TO: **James L. App, City Manager**

FROM: **Joseph M. Deakin, Public Works Director**

SUBJECT: **Award Contract**
Vulnerability Assessment of the Water System

DATE: **December 16, 2003**

NEEDS: For the City Council to consider awarding a contract to prepare a Vulnerability Assessment of the City's water system.

FACTS:

1. In accordance with the Bioterrorism Response Act of 2002, the City is required to prepare a Security Vulnerability Assessment of the City's water system.

2 The study must be submitted and approved by the Environmental Protection Agency (EPA) by June 2004.

3. In September 2003, staff issued a Request for Proposal to twelve companies. Six responded to the RFP.

4. A four (4) member staff committee rated all the proposals and determined that those submitted by Boyle Engineering and Risk Management Professionals were the most comprehensive and addressed the City's concerns best.

5. In November 2003, Mayor Frank Mecham and Councilman Jim Heggarty interviewed Boyle Engineering and Risk Management Professionals, along with staff.

ANALYSIS AND CONCLUSION: At the conclusion of the interview, the committee concluded the Vulnerability Assessment Study should be prepared by a firm specializing in security systems, rather than an engineering firm. They therefore recommend that the City engage the services of Risk

Management Professionals in accordance to the attached Scope of Work.

POLICY REFERENCE: Bioterrorism Act of 2002.

FISCAL IMPACT: The fee to prepare the Vulnerability Assessment Study is $19,925. This cost will be funded from the adopted budget of the Water Division's Maintenance and Operations.

OPTIONS:

a. **(1)** Adopt Resolution No. 03-xx authorizing the City Manager to enter a contract with Risk Management Professionals to prepare a Vulnerability Assessment of the City's Water System in the amount of $19,925; and

(2) Dissolve the ad hoc committee formed in November 2003 to review the two top firms responding to the Vulnerability Assessment RFP.

b. Amend, modify or reject the above option.

Attachments:
1) Resolution 03-xx

2) Scope of Work

RESOLUTION NO. 03-

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF PASO ROBLES AUTHORIZING THE CITY MANAGER TO ENTER A CONTRACT WITH RISK MANAGEMENT PROFESSIONALS

WHEREAS; the Bioterrorism Act of 2002 requires that the City prepare a Security Vulnerability Assessment of its water system; and

WHEREAS, the City issued a Request for Proposal to twelve (12) firms to prepare the Study; and

WHEREAS, six (6) firms responded; and

WHEREAS, two (2) firms were invited to appear before a Selection Committee; and

WHEREAS, the Selection Committee determined that Risk Management Professionals is the best firm to prepare the Study.

NOW, THEREFORE, BE IT RESOLVED, DETERMINED AND ORDERED as follows:

SECTION 1. That the City Council does hereby accept the recommendation of the Selection Committee.

SECTION 2 That the City Council does hereby authorize the City Manager to enter into a contract with Risk Management Professionals in the amount of $19,925.

PASSED AND ADOPTED by the City Council of the City of Paso Robles this 16th day of December 2003 by the following vote:

AYES:
NOES:
ABSTAIN:
ABSENT:

_____
Frank R. Mecham, Mayor

ATTEST:

_____
Sharilyn M. Ryan, Deputy City Clerk

WORK PROGRAM

Methodology

The purpose of the proposed effort is to perform a Vulnerability Assessment of the security of the drinking water system as required by the Public Health Security and Bioterrorism Preparedness and Response Act of 2002. We will use the Risk Assessment Methodology for Water Utilities (RAM-W^{SM}) developed by Sandia National Laboratories as our approach to perform the Security Vulnerability Assessment (SVA). Based on this approach and the USEPA's Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002, we have prepared a project plan which provides a comprehensive, pragmatic, and cost-effective solution to determining vulnerabilities. We have not reiterated the RAM-W^{SM} methodology in this proposal, but have instead focused on describing the effective application of the methodology to meet your specific needs.

