and views using any property of a flow, log, data source or already profiled traffic. Describe how the Security Intelligence system supports this level of customization.			
10.15	The solution **should** support traffic profiling based on IP addresses, groups of IP addresses, source/destination IP pairs etc. Please describe how your solution meets this requirement.			
10.16	The solution **must** support the collection and analysis of packet capture data. Please describe how your solution meets this requirement.			
10.17	The solution **should** provide the ability to extract specific, user defined, fields from packet capture data and use the fields in correlation rules. Please describe how your solution meets this requirement.			
10.18	The solution **should** identify network traffic within a virtual network environment. Please describe how your solution meets this requirement.			

11. ADVANCED THREAT MANAGEMENT

#	Requirement		Response	
11.1	The solution **should** provide the ability to contextually link application activity on the network with security events from monitored devices. Explain how the solution uses network knowledge to validate security events.			
11.2	The solution **must** provide the ability to contextually link reported security events with real-time knowledge of the assets that are being targeted. Explain how the solution uses knowledge of assets within the network to validate security			
11.3	The solution **must** provide the ability to automatically weight the priority of reported security events according to the relative importance of the targeted asset. Please explain how this is accomplished			
11.4	The solution **should** provide the ability to automatically weight the severity of reported security events according to the vulnerability of the targeted assets. Please explain how asset profiles are used to prioritize events			
11.5	The solution **may** provide the ability to assign credibility ratings to monitored security devices. Please describe how your solution meets this requirement.			
11.6	The solution **may** provide a real-time event view of monitored information in raw/original as well as processed/parsed format. Please describe how your solution meets this requirement.			

11.7	The solution **may** be able to automatically change the credibility weightings of security devices in response to network-wide attacks. Please describe how your solution meets this requirement.			

12. SIEM WORKFLOW

#	Requirement		Response	
12.1	The solution **must** provide ability to send notification of correlated alerts via well defined methods (i.e. SNMP trap, email, etc.)? Please describe how your solution meets this requirement.			
12.2	The solution **should** provide embedded workflow capability that security operations staff can use to guide their work? Please describe how your solution meets this requirement.			
12.3	The solution **should** provide bi-directional integration with 3rd party trouble ticketing/help desk systems that security operations staff may use to guide their work? Please describe how your solution meets this requirement.			
12.4	The solution **must** provide a mechanism to capture all relevant aspects of a security incident in a single logical view. This view should include relevant events, network activity data, correlated alerts, vulnerability data, etc.. Please describe how your solution meets this requirement.			
12.5	The solution **must** provide a mechanism to annotate a security incident as it is addressed by the security operations staff. Please			

	describe how your solution meets this requirement.			
12.6	The solution **must** provide a mechanism to track security incidents across a wide range of relevant attributes (i.e. IP addresses, usernames, MAC address, log source, correlation rules, user defined, etc.). The user **must** be able to filter incidents along these defined attributes. Please describe how your solution meets this requirement.			

13. DATA SOURCE REQUIREMENTS

Supporting all possible network and security devices is an integral part of any security or network intelligence solution.

The following are the data source requirements of the system:

#	Requirement		Response	
13.1	The solution **must** support the following vendor products.			
	Windows Server Windows Workstations Mobile devices AIX Servers Linux Servers/workstations IBM I Servers Cisco IBM DS4700 IBM V7000 HP SAN			

	Cisco ASA Industrial power, access control systems			
13.2	The solution **must** support information collected from Microsoft based servers and end-user systems. Please describe your level of support for this type of product.			
13.3	The solution **must** support information collected from Linux/Unix based servers and end-user systems. Please describe your level of support for this type of product.			
13.4	The solution **must** support information collected from mainframe servers. Please describe your level of support for this type of product.			
13.5	The solution **must** support information collected from enterprise class database solutions. Please describe your level of support for this type of product.			
13.6	The solution **must** support information collected from commercial applications (i.e. JD Edwards, SQL Server, Oracle, IBM DB/2 400, WebSphere, Web, etc.). Please describe your level of support for this type of product.			
13.7	The solution **must** support information collected from Data Leak Protection (DLP) Security software and tools. Please describe your			

	level of support for this type of product.			
13.8	The solution **may** support information collected from proprietary applications. Please describe your level of support for this type of product.			
13.9	The solution **should** support information collected for Database Activity Monitoring (DAM) Security software and tools. Please describe your level of support for this type of product.			
13.10	The solution **should** support information collected from File Integrity/Activity Monitoring (FIM/FAM) Security software and tools. Please describe your level of support for this type of product.			
13.11	The solution **should** support information collected from Identity and Access Management Security software and tools (IAM). Please describe your level of support for this type of product.			
13.12	The solution **must** support information collected from Directories (i.e. AD, LDAP) products. Please describe your level of support for this type of product.			
13.13	The solution **must** support information collected from Network flows (i.e. Netflow, J-Flow, S-Flow etc.) products. Please describe your level of support for this			

	type of product.			
13.14	The solution **should** support information collected from network management systems (i.e. McAfee ePolicy Orchestrator, Microsoft MOM, etc.). Please describe your level of support for this type of product.			
13.15	The solution **must** support information collected from Network infrastructure (i.e. switches, routers, etc.). Please describe your level of support for this type of product.			
13.16	The solution **must** support information industry leading vulnerability scanners. Please describe your level of support for this type of product.			

DOCUMENT NOTES: **Please answer the below questions as completely and accurately as possible.**			
ID	**Category**	**Description**	**Response: Please indicate how your solution / company would address the stated need or question**
1.00	**SIEM ABILITIES (Security information and event management)**		
1.01	**Inputs & Access Controls**	What types of inputs/devices can the tool accept? e.g. NetFlow, Syslog, SNMP, Windows, Linux, Applications(AV and Websense) How does the system collect data from proprietary or legacy event sources? How do you provide software based deployments with centralized management? How does the tool leverage Windows Unified Connector? How does the system recognize privileged users?	
1.02	**Normalization/Categorization**	How do you pre-normalize the data before its written to a database? How many dimensions are categorized? (i.e. device type, behavior, outcome, etc.)	
1.03	**Proactive alerting and monitoring**	Besides reactive monitoring what can the tool tell us about network activity in real time? 1) How do you provide geo-IP lookup, port to application mapping, model mapping, and custom field mapping pre-correlation? 2) Global threats and how are we prepared? 3) What services or capabilities does the vendor provide for incident analysis or investigation?	
1.04	**Transactional Assurance/Audit & Accountability**	How do you guarantee event integrity, confidentiality, and availability? (i.e. how does the system monitor and alert when original event source syops sending log data)	
1.05	**Full Text Search**	How does your tool index both unstructured and structured data? How many events per second can the tool return search results for?	
1.06	**Centralized Log Storage**	How many TB's of log data can be stored locally? How do use classification of data to segregate security, compliance, IT operations, etc.?	
1.07	**Linear Scalability**	How many events per second can a single appliance scale to? How do you search across multiple peers without first having to centralize and index data store?	
1.08	**Threat Evaluation**	How do you correlate against past activities related to the target or reference the targets current vulnerabilities? How does your tool handle rule creation?	
1.09	**Notification and Workflow**	What is your process framework for integrating security monitoring and investigations into existing workflow procedures? What type of visual accounting do you provide for showing the complete attack life cycle of a threat?	
1.10	**Threat/Incident Response**	How do you trigger scripts or execute integration with third party solutions to quarantine or block nefarious activity in real-time?	
1.11	**Reputation Correlation**	How does your tool detect threats early? (zero day attacks) How does your tool monitor and protect the reputation of a company's website, assets, and partners not found in a bad reputation list?	
1.12	**Compliance Automation**	How does your tool provide real time alerts and reports for compliance regulations such as NIST?	
1.13	**Pattern Detection**	How does your tool detect low-and-slow attacks that are not easily recognized by pre-existing thresholds?	
2.00	**IPS**		

