

To: Anitian Enterprise Security Date of Request: September 20, 2007
Consultant

From: King County Elections Tabulation Upgrade Security Review/
Department/Agency Threat Analysis
Work Order/Project Name

Work Order Response is due to requesting Agency by: October 1, 2007

Please check appropriate box

- Category A – IT PM
- Category B – IT Solutions
- Category C – Tech Plan and Consult
- Category D – Security & Privacy
- Category E – Training
- Category F – Tech Writing & Documentation
- Category G – Quality Management

Scope of Work (Sections A – D) Responses to this Work Order must be in alignment with the Master contract:

- Agency to complete

- Consultant to complete

Section A. Objective

Agency: Objective

Contract to have a Security Review threat assessment performed of a voting system as part of the acceptance testing process for new tabulation system and software to ensure that threats and vulnerabilities can be identified, mitigation strategies developed and public trust and confidence in the voting system maintained.

Agency: Will your Work Order Need

- *Hardware Yes No
- *Software Yes No
- *Intellectual Property Yes No
- *Non Disclosure Agreement Yes No
- *FTA Yes No

For each **Yes** item identified, attach the correct and completed Addendum to this Work Order

Section B. Description

Agency: Description of Task/Service

- Security Review Threat Assessment Background – pursuant to motion adopted by council 2007-0402, the threat assessment of the Premier Elections Solution (formerly Diebold) Assure 1.2 voting system shall be done within the parameters of the real world election environment in King County.
 - The King County Elections Security Plan (page 3) states that:
 - "Effective security does not rely on a single process, feature, or policy. Effective security requires a number of interrelated processes, systems, and policies that complement and build on each other." The systems, process and policies that comprise layers of security for King County Elections (KCE).
 - The Overview of the California Top To Bottom Review further illustrates this point:
 - "Security traditionally relies on layers of mechanisms; this is called *defense in depth, layered defense, or separation of privilege*. The idea is to force an attacker to breach several security mechanisms to compromise the system, rather than one. Procedures form some of these layers of defensive mechanisms. Proper system configuration and implementation form additional layers of defensive mechanisms. Security plans should *always* rely on multiple layers."
 - "If a problem is discovered, the people who know the law and election policies and procedures can modify their policies and procedures appropriately to attempt to address a problem."
 - "Therefore, the results of this study must be evaluated in light of the context in which these systems are used. This emphasizes a Key point often overlooked in the discussion of the benefits and drawbacks of electronic voting systems: those systems are part of a process, the elections process; and the key question is whether the election process, taken as a whole, meets the requirements of an election as defined by the body politic."
 - "It is commonly accepted that no computer-based system, called an information technology system can be made completely secure."
 - To protect against individuals that have greater access to the hardware and software, a system of defenses that provide for detection of inappropriate activity is critical. The systems employed need to provide this capability and Elections' procedures must implement and enforce this capability.
 - It is within this frame work of King County Election's procedural and physical security that the security review threat assessment of the upgraded vote tabulation system in King County is to be evaluated; so that security concerns can be identified and associated risks mitigated so that voters can have trust and confidence in the voting system in King County.
- The objective of the security review is to identify security threats and vulnerabilities and to develop and document mitigation strategies to maintain public trust and confidence in the voting system.
- Components of Threat Assessment – to be conducted by experts in computer security

and elections professional(s) experienced in the administration of elections:

1. Reviewing the Independent Testing Authority reports from federal certification process as a starting point for the threat assessment. Identify areas not covered by the federal process and review/test those areas.
2. With understanding that the California Top To Bottom Review was done on an older version of the product suite; review the new suite and documentation to determine if issues identified in the California Top To Bottom Review with the TSx and GEMs equipment and systems have been mitigated in the new version of the solution suite and if not, if KCE procedures sufficiently protect against remaining vulnerabilities.
3. Review the report "Software Review and Security Analysis of the Diebold Voting machine Software" done for the Florida Department of State and examine if any of the flaws documented in the report have been mitigated by the newer version of the TSx software and if not, if KCE procedures sufficiently protect against remaining vulnerabilities.
4. Unless the contractor identifies areas they feel were not adequately addressed, the contractor is not to duplicate the efforts of the ITA, California TTBR, or Florida review. Before duplicating any effort, the contractor shall seek the concurrence of the county.
5. Employ voting system threat modeling by examining the inputs and outputs of the system to assist in determining the structure of the intrusion/penetration testing including but not limited to components number 6, 7 and 8.
6. Intrusion or penetration testing of the ballot tabulation system
 - Reviewers will conduct intrusion or penetration testing, of the functions and performance of the Premier Elections Solution Assure 1.2 voting system, to identify and document vulnerabilities, if any, to tampering or error that could cause incorrect recording, tabulation, tallying or reporting of votes or that could alter critical election data such as election definition or system audit data. This testing will be conducted in secured King County Elections' facilities.
7. In order to facilitate an understanding of the system its uses and functions the contractor shall provide a technician to be an operator as part of the tabulation team conducting the mock election and volume testing that are part of the acceptance testing process. The technician will be required to participate in training conducted by the vendors and King County Elections.
8. Finally, the following specific security features or potential vulnerabilities of the of the system will be evaluated
 - Is the encryption of the database implemented in a secure way and in such a way as to make meaningful manipulation of the database impossible?
 - Can the database be accessed outside of the GEMS or CTS system?
 - Are the program certificates of authentication implemented such that the certificates can be trusted to ensure application programs in use are the original unmodified federally certified applications?
 - Can the results from a ballot that was electronically duplicated be manipulated outside of the CTS application?
 - Is it possible to preview cumulated election results within or outside the system going around established procedures and if all security features (including smart card technology) are properly implemented?

- Is the database replication among scanner units performed in a secure manner?
- Is application level access control performed by the security module adequate – can rights, privileges, use of smart card etc be bypassed or escalated outside of the application?
- Are the scanned ballot images stored securely? Is it possible to access ballot images by bypassing any security controls?
- The contractor will inform the County of any software tools and methods needed to facilitate the threat assessment. All software tools necessary to conduct the threat assessment will be provided by the consultant.
- Collaboration with Elections Administration Expert(s) – consistent with the intent of the council it is required that the threat assessment include an election administration expert(s) to ensure that testing occurs in real world election environment and to assist with identifying policies and procedures to be used as mitigation strategies.

Consultant: Proposal (Description of approach to the task/Service specified)

Anitian Enterprise security is honored, once again, to respond to a King County work order. Anitian has put together a project plan and proposal that will ensure King County receives a thorough and comprehensive risk and security analysis of their elections systems.

The Anitian Advantage

Anitian is the best choice for this project for the following reasons:

- **Experience:** Anitian has already completed numerous assessments for King County (including the BHIP assessment last year) with great success. The lead Security Analyst on this project has been performing application security assessments for over 7 years. In his previous job, he worked as a defense contractor and audited numerous DOD web applications, and most recently performed the security assessments of both the King County PeopleSoft Portal and the DSP/Cerberus application. Anitian is very familiar with the King County environment both technically and politically. We have a strong rapport with King County CISO and other IT managers. Mostly, Anitian has repeatedly met and exceeded the expectations of King County.
- **Expertise:** Anitian will provide King County a team of world-class security and elections experts for this project. Moreover, Anitian will provide an industry veteran in elections systems and practices for consultation.
- **Methodology:** One of the hallmarks of Anitian is our use of the scientific method for security analysis. Unlike many security analysts who rely on speculation, checklists and generalized risk profiles, Anitian customizes our analysis for each engagement, based on the practical and realistic threats and risks that are possible for an environment. Furthermore, we draw all conclusions from observable facts, not speculation or hype. Our results include detailed proof and evidence that support our conclusions. The end result is a realistic and reliable

Consultant: Proposal (Description of approach to the task/Service specified)

security assessment that the citizens and employees of King County can trust.

- **Value:** Anitian respects the tight timelines and budgets of King County and will deliver this project on time and within a reasonable budget.

Overview

Anitian views this project fundamentally as a risk analysis project. We will conduct a series of tests and reviews to analyze the security risks and threats relevant to the new King County elections system.

Anitian proposes the following general tasks for this project:

- **Documentation Review:** Anitian and the elections expert will thoroughly review all the existing documentation and procedures for the elections system as well as all previous security reports.
- **Interviews:** Anitian will interview KCE staff and determine how well staff understand and follow procedures. Anitian will also assess the general awareness of security issues and practices.
- **Gap Analysis:** Anitian will compile all the data of the documentation review and interviews and produce a Preliminary Security Assessment Report that will outline the risks or security weaknesses that pose a realistic and practical threat to KCE and the elections process. Anitian will specifically highlight any issues that the previous reports have not addressed or that KCE has failed to mitigate.
- **Technical Analysis & Mock Election:** Following the documentation review, Anitian will conduct a series of technical reviews and tests on the KCE GEMs and TSx system(s) and supporting infrastructure. The focus of this phase is to validate (or invalidate) any concerns discovered during the Gap Analysis phase. This phase will also consist of monitoring a mock elections cycle.
- **Reporting:** After the Technical Analysis & Mock Elections, Anitian will compile all our findings in to a Security Assessment Report.
- **Executive Briefings:** Anitian can provide on-site executive level briefings for Commissioners and other management to present our findings.