As identified in the RAM-W^{SM} methodology, the SVA is the foundation upon which informed decisions can be made to reduce risks from malevolent actions. This basis for decisions is needed to ensure that you will gain as much as possible from the funds set aside to implement the recommended improvements to facilities, equipment, and procedures. This decision-making platform is developed by creating a comprehensive list of scenarios and an assessment of the likelihood and severity for each scenario. This list will be developed through the use of a systematic approach and the participation of a team with expertise in security. Our experience has shown that a prioritized list of recommendations (typically not provided by SVA Contractors) provides significantly increased value to you by allowing the prioritization of finite resources. This team approach that includes specific participation by the water utility is a unique approach used by the RMP Project Team that removes the potential for outlandish and unusable recommendations (often produced by other SVA Contractors that perform this key evaluation without direct customer involvement).

Using the modified RAM-W^{SM} methodology and other techniques which have been applied in the process safety field, potential scenarios based upon malevolent acts towards critical facilities will be identified and evaluated. These scenarios will be ranked according to their severity and likelihood by a panel of experts from our Project Team and key water personnel. The ranked list of scenarios will provide the basis for recommending changes to current emergency response and security programs, and improvements to other programs and activities, facilities, and systems (i.e., capital

improvements). The ranking also allows water management to prioritize the recommendations and develop a cost-effective plan for improving security and reducing vulnerability.

In summary, the foundation of our approach builds on the lessons-learned from our Tier I SVA projects to enhance the Sandia RAM-W^{SM} methodology to:

- Focus on the analysis tasks that yield the greatest information for the effort expended
- Provide recommended improvements that are usable to you
- Prioritize the recommendations to facilitate the development of an action plan

Advantages of Using Our Focused RAM-W^{SM} Approach vs. Alternates (e.g., VSAT)

Based on our experience with Tier I SVA Projects, Risk Management Professionals has adopted an approach for Tier II SVA Projects that uses those elements of the Sandia RAM-W^{SM} Methodology that provide measurable insights and tangible results, but does not use those optional elements of the RAM-W^{SM} Methodology that provide minimal value. In this manner, we have crafted a focused RAM-W^{SM} approach that addresses all of the EPA requirements. In addition to our extensive knowledge of the RAM-W^{SM} methodology, we have also been trained in VSAT and are proficient in the use of the software, even though we are not recommending its use for this project.

VSAT is a useful tool that facilitates a single-user's ability to consider large numbers of threats, assets, and countermeasures. Although requiring an extensive time investment, it would typically be used by a single water utility representative. The VSAT approach also requires the performance of an up-front Threat Assessment, Asset Prioritization, and the creation of budgeted Implementation Plans for recommendations stemming from the Security Vulnerability Assessment.

Our focused RAM-W^{SM} approach also includes an up-front Threat Assessment, Asset Prioritization, and the creation of budgeted Implementation Plans for recommendations stemming from the Security Vulnerability Assessment. However, by contrast, instead of a single individual investing a large amount of time considering all asset-threat-countermeasure combinations, we use a team approach for our Scenario Identification and Analysis (SIA) Sessions that efficiently captures the insights and varying perspectives of a diverse team.

The unique feature of the SIA Sessions is that they are patterned after techniques utilized for safety assessments that are extremely proficient at efficiently analyzing

hazardous scenarios and deriving a consensus conclusion. This allows for the assimilation of diverse perspectives to achieve higher quality results with less total manpower than might be invested in VSAT. Our SIA Session approach also utilizes specialized software (PHAPlus™) to assist in the facilitation of team sessions and documentation.

V-SAT	RAM-W℠
VSAT allows one individual with a strong security background and a deep understanding of the water system to determine the vulnerabilities of each facility.	Our approach takes advantage of the backgrounds and experience of a diverse group of individuals to determine the most important vulnerabilities.
VSAT is asset-based and examines each part of a facility to identify potential security vulnerabilities.	Our approach determines the routes of exposure and focuses on those routes rather than spending a significant amount of time on routes which are not likely to be threats.