ID	Category	Description	Response: Please indicate how your solution / company would address the stated need or question
2.01	**IPS Analytics**	How do your IPS analytics work? (i.e. how do you gain/foster insight around new and existing threats)	
2.02	**IDS/IPS**	Does the solution include IDS/IPS or does it leverage existing customer deployments? How does this solution integrate with SIEM? How do you deploy multiple devices and polices?	
2.03	**Wireless IDS/IPS**	How do you reduce false positive alerts and use classification and mitigation techniques to block unauthorized wireless traffic without disrupting the performance of authorized wireless devices	
2.04	**Type of detection**	How do you monitor all ports (i.e. 50+ protocols) to protect against all targeted and advanced attacks specific to the network and mail environment. How does this capability integrate with SIEM and other security controls	
2.05	**Real-time network enforcement**	How do you provide zero day vulnerability filters specific to SCADA systems? List your SCADA filters?	
2.06	**Protocol Filters**	How do you provide custom filters? Do you have filters designed specifically for manufacturers, Siemens, Schneider Electric, General Electric, DATAC, WEBTAC, etc. Do you support the major protocols such as MODBUS, DNP3, and ICCP?	
3.00	**Application Protection**		
3.01	**Vulnerability Scans**	How do you provide Static binary and byte code analysis reviews of compiled code, libraries and third party plugins rather than source code? Do you reverse engineer software for binary analysis? How do you provide dynamic scans for applications in production?	
3.02	**Integration**	How do you integrate with IPS, WAF, or SIEM?	
3.03	**Sensitivity of Code**	How do you help organizations who cannot send code off premise and do not have the resources in place to provide security to the Software Development Lifecycle internally?	
3.04	**Automated Tool**	What automated tools do you use for scans and how do you scrub out false positives?	
4.00	**Stateless Key Encryption**		
4.01	**Identification and Authentication**	Does your encryption solution support format-preserving options that enable its use in legacy applications? What encryption formats other than format preserving are available in your solution?	
4.02	**Media Protection**	Does your solution support the tokenization of primary account numbers upon authorization? Please describe your solution? Which encryption algorithms are supported?	
4.03	**Deliver Keys to trusted infrastructure components**	How does your solution enable on demand key generation and re-generation without a key store?	
4.04	**Recover keys**	How does your solution avoid databases for key recovery?	
5.00	**Server Automation**		
5.01	**Configuration Management**	How does your solution help to automate your complete server build	
5.02	**Systems and Information integrity**	How does your solution maintain patch compliance?	
5.03	**Software Deployment**	How do you control sequence of install and uninstall of all object types? How do you add software components to devices or groups? How do you track usage to ensure software is deployed properly? How do reuse polices for deployment, update and compliance?	

ID	Category	Description	Response: Please indicate how your solution / company would address the stated need or question
5.04	**Industry Standard compliance policies**	Does your solution have out of the box and ad hoc compliance reports (FISMA)?	
5.05	**Summarize and analyze software issues**	How do you provide automated change detection, config updates, provisioning and patching?	
6.00	**REPORTING**		
6.01	**Top X Reports**	Please provide information on this solution's ability to create "Top X" reports.	
6.02	**Drill Down**	Does this solution have the ability to drill into actual log sources that generated reporting?	
6.03	**Accuracy**	How do you verify the solution is providing accurate reporting that is reliable and runs in a timely fashion	
6.04	**Report Saving**	Does this solution have the ability to create and save reports in a flexible/free form manner (such as search x device for y string/IP/name/port etc.)	
6.05	**Executive Reporting**	Does the solution provide executive reports that are meaningful and do not need to be explained	
6.06	**Timing**	Are metrics available for time to generate statistics or reports based on the number of log entries?	
6.07	**Samples**	Are sample reports available for review?	
7.00	**COMPLIANCE**		
7.01	**Vulnerability Scanning**	Can this solution provide internal and external vulnerability scanning?	
7.02	**NIST**	How many security controls from NIST 800-53/82 does this solution address and which ones?	
7.03	**PCI Experience**	What experience do you have around PCI. How would you rate your overall competency in this space?	
7.04	**Reporting**	What are your reporting and technical abilities surrounding NIST & PCI?	
8.00	**CAPACITY**		
8.01	**Logs**	How long is log information available for analysis? Are older logs archived? If so, what is the process and time requirements to access them?	
9.00	**ARCHITECTURE**		
9.01	**Supported Installations**	**On-Premise solution:** please provide an architectural overview (preferably a picture) of the ideal implementation of your product, including a description. 1) Integration points 2) Delivery methods / options / requirements **Hosted (SaaS) Solution:** please provide an architectural overview (preferably a picture) of the ideal implementation of your product, including a description of: 1) Integration points 2) Delivery methods / options / requirements **What is your preferred and/or most common installation type?** **What percentage of your customers are using a SaaS solution versus an On Premise solution?**	
9.02	**Time Zones**	Does the system support multiple time zones as standard functionality?	

ID	Category	Description	Response: Please indicate how your solution / company would address the stated need or question
9.03	**Browser Support**	What web browsers does your system support?	
10.00	**ARCHITECTURE - ON PREMISE SOLUTION**		
10.01	**Equipment**	Describe all appliances for an on premise install?	
11.00	**EASE OF USE**		
11.01	**GUI**	Does the tool have a GUI that is simple, fast, and easy to use?	
11.02	**Web Based**	Does the tool run in a web browser without having to load a client?	
11.03	**Tool Complexity**	Is the tool intuitive to use? Would other team members not familiar with network security be able to log into the tool and use it with little training?	
11.04	**C/C++, PHP**	is the tool compatible with C/C++, PHP?	
11.05	**Basic Tool Use**	What is the approximate time required to learn basic GUI interface and develop custom reports?	
12.00	**SYSTEM SECURITY**		
12.01	**Protecting Data (systems and communications)**	How would you protect ARRC data from unauthorized access? 1) From outside intrusion? 2) Firewalls in use? 3) Proactive intrusion detection? 4) How are you alerted? 5) Proactive intrusion testing? 6) Internal threats?	
12.02	**Physical Protections**	What physical protections are in place to secure data center servers?	
12.03	**Monitoring**	What type of security monitoring do you do?	
12.04	**Log Review**	What type of security log reviews do you do?	
12.05	**Anti-Virus**	Describe your anti-virus/spyware/malware systems	
13.00	**SYSTEM STABILITY AND SUPPORT**		
13.01	**Maintenance & Support Model**	Describe your maintenance and support model	
13.02	**SLA Details**	What is your typical SLA response time?	
13.03	**System Response Times**	What are the system response times you support?	
13.04	**Support Response Times**	What are the support response times (24/7, 8/5) you support?	
13.05	**Escalation**	What is your escalation path?	
13.06	**Online / Offline**	What online / offline support options do you offer for your system?	
13.07	**System Releases**	How many releases of the software have occurred? (version X.x)	
13.08	**System Release Communications**	How are they communicated?	
13.09	**System Release Implementations**	How are they implemented?	
13.1	**3 - 5 year Product Strategy**	Please describe your product strategy looking out 3 - 5 years	
13.11	**Max # of Concurrent Users**	What is the maximum # of simultaneous users?	
13.12	**Patch Strategy**	Describe your patching strategy	