Approach & Philosophy

Anitian has a unique approach to security assessment. Unlike many security firms that focus on "laboratory" style testing using very rigid requirements, Anitian focuses on "real world" testing and analysis using scientific methods. This philosophical basis results in assessments that are firmly grounded in the operational realities of an organization and not theory or speculation.

When performing risk analysis, all threats have two fundamental components:

- **Severity:** This defines the seriously or potential for damage that a threat possesses. For example, a system configuration that could cause a user to destroy an entire database, would have a very high severity. However, a threat that may

Consultant: Proposal (Description of approach to the task/Service specified)

cause some user preferences to be lost, but not affect the core operation of an application would have a much lower severity. Severity usually, but not always, is a fixed variable. The severity of a risk often remains the same regardless of safeguards or other mitigating factors.

- **Probability:** This defines how likely an threat is given the environment. For example, a virus infection in an unprotected network has a fairly high probability. Likewise, virus infections are very unlikely on a system that has no network connection to the Internet and tight control over removable media. Probability is a very dynamic and volatile component of risk analysis. The existence of safeguards, processes, practices, internal organizational culture and many other factors can significantly alter the probability of a threat.

Anitian's risk analysis process can be summarized in the following process:

- **Determination of Risk:** What threats exist in the environment ("*possible* risks") that can plausibly be exploited. In this phase Anitian will specifically rule out "impossible" threats. For example, for the KCE system, an Internet denial of service attack is impossible since the system is not connected to the Internet.
- **Risk Grading:** What is the severity and probability of the identified threats. This is based on careful analysis of the potential damage a threat can cause and the probability of it actually happening.
- **Determination of the Credible:** Based on a review of the severity and probability of threats, Anitian determines what threats are most *probable and credible*. A credible threat is one that has some probability of happening and/or the severity is high-enough to warrant protection measures regardless of the probability.
- **Determination of Safeguards:** After analyzing the threats, Anitian determines what reasonable safeguards can be implemented to reduce the severity or probability of the threat. Safeguards may include processes, policies, technologies, modifications to existing systems or a combination of some or all of these options.

Our Security Assessment Report will specifically address each of these issues. We will summarize the risk grading and probable events in our Findings section of the report. The Recommendations section will outline the suggested safeguards.

In the case of elections systems, the ultimate threat is the corruption or altering of election results. This risk is, of course, very severe leading to the potential disenfranchisement of voters and significant loss of confidence in government operations.

Given this extreme risk, Anitian will focus our effort on determining the probability of any risk being successfully exploited. Naturally, if the probability is extremely low or non-existent for a particular threat, we will dismiss the threat as improbable.

Consultant: Proposal (Description of approach to the task/Service specified)**Assumptions**

Anitian has bid this project based on the following assumptions.

- **Code Review:** Anitian does not anticipate needed to perform detailed review of source code of the GEMs or TSx systems or relevant databases. Code review is only necessary if the applications or database demonstrate a serious, endemic flaw. If our analysis determines that a detailed source code review would be beneficial to the project, Anitian will discuss this option with KCE staff. Code review work would alter the project scope and cost. Code review work would have to be bid separately. Hourly rate for code review work would be \$250.00 per hour and a typical code review project requires 200 to 300 hours of consulting services.
- **On-site Work:** Anitian estimates that this project will require about three weeks on-site at KCE. This may change based on findings or analysis work.
- **Non-Production Environment:** Anitian understands that security testing will be performed against non-production, test systems and networks that have an identical (or nearly identical) configuration to the production environment.
- **Isolated Network:** Anitian understands that all elections systems are located on a private network that has no public access whatsoever. All testing and scanning will be performed on the local, private network.
- **Confidential Information:** Anitian understands that this project involves a great deal of confidential information. Moreover, Anitian respects the sensitive nature of this project and its potential political implications. Anitian will ensure that all project materials and communications follow strong security measures to protect data. Moreover, Anitian specifically agrees to not discuss the details or findings of this project with any third-party, including members of the press, without explicit written approval from KCE or the King County Council. All other terms of Anitian's agreements with King County will remain in full effect.
- **Focus on Tabulation:** Anitian understands that the majority of this project will focus on the tabulation systems. KCE is moving to an all mail-in system and therefore will have limited polling locations and polling machines. While, Anitian will conduct risk assessment and security analysis on polling systems, our efforts will be predominately focused on the tabulation systems.