Project Approach

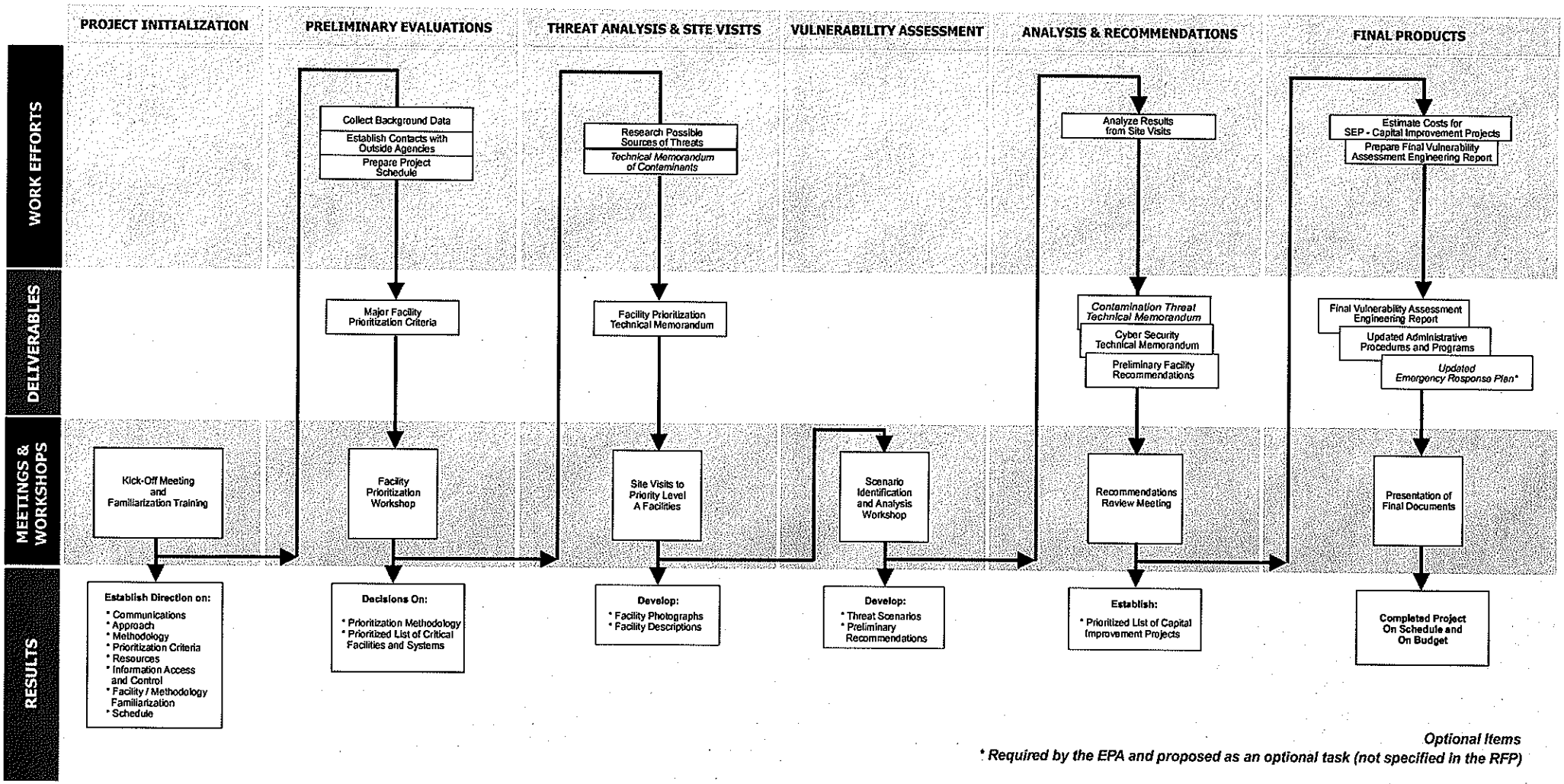
This section of the proposal has been partitioned into sequential work tasks. The next two subsections contain our proposed methodology and the requisite tasks which are required per the EPA's Instructions to Assist Community Water Systems in Complying with the Public Health Security and Bioterrorism Preparedness and Response Act of 2002.

Meetings – The most direct way to communicate with the client and other agencies involved with the project will be through meetings. Meetings will be scheduled to present submittals, to review and discuss your comments, and to report the status of the overall project. We also anticipate meeting on a more frequent and informal basis with Project Team members as required to assist in decision making.

Work Plan – Identification and resolution of issues during the early stages of the project are critical to delivering a quality project to you on time and on budget. One tool that we have found to be helpful is having a work plan that generally shows the key elements of the project. The work plan identifies submittals, meetings, activities, reviews, and goals for the project. A proposed work plan for the project is shown on the following page. This work plan may be modified according to your preferences.