ID	Category	Description	Response: Please indicate how your solution / company would address the stated need or question
13.13	**Warranty**	Describe your solution warranty coverage: 1) Duration? 2) What's covered? 3) Other useful information?	
14.00	**COMPANY SLA FOR INTEGRATED SYSTEM**		
14.01	**Uptime Assurance**	Describe how your system strategy provides maximum uptime (24/7) for ARRC businesses	
14.02	**Downtime Communications**	How do you communicate downtime (planned and unplanned) and maintenance windows?	
14.03	**Proactive Monitoring**	How do you proactively monitor your system for unplanned downtime?	
14.04	**Required Downtime**	Is there any "required" system downtime?	
14.05	**HW/SW Maintenance Protocol**	Outline how hardware and software maintenance will be carried out without loss of service	
14.06	**Backup / Recover Measures**	What data backup and recovery measures do you have in place?	
14.07	**DR Strategy**	Describe your disaster recovery strategy	
14.08	**Issue/Bug Reporting**	What is your process for reporting bugs, issues and services requests?	
14.09	**Recent Uptime**	What has your system uptime been over the last 24 months?	
15.00	**DEVELOPMENT STRATEGY**		
15.01	**SDLC & Change Control**	Describe your SDLC and change control procedures?	
15.02	**QA / Testing Risk Assessment**	Describe your software QA/testing processes?	
15.03	**Update / Release Schedule**	Do you have a standard update release schedule?	
15.04	**Technical Documentation**	Describe your technical systems documentation? Where is it located? 1) Installation Guide 2) Systems Guide 3) Maintenance Guide 4) Etc.	
16.00	**COMPANY QUESTIONS**		
16.01	**Name**	Please provide your company's full legal name, corporate mailing address, main phone number and fax number?	
16.02	**History**	Please provide a brief history of your company, including the year of establishment and number of years in business. Significant business milestones?	
16.03	**Principals**	Who are your principals? How long have they been with the company? What is their active role in the business? Please provide a high level org chart.	
16.04	**Personnel Security**	How many staff do you currently employ and their average tenure?	
16.05	**Staff Breakdown**	Staff breakdown? Developers / Application Support / Corporate Support (AP/AR etc.)	
16.06	**Staff Change Requirements**	What changes would you need to make within your business to support a customer like ARRC?	
16.07	**Customer Count**	How many customers do you currently service? Who would you consider your cornerstone customers?	
16.08	**Competitors**	Whom do you consider to be your primary competitors?	
16.09	**Financial Stability**	Describe the financial stability of the business and its ability to obtain financing?	
16.1	**Financial Statements**	Are you able to provide audited financial statements that are prepared by a CPA in accordance with GAP which reflects the business' financial condition?	
16.11	**SOC 1 (certification, accreditation, and security assessments)**	Can you provide a SOC 1 audit report?	

ID	Category	Description	Response: Please indicate how your solution / company would address the stated need or question
16.12	**D&B Number**	What is your Dun and Bradstreet number/report?	
16.13	**Other Info**	Please share any other information you think would help us evaluate your business	
16.14	**Financial Analysis**	We would like to review your financial statements with the Alaska Railroad CFO	
16.15	**Contact Info for Technical Questions**	Provide a name, contact number and email address for someone who can guide the RFP review team in the technical details of this product and who can help to schedule a presentation.	
17.00	**DEPLOYMENT & ROLLOUT (contingency planning)**		
17.01	**Time to Deployment**	What is the typical time to deploy this solution	
17.02	**Day to Day Support (policies and procedures)**	What are the ongoing hours required by ARRC to "care and feeding" of this solution. How will apply polices and procedures for solution management? What is your framework plan?	
17.03	**Deployment Support**	What are the managed service offerings around the deployment and ongoing production support?	
17.04	**Awareness & Training**	Do you have a standardized training program that will benefit ARRC 1) End Users 2) System Admins	
17.05	**Training: Syllabus**	Can you provide a sample training syllabus?	
17.06	**Training: Standard Docs**	Do you have the following: 1) End User Guide 2) Operational Guide 3) Online or Printed for each?	
17.07	**Training: Costs**	What are the training costs? (initial training/ follow-on training) 1) Onsite training costs 2) Vendor site training costs 3) Remote (web) training costs	
18.00	**SOLUTION COSTS**		
18.01	**Initial Product Costs**	What is the initial base cost of purchasing or licensing this solution? What are the initial maintenance / support costs involved in that initial purchase / licensing?	
18.02	**Ongoing Product Costs**	Please indicate how ongoing billing is determined for your solution, and what these costs are. For example: "Software is billed per user account, at a rate of $45 per user, per month". 1) License count? 2) # of Users? 3) Module(s) deployed? 4) Other?	
18.03	**Ongoing Cost Schedule**	Please list when all of the various costs that will be accrued. For example, "Licenses are purchased once, at a rate of $250 per license. After the first year, all licenses are renewed at the end of each calendar year, at a rate of $25 per license". 1) Monthly? 2) Annually? 3) Per new user?	
18.04	**Maintenance & Support Contracts**	How are maintenance and support services charged and billed? 1) What are the costs? 2) What is the billing cycle? (Annual, Quarterly, etc.)	

ID	Category	Description	Response: Please indicate how your solution / company would address the stated need or question
18.05	**Professional Services: Implementation**	What are the expected professional service costs for an implementation such as the one SSI has described? (Ranges are ok.) 1) Installation / Configuration work 2) Customization work 3) Implementation management time 4) Etc. What is your professional services rate for ongoing development / configuration work?	
18.06	**Professional Services: Ongoing Support**	What are the rates for professional service to provide ongoing support of an installation like the one ARRC has described? 1) Configuration work 2) Customization work 3) Etc.	
18.07	**Pricing Incentives**	What discounts / incentives will be available to ARCC to execute a purchase in January?	
19.00	**REFERENCES**		
19.01	**Customer References**	Please provide at least three (3) pertinent customers who make significant use of your services (i.e. one rail road example and one software example/reference). Please include: 1) Company Name 2) Contact Name and Title 3) Address 4) Telephone number 5) Deployment type (SaaS or On Premise) 6) Description of the scope of work / support supplied to the customer, the duration, etc.	

ARRC RFP - SIEM Attachment 4.

ATTACHMENT #4

This is the NIST SP 800-82 (Revision 2) guidance.

Table of concerns and specific guidance to protect SCADA and ICS systems. This is the conclusion of the NIST SP 800-82 documents and a summary of general concerns over protecting these systems and networks.