Section C. Deliverables

Agency: List anticipated deliverables with frequency of status reports.

- During the threat assessment, status reports shall be provided to King County Elections on the progress at least weekly, or more often if significant issues arise.
- If during the penetration testing a vulnerability is detected that is of such magnitude that a targeted source review is warranted, Anitian shall report this to the King County Elections Management Team, the King County Council Policy Staff Director and King County's Chief Information Security and Privacy Officer.
- After completion of the threat assessment and prior to the release of the final report, the King County Elections Management Team, the King County Council Policy Staff Director, King County's Chief Information Security and Privacy Officer, and member from Agora (a professional organization of private and public information security experts) will be briefed and review the draft of the final report.
- Report pursuant to King County Council Motion 2007-0402 (Section D) "Within 10 calendar days after completion of the security testing by third party experts, a report of the results prepared by the third party experts shall be simultaneously provided to the executive, the council, the citizens' election oversight committee, the public and the media." All specific data that could compromise the security of the voting system, other King County's information assets or compromise the vendor's proprietary rights will be included in a separate appendix provided to King County Elections but not publicly released.

All reports will follow the work order objective of identifying security threats and vulnerabilities and documenting mitigation strategies to maintain public trust and confidence in the voting system.

Consultant: Proposal (Description of deliverables and timing)

This may be adjusted at a later date in the development of the project plan but provide estimates.

WORK PERFORMED AND DELIVERABLES

This section details the work Anitian will perform for each phase of the project as well as the deliverables involved.

1. Project Planning & Discovery

Anitian's analysts will meet with relevant King County staff to gather requirements and expectations. The main goal of this phase is project logistics and will consist of the following general tasks:

- Introductions: meet staff members and exchange contact information.
- Walkthrough: An informal walkthrough of the KCE environment.
- Alignment of Expectations: Discuss project goals and expectations with

Consultant: Proposal (Description of deliverables and timing)

This may be adjusted at a later date in the development of the project plan but provide estimates.

KCE staff.

- Timeline: Review proposed schedule and adjust accordingly.
- Discovery: Gather documents from KCE staff. cursory review to ensure completeness and relevance.

Deliverables

- Project Definition Document which contains:
 - Statement of goals and expectations
 - Project plan & detailed schedule.
 - Contact information for project participants.
 - Reiteration of assumptions and known issues.
- List of requested documents.

Duration: 2-5 days

2. Documentation Review:

Anitian and the elections expert will review all the relevant documentation and methods. Anitian will use this phase to determine what, if any gaps exist in the security of the KCE system(s) and their implementation of the GEMs and TSx systems. This phase includes a review of the following documents:

- Federal Independent Testing Authority reports
- California Top to Bottom Review materials
- Current documentation for the GEMs and TSx
- Software Review and Security Analysis of the Diebold Voting machine Software done for the Florida Department of State.
- Existing KCE security policies and procedures
- Network & system design and deployment diagrams or documents.
- Any other relevant documentation that KCE identifies.

Deliverables: This phase will not have any specific deliverables to KCE.

Duration: 10-14 days

Consultant: Proposal (Description of deliverables and timing)

This may be adjusted at a later date in the development of the project plan but provide estimates.

3. Staff Interviews

Anitian will meet with key elections staff members to discuss their roles, responsibilities and practices with the KCE systems. This may involve some demonstrations of the systems and their function. Anitian will work with KCE to identify the correct personnel to interview based on roles and responsibilities.

Deliverables: This phase will not have any specific deliverables to KCE.

Duration: 10-14 days

4. Gap Analysis & Threat Modeling

This is a critical phase of the project. At this point, Anitian and the elections expert will have an understanding of the KCE systems and their use. This phase is specifically dedicated to identifying any threats or issues that have been overlooked or require detailed investigation.