Work Plan

SECURITY VULNERABILITY ASSESSMENT FOR THE CITY OF PASO ROBLES



Optional Items

** Required by the EPA and proposed as an optional task (not specified in the RFP)*

Proposed Scope of Work for Compliance with EPA Requirements

The final products of the proposed effort will include the following:

- A Security Vulnerability Assessment Report
- A ranked list of potential sources of threat to critical facilities
- A list of recommendations and their risk-based justification
- *A background information technical memorandum describing chemical, biological, and radiological threats*

Security and Confidentiality of Project Information

We understand that disclosure of any information gathered as part of the assessment has the potential to pose a significant risk to public health and safety. During the project, RMP and all member companies of the Project Team will take every precaution to secure all project records and destroy all drafts. After the project is completed, RMP and all member companies of the Project Team will return all documents obtained or generated during the course of this project.

We have developed specific procedures for obtaining, processing, storing, and transporting security-sensitive information. The procedure offers various options for our clients, and our standard security procedures include use of secure computer drives, use of a fireproof safe, and use of latest electronic encryption methods. These procedures and options will be discussed with your management team during the project initiation task to make a final determination of the approach that will be used to ensure long-term security of the information.

All members of the Project Team (including support staff) will be specifically instructed to keep confidential all information (paper, electronic, and verbal) obtained or generated in the course of the proposed project. Task leaders and project management will maintain strict vigilance while implementing this critical aspect of the project.

Quality Control

RMP has an established internal quality assurance practice that requires work products to be reviewed by an independent, senior member of the project team. For projects on which our clients required a formal quality control process, RMP and our subconsultants implement the following steps:

- A senior member of the technical staff is identified as the person responsible for quality control and is not assigned any efforts associated with that project task.
- As each work product is drafted, the person responsible for quality control reviews it and then generates an internal memo providing comments back to the technical leads.
- The work product is updated by the responsible analyst and resubmitted for quality control review.
- The review process is repeated until the Project Manager verifies completion of the work product.
- The same review process is applied to all deliverables to the client. All deliverables must receive an authorization from the Project Manager to be released to the client for review.

Documentation for the review process is created and maintained with the project files.

Proposed Technical Approach

The project will be conducted according to the following Tasks summarized below:

Task 1 Project Initiation and Facility Prioritization (define mission objectives)

Task 2 Threat Assessment

- Physical Threat Assessment
- Cyber Threat Assessment
- *Chemical, Biological, and Radiological Threat Background Information*

Task 3 Analysis of Priority Level A Facilities (Facility Characterization, System Effectiveness Determination, and Risk Assessment)

- Facility Walkdowns (Site Visits)
- Scenario Identification and Analysis (SIA) Sessions involving Utility Personnel
- Development of Risk Values and Risk-Ranked Recommendations

Task 4 Prepare Reports

Task 5 Project Reporting

Task 6 Security Enhancement/Prioritization Plan (SEPP) – Capital Improvements

Task 7 Emergency Response Plan Update (Optional)

Task 1 Project Initiation and Facility Prioritization (define mission objectives)

A kick-off meeting and familiarization training will be held with utility management and key members of the Project Team. The following subjects will be addressed during this meeting:

Project Initiation

- **Scope Verification** - The physical systems to be included in the Security Vulnerability Assessment (SVA) will be verified.
- **Methodology** - A presentation of the specific methodology for the SVA will be provided by the Project Manager. As noted in the preceding section, key elements of the RAM-W^{SM} methodology developed by Sandia will be used as the basis of the SVA.
- **Criteria for Facility/Systems Prioritization** - A set of criteria for prioritizing facilities will be proposed for review and approval. Measures such as "Percentage of Demand" and "Criticality of Users" may be used to develop the facility prioritization criteria. These criteria will then be used to work with utility personnel to interactively prioritize facilities.
- **Schedule** - Key milestones for: interim results presentation, draft reports submittals, and final report submittals will be discussed.
- **Resources (Utility Personnel)** - Operational and supervisory personnel are specifically included in the brainstorming sessions and management personnel will be involved in making key decisions. The project kick-off meeting will also summarize the roles of utility personnel and the specific levels of effort for each project activity. For Scenario Identification and Analysis (SIA) Sessions, the participation of area managers from water operations, operations personnel, the security manager, engineering personnel, and SCADA system personnel will be required to achieve the desired quality.
- **Resources (Documentation)** – You will be provided with a list of data which will be required including: engineering drawings, procedures, water quality reports, etc.