Solutions must identify the method these will be controlled. It could be from another technology platform at ARRC.

NIST Items specifically listed	Description of concern
Concern1	Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation
Concern2	Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life
Concern3	Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects
Concern4	ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects
Concern5	Interference with the operation of safety systems, which could endanger human life.
	Major security objectives for an ICS implementation should include the following:
MS1	Restricting logical access to the ICS network and network activity. This includes using a demilitarized zone (DMZ) network architecture with firewalls to prevent network traffic from passing directly between the corporate and ICS networks, and having separate authentication mechanisms and credentials for users of the corporate and ICS networks. The ICS should also use a network topology that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
MS2	Restricting physical access to the ICS network and devices. Unauthorized physical access to components could cause serious disruption of the ICS's functionality. A combination of physical access controls should be used, such as locks, card readers, and/or guards.
MS3	Protecting individual ICS components from exploitation. This includes deploying security patches in as expeditious a manner as possible, after testing them under field conditions; disabling all unused ports and services; restricting ICS user privileges to only those that are required for each person's role; tracking and monitoring audit trails; and using security controls such as antivirus software and file integrity checking software where technically feasible to prevent, deter, detect, and mitigate malware.
MS4	Maintaining functionality during adverse conditions. This involves designing the ICS so that each critical component has a redundant counterpart. Additionally, if a component fails, it should fail in a manner that does not generate unnecessary traffic on the ICS or other networks, or does not cause another problem elsewhere, such as a cascading event.
MS5	Restoring system after an incident. Incidents are inevitable and an incident response plan is essential. A major characteristic of a good security program is how quickly a system can be recovered after an incident has occurred.

ICS In-Depth Strategy Guidance	
ID1	Developing security policies, procedures, training and educational material that apply specifically to the ICS.
ID2	Considering ICS security policies and procedures based on the Homeland Security Advisory System Threat Level, deploying increasingly heightened security postures as the Threat Level increases.
ID3	Addressing security throughout the lifecycle of the ICS from architecture design to procurement to installation to maintenance to decommissioning.
ID4	Implementing a network topology for the ICS that has multiple layers, with the most critical communications occurring in the most secure and reliable layer.
ID5	Providing logical separation between the corporate and ICS networks (e.g., stateful inspection firewall(s) between the networks).
ID6	Employing a DMZ network architecture (i.e., prevent direct traffic between the corporate and ICS networks).
ID7	Ensuring that critical components are redundant and are on redundant networks.
ID8	Designing critical systems for graceful degradation (fault tolerant) to prevent catastrophic cascading events.
ID9	Disabling unused ports and services on ICS devices after testing to assure this will not impact ICS operation.
ID10	Restricting physical access to the ICS network and devices.
ID11	Restricting ICS user privileges to only those that are required to perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege).
ID12	Considering the use of separate authentication mechanisms and credentials for users of the ICS network and the corporate network (i.e., ICS network accounts do not use corporate network user accounts).
ID13	Using modern technology, such as smart cards for Personal Identity Verification (PIV).
ID14	Implementing security controls such as intrusion detection software, antivirus software and file integrity checking software, where technically feasible, to prevent, deter, detect, and mitigate the introduction, exposure, and propagation of malicious software to, within, and from the ICS.
ID15	Applying security techniques such as encryption and/or cryptographic hashes to ICS data storage and communications where determined appropriate.
ID16	Expeditiously deploying security patches after testing all patches under field conditions on a test system if possible, before installation on the ICS.
ID17	Tracking and monitoring audit trails on critical areas of the ICS.

This table is the mapping of areas of concern for NIST SP 800-53 (Revision 4) to NIST SP 800-82. This table discusses specific challenges for SCADA and ICS systems and networks.

800-53	NIST 82	NIST 82 Guidance for the issue (Differentiator)
X	**6.1 Management Controls**	
X	**6.1.1 Risk Assessment**	Organizations must consider the potential consequences resulting from an incident on an ICS. Well-defined policy and procedures lead to mitigation techniques designed to thwart incidents and manage the risk to eliminate or minimize the consequences. The degradation of the physical plant, economic status, or national confidence could justify mitigation. For an ICS, a very important aspect of the risk assessment is to determine the value of the data that is flowing from the control network to the corporate network. In instances where pricing decisions are determined from this data, the data could have a very high value. The fiscal justification for mitigation has to be derived by the cost benefit compared to the effects of the consequence. However, it is not possible to define a one-size-fits-all set of security requirements. A very high level of security may be achievable but undesirable in many situations because of the loss of functionality and other associated costs. A well-thought-out security implementation is a balance of risk versus cost. In some situations the **risk may be safety, health, or environment-related** rather than purely economic. The risk may result in an **unrecoverable consequence rather than a temporary financial setback.**
	6.1.2 Planning	A security plan for an ICS should build on appropriate existing IT security experience, programs, and practices. However, the critical differences between IT and ICS addressed in Section 3.1 will influence how security will be applied to the ICS. **A forward-looking plan is needed to provide a method for continuous security improvements**. ICS security is a rapidly evolving field requiring the security planning process to constantly explore **emerging ICS security capabilities as well as new threats** that identified by organizations such as the US-CERT Control Systems Security Center (CSSC).
X	**6.1.3 System and Services Acquisition**	In support of the acquisition of secured ICS, the Process Control Security Requirements Forum (PCSRF), an industry-based effort being lead by NIST, has documented a cohesive, cross-industry set of requirements for new ICS [48] with follow-up work addressing SCADA and subcomponent-level requirements. The SCADA and Control System Procurement Project [49] is also developing a procurement language for specifying security requirements when procuring new systems or maintaining existing systems. The security requirements of an organization outsourcing the management and control of all or some of its information systems, networks, and desktop environments should be addressed in a contract agreed between the parties. External suppliers that have an impact on the security of the organization must be held to the same security policies and procedures to maintain the overall level of ICS security. Security policies and procedures of second and third-tier suppliers should also be in compliance with corporate cyber security policies and procedures in the case that they impact ICS security.

X	**6.1.4 Certification, Accreditation, and Security Assessments**	

X	**6.2 Operational Controls**	
X	**6.2.1 Personnel Security**	Positions should be categorized with a risk designation and screening criteria, and individuals filling a position should be screened against this criteria as well as complete an access agreement before being granted access to an information system. Personnel should be screened for the critical positions controlling and maintaining the ICS.
X	**6.2.2 Physical and Environmental Protection**	The physical protection of the cyber components and data associated with the ICS must be addressed as part of the overall security of a plant. Security at many ICS facilities is intimately tied to plant safety. A primary goal is to keep people out of hazardous situations without preventing them from doing their job or carrying out emergency procedures. Gaining physical access to a control room or control system components often implies gaining logical access to the process control system as well. Likewise, having logical access to systems such as main servers and control room computers allows an adversary to exercise control over the physical process. If computers are readily accessible, and they have removable media drives (e.g., floppy disks, compact discs, etc.) or USB ports, the drives can be fitted with locks or removed from the computers and USB ports disabled. Depending on security needs and risks, it might also be prudent to disable or physically protect power buttons to prevent unauthorized use. For maximum security, servers should be placed in locked areas and authentication mechanisms (such as keys) protected. Also, the network devices on the ICS network, including switches, routers, network jacks, servers, workstations, and controllers, should be located in a secured area that can only be accessed by authorized personnel. The secured area should also be compatible with the environmental requirements of the devices. A defense-in-depth solution to physical security should include the following attributes: -- Protection of Physical Locations. Classic physical security considerations typically refer to a ringed architecture of layered security measures. Creating several physical barriers, both active and passive, around buildings, facilities, rooms, equipment, or other informational assets, establishes these physical security perimeters. Physical security controls meant to protect physical locations include fences, anti-vehicle ditches, earthen mounds, walls, reinforced barricades, gates, or other measures. Most organizations include this layered model by preventing access to the plant first by the use of fences, guard shacks, gates, and locked doors. -- Access Control. Access control systems should ensure that only authorized people have access to controlled spaces. An access control system should be flexible. The need for access may be based on time (day vs. night shift), level of training, employment status, work assignment, plant status, and a myriad of other factors. A system must be able to verify that persons being granted access are who they say they are (usually using something the person has, such as an access card; something they know, such as a personal identification number (PIN); or something they are, using abiometric)Access control should be highly reliable yet not interfere with the routine or 6-8

	Additionally for 6.2.2	GUIDE TO SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) AND INDUSTRIAL CONTROL SYSTEMS SECURITY (DRAFT) emergency duties of plant personnel. Integration of access control into the process system allows a view into not only security access, but also physical and personnel asset tracking, dramatically accelerating response time in emergencies, helping to direct individuals to safe locations, and improving overall productivity. Within an area, access to network and computer cabinets should be limited to only those who have a need, such as network technicians and engineers, or computer maintenance staff. Equipment cabinets should be locked and wiring should be neat and within cabinets. Consider keeping all computers in secure racks and using peripheral extender technology to connect human-machine interfaces to the racked computers. Access Monitoring Systems. Access monitoring systems include still and video cameras, sensors, and various types of identification systems. Examples of these systems include cameras that monitor parking lots, convenience stores, or airline security. These devices do not specifically prevent access to a particular location; rather, they store and record either the physical presence or the lack of physical presence of individuals, vehicles, animals, or other physical entities. Adequate lighting should be provided based on the type of access monitoring device deployed. Access Limiting Systems. Access limiting systems may employ a combination of devices to physically control or prevent access to protected resources. Access limiting systems include both active and passive security devices such as fences, doors, safes, gates, and guards. They are often coupled with Identification and monitoring systems to provide role-based access for specific individuals or groups of individuals.
	Additionally for 6.2.2	-- People and Asset Tracking. Locating people and vehicles in a large installation is important for safety reasons, and it is increasingly important for security reasons as well. Asset location technologies can be used to track the movements of people and vehicles within the plant, to ensure that they stay in authorized areas, to identify personnel needing assistance, and to support emergency response. -- Environmental Factors. In addressing the security needs of the system and data, it is important to consider environmental factors. For example, if a site is dusty, systems should be placed in a filtered environment. This is particularly important if the dust is likely to be conductive or magnetic, as in the case of sites that process coal or iron. If vibration is likely to be a problem, systems should be mounted on rubber bushings to prevent disk crashes and wiring connection problems. In addition, the environments containing systems and media (e.g., backup tapes, floppy disks) should have stable temperature and humidity. An alarm to the process control system should be generated when environmental specifications such as temperature and humidity are exceeded. Environmental Control Systems. Heating, ventilation, and air conditioning (HVAC) systems for control rooms must support plant personnel during normal operation and emergency situations, which could include the release of toxic substances. Fire systems must be

		carefully designed to avoid causing more harm than good (e.g., to avoid mixing water with incompatible products). HVAC and fire systems have significantly increased roles in security that arise from the interdependence of process control and security. For example, fire prevention and HVAC systems that support industrial control computers need to be protected against cyber incidents. Power. Reliable power for the ICS is essential, so an uninterruptible power supply (UPS) should be provided. If the site has an emergency generator, the UPS battery life may only need to be a few seconds; however, if the site relies on external power, the UPS battery life may need to be hours.
		6.2.2.1 Control Center/Control Room Providing physical security for the control center/control room is essential to reduce the potential of many threats. Control centers/control rooms frequently have consoles continuously logged onto the primary control server, where speed of response and continual view of the plant is of utmost importance. These areas will often contain the servers themselves, other critical computer nodes, and sometimes plant controllers. It is essential to limit access to these areas using authentication methods such as smart or magnetic identity cards or biometric readers. In extreme cases, it may be considered necessary to make the control center/control room blast-proof, or to provide an offsite emergency control center/control room so that control can be maintained if the primary control center/control room becomes uninhabitable.
		6.2.2.2 Portable Devices Computers and computerized devices used for ICS functions (such as PLC programming) should never leave the ICS area. Laptops and portable engineering workstations should be tightly secured and never used outside the ICS network. Antivirus and patch management should be kept current.

		6.2.2.3 Cabling Cabling for the control network should be addressed in the cyber security plan. Unshielded twisted pair communications cable, while acceptable for the office environment, is generally not suitable for the plant environment due to its susceptibility to interference from magnetic fields, radio waves, temperature extremes, moisture, dust, and vibration. Industrial RJ-45 connectors should be used in place of other types of twisted pair connectors to provide protection against moisture, dust and vibration. Fiber-optic cable and coaxial cable are often better network cabling choices for the control network since they are immune to many of the typical environmental conditions including electrical and radio frequency interference found in an industrial control environment. Cable and connectors should be color-coded and labeled so that the ICS and IT networks are clearly delineated and potential for an inadvertent cross-connect is reduced. Cable runs should be installed so that access is minimized and equipment installed in locked cabinets with adequate ventilation and air filtration.
X	**6.2.3 Contingency Planning**	Contingency plans cover the full range of failures or problems that could be caused by failures in the ICS cyber security program. Contingency plans should include procedures for restoring systems from known valid backups, separating systems from all non-essential interferences and connections that could permit cyber security intrusions, and alternatives to achieve necessary interfaces and coordination. Contingency plans should be periodically tested to ensure that they continue to meet their objectives. Organizations also have business continuity plans and disaster recovery plans that are closely related to contingency plans. Because business continuity and disaster recovery plans are particularly important for ICS, they are described in more detail in the sections to follow.
		6.2.3.2 Disaster Recovery Planning A disaster recovery plan (DRP) is essential to continued availability of the ICS. The DRP should include the following items: -*- Required response to events or conditions of varying duration and severity that would activate the recovery plan -*- Procedures for operating the ICS in manual mode with all external electronic connections severed until secure conditions can be restored -*- Roles and responsibilities of responders -*- Processes and procedures for the backup and secure storage of information -*- Complete and up-to-date logical network diagram -*- Personnel list for authorized physical and cyber access to the ICS -*- List of personnel to contact in the case of an emergency including ICS vendors, network administrators, ICS support personnel, etc -*- Current configuration information for all components