- **Resources (Local Authorities)** – You are encouraged to invite the participation of personnel from local law enforcement and emergency response organizations having jurisdiction over utility assets. Participation from other interfacing water agencies might also be desirable. These personnel may also be providing documentation to be used during the brainstorming sessions and other portions of the project. During the course of the project, we will discuss your preferred method of approaching other groups for information and participation.
- **Communication** - Electronic communication policies (i.e., file encryption) will be discussed.
- **Information Control** - Steps which RMP and the utility will take to protect and control the information that will be generated while conducting this project will be verified during the Project Kick-off Meeting.

Facility Prioritization

Immediately subsequent to the kick-off meeting, utility facilities will be prioritized using the criteria assigned. For example, for the measure "Percentage of Demand," each facility will be compared to all the other facilities based on the number of people served. The process will be repeated for each criteria defined in this Task. We plan to hold the prioritization meeting immediately following the Project Initiation meeting to ensure that efforts are focused.

During the course of the Facility Prioritization session, the Project Team will use customized software assembled by Risk Management Professionals to interactively rank the facilities in terms of their contributions to utility criteria. The prioritized list will allow the Project Team to focus on the facilities which are higher priority. Based on past experience of the Project Team in analyzing large complex systems, it is expected that the facilities will be binned into two priority groups.

- Priority Level A, the high priority facilities, will be analyzed first using the full extent of recommended approach.
- Priority Level B, the lower priority facilities, may be visited during the Walkdowns, and if there is sufficient time during the schedule meetings, will be analyzed as appropriate.

Task 1 Deliverables:

- Criteria for facility prioritization
- Project plan presentation

- Methodology summary presentation
- Schedule of deliverables, meetings, topics, and participants
- A description of prioritization methodology
- A prioritized list of facilities and systems
- A list of facilities to be included in the Security Vulnerability Assessment

Task 1 Specialties:

- Customized software that enhances performance efficiency and allows interactive projection of results during the team meetings.
- Experience which facilitates the rapid completion of this task.

Task 2 Threat Assessment

Three key issues will be addressed in Task 2:

Physical Threat Assessment - The objective of this part of the task is to gain an understanding of the nature and motives of groups or individuals who might wish to cause harm to utility facilities or its customers. Law enforcement and military experts on the Project Team (based on their knowledge, experience, and consultation with authorities) will gather information about possible sources of threat, their motivations, past activities, modus operandi, and possible interest in utility facilities. In addition to terrorist acts, the Project Team will analyze sabotage threats. These results will be used to determine the likelihood of attack for each of the scenarios.

Cyber Threat Assessment - The Project Team will analyze the utility SCADA System for potential vulnerabilities via the internet, dial-up links, or direct access to control equipment by unauthorized personnel. These vulnerabilities, in conjunction with the Physical Threat Assessment, will provide a likelihood of attack on the SCADA System via electronic methods and identify recommendations for improvement. This portion of the SVA will focus on potential weaknesses and will include an analysis of firewall protection, dial-in weaknesses (if any), and physical security of access points. Particular emphasis on this evaluation will be placed on any modem access points, intrusion detection systems, routers, firewall, switches, and radio and land-based telemetry systems. This SCADA System design does not typically include connections to the business network, so an Information Technology assessment is not planned for this Cyber Threat Assessment task, however, specific concerns will be addressed as appropriate.

Additionally, a review of IS and SCADA policies will be conducted. This will include a review of e-mail policies, acceptable internet use policies, password policies, hiring/termination policies, anti-virus policies, system log policies, incident response policies, remote access policies, system/network administrator certification and training policies, backup and restore policies, and business continuity disaster recovery plans and policies. We will be performing the Cyber Security Analysis, however we understand that the District has a SCADA subcontractor that will be available to assist us during the study.

Optional – Chemical, Biological, and Radiological Threat Background Information – A technical memorandum detailing the impacts of chemical, biological, and radiological contaminants can be provided to the utility as background information for the Scenario Identification and Analysis (SIA) Sessions. Please note that this technical memorandum is not required by the EPA, however, it will provide greater insight to potential threats and so has been included as an optional task.