		The plan should also indicate requirements for the timely replacement of components in the case of an emergency. If possible, replacements for hard-to-obtain critical components should be kept in inventory. The security plan should define a comprehensive backup and restore policy. In formulating this policy, the following should be considered: -*- The speed at which data or the system must be restored. This requirement may justify the need for a redundant system, spare offline computer, or valid file system backups. -*- The frequency at which critical data and configurations are changing. This will dictate the frequency and completeness of backups. -*- The safe onsite and offsite storage of full and incremental backups -*- The safe storage of installation media, license keys, and configuration information -*- Identification of individuals responsible for performing, testing, storing, and restoring backups
X	**6.2.4 Configuration Management**	A formal change management procedure is used to insure that all modifications to an ICS network meet he same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans. Risk assessment should be performed on all changes to the ICS network that could affect security, including configuration changes, the addition of network components, and installation of software. Changes to policies and procedures may also be required. The current ICS network configuration must always be known and documented.
		A formal change management procedure is used to insure that all modifications to an ICS network meet he same security requirements as the original components identified in the asset evaluation and the associated risk assessment and mitigation plans. Risk assessment should be performed on all changes to the ICS network that could affect security, including configuration changes, the addition of network components, and installation of software. Changes to policies and procedures may also be required. The current ICS network configuration must always be known and documented.
X	**6.2.5 Maintenance**	
X	**6.2.6 System and Information Integrity**	Controls exist for malicious code detection, spam and spyware protection, and intrusion detection, although they may not be appropriate for all ICS applications.
		6.2.6.1 Malicious Code Detection Antivirus tools only function effectively when installed, configured, running full-time, and maintained properly against the state of known attack methods and payloads. While antivirus tools are common security practice in IT computer systems, their use with ICS may require adopting special practices including compatibility checks, change management issues, and performance impact metrics. These special practices should be utilized whenever new signatures or new versions of antivirus software are installed.

		Major ICS vendors recommend and even support the use of particular antivirus tools. In some cases, control system vendors may have performed regression testing across their product line for supported versions of a particular antivirus tool and also provide associated installation and configuration documentation. There is also an effort to develop a general set of guidelines and test procedures focused on ICS performance impacts to fill the gaps where ICS and antivirus vendor guidance is not available [57]. Generally: -*- Windows, Unix, Intel chip set computers used as consoles, engineering workstations, data historians, pseudo-DCSs (PLC supervisors) such as Wonderware, HMIs, and general purpose SCADA and backup servers can be secured just like commercial IT equipment: install push- or auto-updated antivirus and patch management software with updates distributed via an anti-virus server and patch management server located inside the process control network and auto-updated from the IT network -*- Follow vendor recommendations on all other servers and computers (DCS, PLC, instruments) that have time-dependent code, modified or extended the operating system or any other change that makes it different from any standard PC that one could buy at an office supply or computer store. Expect the vendor to make periodic maintenance releases that include security patches.
		6.2.6.2 Intrusion Detection and Prevention An effective IDS deployment typically involves both host-based and network-based IDSs. In the ICS environment, network-based IDSs are most often deployed between the control network and the corporate network in conjunction with a firewall; host-based IDSs are most often deployed on the computers that use general-purpose OSs or applications such as HMIs, SCADA servers, and engineering workstations. Properly configured, an IDS can greatly enhance the security management team's ability to detect attacks entering or leaving the system, thereby improving security. They can also potentially improve a control network's efficiency by detecting non-essential traffic on the network. However, even when IDSs are implemented, security staff can primarily recognize individual attacks, as opposed to organized patterns of attacks over time. Additionally, care should be given to not confuse unusual ICS activity, such as during transient conditions, as an attack. Current IDS and IPS products are effective in detecting and preventing well-known Internet attacks, but until recently they have not addressed ICS protocol attacks. IDS and IPS vendors are beginning to develop and incorporate attack signatures for various ICS protocols such as Modbus, DNP, and ICCP. [59] [60] Appendix D provides some additional information on emerging IDS capabilities.
		6.2.6.3 Patch Management Applying patches to OS components creates another situation where significant care should be exercised in the ICS environment. Patches should be adequately tested to determine the

		acceptability of side effects. Regression testing is advised. It is not uncommon for patches to have an adverse effect on other software. A patch may remove a vulnerability, but it can also introduce a greater risk from a production or safety perspective. Patching the vulnerability may also change the way the OS or application works with control applications, causing the control application to lose some of its functionality. Once the decision is made to deploy a patch, there are other tools that automate this process from a centralized server and with confirmation that the patch has been deployed correctly. Consider separating the automated process for ICS patch management from the automated process for non-ICS applications. Patching should be scheduled to occur during planned ICS outages.
X	**6.2.7 Media Protection**	Media assets include removable media and devices such floppy disks, CDs, DVDs and USB memory sticks, as well as printed reports and documents. Physical security controls should address specific requirements for the safe maintenance of these assets and provide specific guidance for transporting, handling, and erasing or destroying these assets. Security requirements could include safe storage from loss, fire, theft, unintentional distribution, or environmental damage. If an adversary gains access to backup media associated with an ICS, it could provide valuable data for launching an attack. Recovering an authentication file from the backups might allow an adversary to run password cracking tools and extract usable passwords. In addition, the backups typically contain machine names, IP addresses, software version numbers, usernames, and other data useful in planning an attack. The use of any unauthorized CDs, DVDs, floppy disks, USB memory sticks, or similar removable media on any node that is part of or connected to the ICS should not be permitted; this can prevent the introduction of malware or the inadvertent loss or theft of data. Where the system components use unmodified industry standard protocols, mechanized policy management software can be used to enforce media protection policy.

X	**6.2.8 Incident Response**	Regardless of the steps taken to protect an ICS, it is always possible that it may be compromised by an intentional or unintentional incident. The following symptoms can arise from normal network problems, but when several symptoms start to appear, a pattern may indicate the ICS is under attack and may be worth investigating further. If the adversary is skilled, it may not be very obvious that an attack is underway. The symptoms of an incident could include any of the following: -- Unusually heavy network traffic -- Out of disk space or significantly reduced free disk space -- Unusually high CPU usage -- Creation of new user accounts -- Attempted or actual use of administrator-level accounts -- Locked-out accounts -- Account in-use when the user is not at work -- Cleared log files -- Full log files with unusually large number of events -- Antivirus or IDS alerts -- Disabled antivirus software and other security controls -- Unexpected patch changes -- Machines connecting to outside IP addresses -- Requests for information about the system (social engineering attempts) -- Unexpected changes in configuration settings -- Unexpected system shutdown.
	Additionally for 6.2.8	To minimize the effects of these intrusions, it is necessary to plan a response. Incident response planning defines procedures to be followed when an intrusion occurs. NIST SP 800-61, Computer Security Incident Handling Guide, provides guidance on incident response planning, which might include the following items: -- Classification of Incidents. The various types of ICS incidents should be identified and classified as to potential impact and likelihood so that a proper response can be formulated for each potential incident. -- Response Actions. There are several responses that can be taken in the event of an incident. These range from doing nothing to full system shutdown (although full shutdown is highly unlikely for an ICS). The response taken will depend on the type of incident and its effect on the ICS system and the physical process being controlled. A written plan documenting the types of incidents and the response to each type should be prepared. This will provide guidance during times when there might be confusion or stress due to the incident. This plan should include step-by-step actions to be taken by the various organizations. If there are reporting requirements, these should be noted as well as where the report should be made and phone numbers to reduce reporting confusion.