Task 2 Deliverables:

- A list of all data gathered and records researched to determine threats
- An analysis of vulnerabilities to cyber threats and recommendations for correction
- *A background information technical memorandum describing chemical, biological, and radiological threats*

Task 2 Specialties:

- Experience in security and threat assessment maximizes the value of the Physical Threat Assessment results.
- Experience in water system design and construction enhances our understanding of the chemical, biological, and radiological threats and their impact.

Task 3 Analysis of Priority Level A Facilities (Facility Characterization, System Effectiveness Determination, and Risk Assessment)

The objectives of Task 3 are as follows:

- Identify a comprehensive list of scenarios for possible avenues of attack, and existing safeguards that may prevent or mitigate an attack
- Determine a consequence level for each scenario

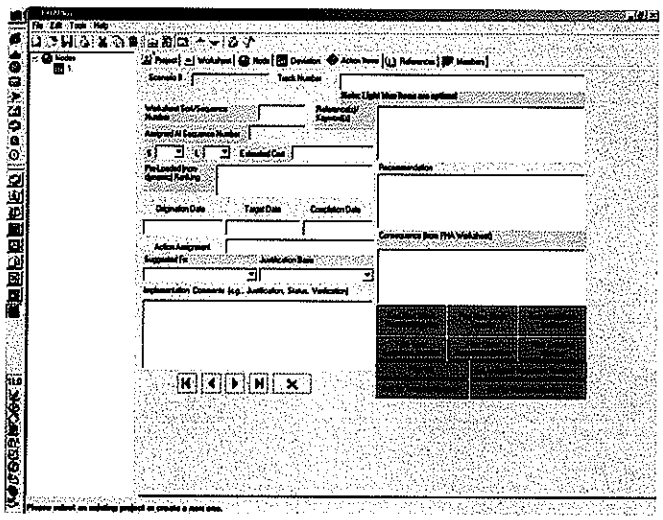
- Determine qualitative probabilities for each scenario
- Determine the risk of each scenario
- Create a preliminary list of recommendations

For Priority Level A facilities, the Project Team and utility personnel will conduct inspections of the facilities, and determine both the likely routes of attack and any safeguards already present to prevent or mitigate an attack. Facilities will be photographed during the inspections. Our experience has shown that extensive use of facility and equipment photographs has been conducive to creating a high-quality product.

Brainstorming sessions (Scenario Identification and Analysis (SIA) Sessions) will be held with the Project Team and utility staff to identify scenarios, their consequences, their safeguards, and their severities. Both hardware and administrative/operational procedures will be taken into account when determining safeguards. During the process, the Emergency Response Plan, the emergency training practices, and utility administrative policies, procedures, and programs will also be assessed. Safeguards will be categorized as Deterrence, Detection, Delay, Response, or Other.

In addition to the core members, various experts from both the Project Team and utility staff may be invited to portions of the meeting to provide insight into particular scenarios.

The SIA Sessions will produce a list of specific recommendations for protecting vulnerable water distribution system elements, enhancing the physical security of the facilities, modifying existing administrative programs and procedures, and updating the Emergency Response Plan. Recommendations will be categorized based upon implementation, for example: as Security Hardware, Administrative, etc.



Risk Management Professionals' custom software (PHAPlus™) will be used to record and document the sessions, and for tracking recommendations. This software includes support for Security Vulnerability Assessments, and as a value-added benefit, RMP, will provide a copy of PHAPlus™ to provide flexibility and the option to perform periodic updates. RMP is the only Security Vulnerability Assessment specialist with this particular capability.

Task 3 Deliverables:

- Facility photographs, site sketches, and/or other appropriate documentation (the delivery CD at the end of the project will include all original digital image files (JPG), as well as a cataloged collection (using MS PowerPoint) suitable for report documentation and referencing)
- A description of the physical system (production, distribution, storage, population, area, etc.)
- A description of water sources and their locations
- A report section documenting the methodology used to determine the scenarios
- A worksheet containing the scenarios characterizing malevolent acts, existing safeguards, and risk of the scenarios for critical facilities (will be incorporated into and enhanced in later tasks)
- A preliminary list of recommendations that will include a brief description and basis
- A complementary copy of PHAPlus™ Software at project completion

Task 3 Specialties:

- Use of PHAPlus™ enhances performance efficiency and has an integrated action item tracking tool for SVA recommendations that saves time and effort for SVA follow-up activities and minimizes the potential for the non-completion of recommendations (which are predicted to be a subject of future USEPA or DHS audits).
- The SIA Session approach used by Risk Management Professionals is a hybrid approach where we have adopted some of the practices that we have employed for years in the performance of safety assessments. A unique feature of our SIA Sessions is the use of two individuals and two personal computers to help efficiently guide the Project Team. One individual uses a personal computer to display key photographs from our walkdowns, using a projector, to help focus and guide the team discussions, while the other individual records key information using the PHAPlus™.