		-- Recovery Actions. The results of the intrusion might be minor or could cause many problems in the ICS. Prior analysis should be conducted to determine the sensitivity of the physical system being controlled to failure modes in the ICS. In each case, step-by-step recovery actions should be documented so that the system can be returned to normal operations as quickly and safely as possible. During the preparation of the incident response plan, input should be obtained from the various stakeholders including operations, management, organized labor, legal, and safety. These stakeholders should also review and approve the plan.
	6.2.9 Awareness and Training	For the ICS environment, this must include control system-specific information security awareness and training for specific ICS applications. In addition, an organization must identify, document, and train all personnel with significant information system roles and responsibilities. Awareness and training must cover the physical process being controlled as well as the ICS. Security awareness is a critical part of ICS incident prevention, particularly when it comes to social engineering threats. Social engineering is a technique used to manipulate individuals into giving away private information, such as passwords. This information can then be used to compromise otherwise secure systems. Implementing an ICS security program may bring changes to the way in which personnel access computer programs, applications, and the computer desktop itself. Organizations should design effective training programs and communication vehicles to help employees understand why new access and control methods are required, ideas they can use to reduce risks, and the impact on the organization if control methods are not incorporated. Training programs also demonstrate management's commitment to, and the value of, a cyber security program. Feedback from staff exposed to this type of training can be a valuable source of input for refining the charter and scope of the security program.

X	**6.3 Technical Controls**	
X	**6.3.1 Identification and Authentication**	Computer systems in ICS environments typically rely on traditional passwords for authentication. Control system suppliers often supply systems with default passwords. These passwords are often easy to guess or are changed infrequently, which creates additional security risks. Also, protocols currently used in ICS environments generally have inadequate or no network service authentication. There are now several forms of authentication available in addition to traditional password techniques being used with ICS. Some of these, including password authentication, are presented in the following sections with discussions regarding their use with ICS.
	Additional Information for 6.3.1	6.3.1.1 Password Authentication One problem with passwords unique to the ICS environment is that a user's ability to recall and enter a password may be impacted by the stress of the moment. During a major crisis when human intervention is critically required to control the process, an operator may panic and have difficulty remembering or entering the password and either be locked out completely or be delayed in responding to the event. Biometric identifies may have similar drawbacks. It is recommended not to use password authorizations on these critical control systems but instead to use other compensating controls, such as rigorous physical security controls. Some ICS operating systems make setting secure passwords difficult, as the password size is very small and the system allows only group passwords at each level of access, not individual passwords. Some industrial (and Internet) protocols transmit passwords in plaintext, making them susceptible to interception. In cases where this practice cannot be avoided, it is important that users have different (and unrelated) passwords for use with encrypted and non-encrypted protocols. The following are general recommendations and considerations with regards to the use of passwords. Specific recommendations are presented in ISA-TR99.00.02-2004 [27]. -- The length, strength, and complexity of passwords should balance security and operational ease of access within the capabilities of the software and underlying OS. -- Passwords should have appropriate length and entropy characterization for the security required. In particular, they should not be able to be found in a dictionary or contain predictable sequences of numbers or letters.
		6.3.1.3 Physical Token Authentication Two-factor authentication is an accepted good practice for access to ICS applications from outside the ICS firewall. Physical/token authentication has the potential for a strong role in ICS environments. An access card or other token can be an effective form of authentication for computer access, as long as the computer is in a secure area (e.g., once the operator has gained access to the

		room with appropriate secondary authentication, the card alone can be used to enable control actions).
		6.3.1.4 Biometric Authentication Biometric devices make a useful secondary check versus other forms of authentication that can become lost or borrowed. Using biometric authentication in combination with token-based access control or badge-operated employee time clocks increases the security level. A possible application is in a control room that is environmentally controlled and physically secured [34].
		-- Passwords should be used with care on operator interface devices such as control consoles on critical processes. Using passwords on these consoles could introduce potential safety issues if operators are locked out or delayed access during critical events. -- The keeper of master passwords should be a trusted employee, available during emergencies. A copy of the master passwords may want to be stored in a very secure location. -- The passwords of privileged users (such as network technicians, electrical or electronics technicians and management, and network designers/operators) should be most secure and be changed frequently. Authority to change master passwords should be limited to trusted employees. A password audit record, especially for master passwords, should be maintained separately from the control system. -- In environments with a high risk of interception or intrusion (such as remote operator interfaces in a facility that lacks local physical security access controls), organizations should consider supplementing password authentication with other forms of authentication such as challenge/response or two-factor authentication using biometric or physical tokens. -- For user authentication purposes, password use is common and generally acceptable for users logging directly into a local device or computer. Passwords should not be sent across any network unless protected by some form of FIPS-approved encryption or salted cryptographic hash specifically designed to prevent replay attacks. It is assumed that the device used to enter a password is connected to the network in a secure manner. -- For network service authentication purposes, passwords should be avoided if possible. There are more secure alternatives available, such as challenge/response or public key authentication.
X	**6.3.2 Access Control**	6.3.2.1 Role-based Access Control (RBAC) RBAC can be used to provide a uniform means to manage access to ICS devices while reducing the cost of maintaining individual device access levels and minimizing errors. RBAC should be used to restrict ICS user privileges to only those that are required to perform each person's job (i.e., configuring each role based on the principle of least privilege).

		6.3.2.2 Web Servers SCADA and historian software vendors typically provide Web servers as a product option so that users outside the control room can access ICS information. In many cases, software components such as ActiveX controls or Java applets must be installed or downloaded onto each client machine accessing the Web server. Some products, such as PLCs and other control devices, are available with embedded Web, FTP, and e-mail servers to make them easier to configure remotely and allow them to generate e-mail notifications and reports when certain conditions occur.
		6.3.2.3 Virtual Local Area Network (VLAN) VLANs have been effectively deployed in ICS networks, with each automation cell assigned to a single VLAN to limit unnecessary traffic flooding and allow network devices on the same VLAN to span multiple switches [34].
		6.3.2.4 Dial-up Modems -*- Consider using callback systems when dial-up modems are installed in an ICS. This ensures that a dialer is legitimate by having the modem establish the working connection based on the dialer's information and a callback number stored in a database. -*- Ensure that default passwords have been changed and strong passwords are in place for each modem. -*- Physically identify modems in use to the control room operators. -*- Configure remote control software to use unique user names and passwords, encryption, and audit logs. Use of this software by remote users should be monitored on an almost real-time frequency. -*- If possible, disconnect modems when not in use. It should be noted that sometimes modem connections are part of the legal support agreement with the vendor (e.g., 24x7 support with 15 minute response time). Personnel should to be aware that disconnecting/removing the modems may require that contracts be renegotiated.
		6.3.2.5 Wireless -*- Prior to installation, a wireless survey should be performed to determine antenna location and strength to minimize exposure of the wireless network. The survey should take into account the fact that attackers can use powerful directional antennas, which extend the effective range of a wireless LAN beyond the expected standard range. -*- Wireless users' access should utilize IEEE 802.1x authentication using a secure authentication protocol (e.g., Extensible Authentication Protocol [EAP] with TLS [EAP-TLS]) that authenticates users via either user certificates or a Remote Authentication Dial In User Service (RADIUS) server. -*- The wireless access points and data servers for wireless worker devices should be located on an isolated network with documented and minimal (single if possible)

		connections to the ICS network topology. -*- Wireless access points should be configured to have a unique service set identifier (SSID), disable SSID broadcast, and enable MAC filtering at a minimum. -*- Wireless devices, if being utilized in a Microsoft Windows ICS network, should be configured into a separate organizational unit of the Windows domain. -*- Wireless device communications should be encrypted and integrity-protected. The encryption must not degrade the operational performance of the end device. Encryption at OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency. The use of hardware accelerators to perform cryptographic functions should also be considered. For mesh networks, consider the use of broadcast key versus public key management implemented at OSI Layer 2 to maximize performance. Asymmetric cryptography should be used to perform Administrative functions and Symmetric encryption should be used to secure each data stream as well as network control traffic. An adaptive routing protocol should be considered if the devices are to be used for wireless mobility. The convergence time of the network should be as fast as possible supporting rapid network recovery in the event of a failure or power loss. It should also be noted that deployment of a mesh network may provide fault tolerance thru alternate route selection and pre-emptive fail-over of the network The ISA-SP10019 Committee is working to establish standards, recommended practices, technical reports, and related information that will define procedures for implementing wireless systems in the automation and control environment with a focus on the field level. Guidance is directed towards those responsible for the complete life cycle including the designing, implementing, on-going maintenance, scalability or managing manufacturing and control systems, and shall apply to users, system integrators, practitioners, and control systems manufacturers and vendors.
X	**6.3.3 Audit and Accountability**	It is necessary to determine that the system is performing as intended. Periodic audits of the ICS should be performed to validate the following items: -*- The security controls present during system validation testing are still installed and operating correctly in the production system. -*- The production system is free from security compromises and provides information on the nature and extent of compromises as feasible, should they occur. -*- The management of change program is being rigorously followed with an audit trail of reviews and approvals for all changes. The results from each periodic audit should be expressed in the form of performance against a set of predefined and appropriate metrics to display security performance and security trends. Security performance metrics should be sent to the appropriate

		stakeholders, along with a view of security performance trends. Traditionally, the primary basis for audit in IT systems has been recordkeeping. Using appropriate tools within an ICS environment requires extensive knowledge from an IT professional familiar with critical production and safety implications for the facility. Many of the process control devices that are integrated into the ICS have been installed for many years and do not have the capability to provide the audit records described in this section. Therefore, the applicability of these more modern tools for auditing system and network activity is dependent upon the capabilities of the components in the ICS. The critical tasks in managing a network in an ICS environment are ensuring reliability and availability to support safe and efficient operation. In regulated industries, regulatory compliance can add complexity to security and authentication management, registry and installation integrity management, and all functions that can augment an installation and operational qualification exercise. Diligent use of auditing and log management tools can provide valuable assistance in maintaining and proving the integrity of the ICS from installation through the system life cycle. The value of these tools in this environment can be calculated by the effort required to requalify or otherwise retest the ICS where the integrity due to attack, accident, or error is in question. The system should provide reliable, synchronized time stamps in support of the audit tools. Monitoring of sensors, logs, IDS, antivirus, patch management, policy management software, and other security mechanisms should be done on a real-time basis where feasible. A first-line monitoring service would receive alarms, do rapid initial problem determination and take action to alert appropriate facility personnel to intervene. System auditing utilities should be incorporated into new and existing ICS projects. These tools can provide tangible records of evidence and system integrity. Additionally, active log management utilities may actually flag an attack or event in progress and provide location and tracing information to help respond to the incident [34]. There should be a method for tracing all console activities to a user, either manually (e.g., control room sign in) or automatic (e.g., login at the application and/or OS layer). Policies and procedures for what is logged, how the logs are stored (or printed), how they are protected, who has access to the logs and how/when are they reviewed should be developed. These policies and procedures will vary with the ICS application and platform. Legacy systems typically employ printer loggers, which are reviewed by administrative, operational, and security staff. Logs maintained by the ICS application may be stored at various locations and may or may not be encrypted.
		OSI Layer 2 should be considered, rather than at Layer 3 to reduce encryption latency. In addition, encrypted messages are often larger than unencrypted messages due to one or more of the following: -- Additional checksums to reduce errors -- Protocols to control the cryptography -- Padding (for block ciphers)

		-- Authentication procedures -- Other required cryptographic processes. Cryptography also introduces key management issues. Sound security policies require periodic key changes. This process becomes more difficult as the geographic size of the ICS increases, with extensive SCADA systems being the most severe example. Because site visits to change keys can be costly and slow, it is useful to be able to change keys remotely.
	Additional Information for 6.3.3	Before deploying encryption, first determine if encryption is the appropriate solution for the specific ICS application, as authentication and integrity are generally the key security issues for ICS applications. If cryptography is selected, the most effective safeguard is to use a complete cryptographic system approved by the NIST/ Communications Security Establishment (CSE) Cryptographic Module Validation Program (CMVP)20. Within this program standards are maintained to ensure that cryptographic systems were studied carefully for weaknesses by a wide range of experts, rather than being developed by a few engineers in a single organization. At a minimum, certification makes it probable that: -- Some method (such as counter mode) will be used to ensure that the same message does not generate the same value each time -- ICS messages are protected against replay and forging -- Key management is secure throughout the life cycle of the key -- The system is using an effective random number generator -- The entire system has been implemented securely. Even then, the technology is only effective if it is an integral part of an effectively enforced information security policy. American Gas Association (AGA) report 12-1 [5] contains an example of such a security policy. While it is directed toward a gas SCADA system, many of its policy recommendations could apply to any ICS. For an ICS, encryption can be deployed as part of a comprehensive, enforced security policy. Organizations should select cryptographic protection matched to the value of the information being protected and ICS operating constraints. Specifically, a cryptographic key should be long enough so that guessing it or determining it through analysis takes more effort, time, and cost than the value of the protected asset. The encryption hardware should be protected from physical tampering and uncontrolled electronic connections. Assuming cryptography is the appropriate solution, organizations should select cryptographic protection with remote key management if the units being protected are so numerous or geographically dispersed that changing keys is difficult or expensive. [34]
X	**6.3.4 System and Communications Protection**	6.3.4.1 Encryption The use of encryption within an ICS environment could introduce communications latency due to the additional time and computing resources required to encrypt, decrypt, and

		authenticate each message. For ICS, any latency induced from the use of encryption, or any other security technique, must not degrade the operational performance of the end device. Encryption at
		6.3.4.2 Virtual Private Network (VPN) VPNs are most often used in the ICS environment to provide secure access from an untrusted network to the ICS control network. Untrusted networks can range from the Internet to the corporate LAN. Properly configured, VPNs can greatly restrict access to and from control system host computers and controllers, thereby improving security. They can also potentially improve control network responsiveness by removing unauthorized non-essential traffic from the intermediary network. VPN devices used to protect control systems should be thoroughly tested to verify that the VPN technology is compatible with the application and that the VPN devices do not unacceptably affect network traffic characteristics of the implementation [34].