Task 4 Prepare Report

A complete Security Vulnerability Assessment Report will be provided to the utility and will include the following:

- A summary of the methodology and approach employed, including prioritization criteria
- A prioritized list of facilities reviewed
- Names and qualifications of both Project Team and utility members
- A ranked list of scenarios identified for critical facilities, along with existing mitigation features
- Final prioritized list of recommendations
- An EPA submittal document

During the Project Initiation Meeting the report contents will be reviewed with the Project Team and adjusted as necessary to optimize report usefulness. The table on the following page contains a typical table of contents for one of our Tier II SVA Reports.

All reports and deliverables will undergo a thorough quality control review process by the Project Team before delivery. In addition, a draft of each portion of the report will be issued for key utility personnel to review and approve so their comments can be incorporated into the final version.

As noted in the preceding section, all reports and work products will be treated as confidential materials and will be strictly controlled by all members of the Project Team.

Task 4 Deliverables:

- Draft Reports for Review
- Final Security Vulnerability Assessment Report (5 hardcopies and a CD containing all electronic files)
- All Security Vulnerability Assessment Supporting Documentation
- EPA Submittal Document

Task 4 Specialties:

- Unlike many pure security firms, the RMP Team Members are accustomed to report writing and the logistics associated with producing a quality report.

Example Tier II SVA Report Table of Contents

TABLE OF CONTENTS

Note: Appendices are not included in the EPA submittal

Task 5 Project Reporting (Optional)

RMP will present the SVA report at 90% completion to utility management to discuss process and results. This proposal has been prepared using the assumption that only one such meeting for a management presentation will be required. Since this meeting is not required for successful completion for the EPA, it has been presented as an optional task.

Task 5 Deliverables:

- *A formal presentation to utility management*
- *Presentation notes*

Task 6 Security Enhancement/Prioritization Plan (SEPP) – Capital Improvements

Recommendations precipitating from this SVA are expected to include recommendations for capital improvements, such as installation of tamper-resistant equipment, alarm and surveillance systems, etc. While the utility can develop cost and schedule for these items on its own, we find that many clients wish to determine the budget and schedule, and so we have included this. An estimated Security Enhancement Plan and justification for the proposed capital improvements will be developed to explain why and how recommendations should be completed. Project estimates will be detailed enough to prepare construction cost, annual operations, and maintenance cost estimates within approximately 30 percent of actual costs. The cost estimate provided in this proposal is based on approximately 20 prioritized security and 20 prioritized engineering related recommendations.

The Project Team will develop a security strategy that balances industry standards with critical Facility specific conditions. This development is commonly called "Security System Integration". The strategy shall address physical equipment (types, locations, ranges, etc.), operational procedures, alarms, tiers of protection, etc. The Project Team will meet with stakeholders while developing this strategy. Please note that system integration, while highly recommended, is not required by law or regulation as a part of the Security Vulnerability Assessment.

Task 6 Deliverables:

- A report of the capital improvement recommendations including the following:
  - A description and basis for the capital improvement projects
  - A possible implementation schedule for each capital improvement project
  - Preliminary construction/maintenance cost estimates
  - Preliminary estimate for annual operating and maintenance expenses

Task 6 Specialties:

- In their field of expertise, NWTC is extremely well qualified for developing effective recommendation implementation plans and budgets.

Task 7 Emergency Response Plan (Optional)

The Emergency Response Plan will be updated using the scenarios postulated and ranked in the preceding tasks, as well as ensuring that the Emergency Response Plan is compatible with Standardized Emergency Management System (SEMS) specifications. SEMS specifications were originally developed to apply to state and local emergency response agencies and to standardize response to emergency involving multiple jurisdictions or multiple agencies. However, a good quality facility Emergency Response Plan should be compatible with SEMS to allow a smooth interface with the operations of the municipal emergency response agency to ensure effective response to an emergency and provide the ability to operate under Unified Command.

The Emergency Response Plan will be updated to address each threat scenario, and the identification of potential weaknesses. The Emergency Response Plan will incorporate the recommendations developed by the team.

Task 7 Deliverables:

- *A list of recommendations to incorporate into the Emergency Response Plan*
- *An Emergency Response Plan with recommendations incorporated*

WORK BUDGET

Risk Management Professionals, Inc. will conduct the proposed primary effort as described in this proposal on a time and materials basis with a not-to-exceed budget of $19,925.00 (not including the recommended optional tasks described in the Cost Summary). The following page provides a detailed summary of this budget, delineated by task.

During contract negotiations, we would be happy to discuss mechanisms for maximizing value and reducing cost, by varying task scope or through direct involvement of your personnel.

As part of the cost summary, Risk Management Professionals, Inc. has partitioned the estimated Project Team personnel labor hours per task, including classification and billing rate, for each task separately. Included in this section is a table detailing the estimated involvement hours of all Project Team members listed by tasks as described in the scope of work in this proposal. In addition to the cost summary, we have further provided a standard rate schedule including hourly rate for each person assigned to this project and any other applicable direct costs, such as mileage and travel expenses in Appendix B.

Invoices will be issued monthly, and will include a brief description of project work conducted within the billing period and a breakdown of the fee, by the hours charged and individuals charging those hours.

Cost Summary for the City of Paso Robles Security Vulnerability Assessment

Please see legend below for billing rate information for each job classification.	RMP			NWTC, Inc.
Project Management Job Classification	PC	PE II	TS	SSC
Primary Tasks:	Hours	Hours	Hours	Hours
Project Administration	5			
PHASE 1:				
Task 1 - Project Initiation				
Kickoff Meeting and Familiarization Training	4	2		
Facility Prioritization	6	6		
Task 2 - Threat Assessment				
Physical Threat Assessment (Assessment of Potential Adversaries)		4		20
Cyber Threat Assessment	2	14	4	
Task 3 - Analysis of Priority Level A Facilities				
Walkdowns - High Priority Facilities	9	7	3	
Scenario Identification and Analysis (SIA) - High Priority Facilities	27	18		
Risk Analysis and Recommendation Prioritization	6		2	
Task 4 - Prepare Reports				
Report Generation	5	4	12	
PHASE 2:				
Task 6 - Capital Improvements				
Security Enhancement / Prioritization Plan (SEPP)	8	14	2	
Recommendations Review with Client	3			
Subtotal of Primary Tasks	$9,750	$6,210	$1,265	$2,700
Total Project Cost for the City - Primary (Non-Optional) Tasks Only	$19,925			

Recommended Optional Tasks:

Phase 1: Task 2 - Threat Assessment				
Chemical/Biological/Radiological Threat Background Information Technical Memorandum	1	4	1.5	
Phase 1: Task 3 - Analysis of Priority Level A Facilities				
Participation by NWTC in SIA Sessions				16
Travel Cost for NWTC Participation in SIA Sessions				$1,400
Phase 1: Task 5 - Project Reporting				
Management Presentation	3		1	
Phase 3: Task 7 - Emergency Response Plan Update*				
Emergency Response Plan Update	10	18	8	

LEGEND:	
RMP	Hourly Rate
PC - Principal Consultant (SRM, STM)	$130
PE II - Consultant/Project Engineer II (DLJ, JAL, MGM, RER)	$90
TS - Administrative/Technical Specialist (KDS)	$55
NWTC, Inc.	
SSC - Senior Security Consultant (BPF, HS, KSP, JAS, MG)	$135

- Please note that five copies of the SVA Report are included in the estimated budget. Additional copies may be requested at $150 per copy.
- The optional items should be treated as separate tasks. Customer may choose to perform any or all tasks separately, at its discretion, to offset the project cost.
- During contract negotiations, we would be happy to discuss mechanisms for maximizing value and reducing cost (possibly 5-20%), by varying task scope or through direct involvement of City personnel.

* Although not specified in the RFP, an Emergency Response Plan Update has been included as an optional task to comply with EPA requirements.