In addition to identifying threats, Anitian will conduct threat modeling sessions with internal security experts and the elections expert. This will help qualify any gaps and detail the exact nature of the risk associated to each threat.

Furthermore, Anitian will identify what tools or methods will be necessary to perform security testing during the next phase.

Anitian will specifically focus on the following areas;

- Threats or security weaknesses the previous reports and/or tests have overlooked or failed to address.
- Whether KCE's specific implementation and updated procedures and practices mitigate or eliminate the threats.
- What, if any, general security flaws or weaknesses might exist in the design or implementation of the GEMs or TSx systems.
- How KCE's elections procedures compare to accepted best practices for conducting elections.
- Any missing or outdated documentation.
- The practical risk associated to each identified threat based on the risk analysis methodology discussed earlier in this proposal.

Deliverable: Preliminary Assessment Report

Anitian will document all threats or issues that were identified in a Preliminary Security Report. Prior to publishing this report, Anitian will review each issue with KCE and allow for open discussion regarding the issues and mitigation strategies.

The report will also help focus and direct the efforts of the Technical Assessment and Mock Election. With clearly identified risks, Anitian's analysts can pinpoint

Consultant: Proposal (Description of deliverables and timing)

This may be adjusted at a later date in the development of the project plan but provide estimates areas of concern and establish the true nature of the risk.

Duration: Anitian will require approximately 14-21 days to compile the report, conduct peer review and edit the document with KCE staff.

5. Technical Analysis & Mock Election

For this phase, Anitian and the elections expert will work alongside KCE staff to conduct a series of tests and mock elections (or election processes). These tests will have the following goals:

- Validate (or invalidate) threats identified in the gap analysis phase.
- Identify any additional threats.
- Confirm that documented policies and procedures are being followed.
- Confirm the proper operation and security of the GEMs and TSx systems.

Deliverables: This phase will not have any specific deliverable, per se. Rather, all results will be documented in the Security Assessment Report.

Duration: Anitian anticipates this phase requiring 7 to 10 days, but has budgeted for 14 in case some additional issues are discovered.

6. Security Assessment Report

At the conclusion of the technical analysis and mock elections, Anitian will gather all the results of the testing and produce a final Security Assessment Report. A draft version of this document will be released to KCE for review among the council policy staff, chief information security & privacy officer and a member of the Agora group.

The report will contain the following general sections (Anitian may revise this to suit specific content.)

- **Executive Summary:** A high-level summary of the project, its findings and results. This will be about 2-5 pages.
- **Findings:** A nonjudgmental presentation of facts. This section outlines the threats discovered and all relevant information about those threats. It will also define whether a threat is credible or not. It will likely be the same as the gap analysis, but will include the results of the technical analysis and mock election.
- **Recommendations:** Anitian will offer expert suggestions on methods, practices, processes or solutions that can mitigate or eliminate any existing threats that are deemed credible.
- **Technical Data:** Anitian will include complete, raw technical data. This may include a wide variety of data culled from numerous tools and

Consultant: Proposal (Description of deliverables and timing)

This may be adjusted at a later date in the development of the project plan but provide estimates.

systems. The most common example of technical data is raw scanning reports that detail vulnerabilities discovered and their severity.

Deliverables: Security Assessment Report (draft and final versions).

Duration: Anitian will require approximately 21 to 30 days to compile this report.

7. **Executive Briefing:** At the conclusion of the project, Anitian will meet with relevant King County staff or Council members to discuss our results and clarify any issues. This will provide King County an opportunity to question the analysts and discuss the details.

If necessary, Anitian can provide expert testimony to the King County Council or any other governing board. This proposal provide up to 8 hours of executive meetings. Should KCE require additional meeting time, Anitian would need to revise our proposal.

Resources Required

Anitian will require the following resources:

- Access to all documentation pertaining to the development, installation and management of the elections system.
- Copies of all the relevant elections reports.
- 2-4 hours of time with key staff members for interviews and discussions. This would include system administrators, business owners, database administrators, programmers, project managers and security administration staff. Anitian can provide a more detailed list of the people who we will need to meet with after the initial kick-off meeting, where we will learn the roles and responsibilities of the relevant KCE staff members.
- Access to the GEMs and TSx systems and supporting hardware. Anitian will require user and administrative accounts on the relevant systems and/or network. These accounts are necessary to run security tests on different user types.
- Reasonable location to work while on-site. This can be a conference room or available desk. Anitian will provide our own laptops and computer equipment.
- Consultants will require Internet access from time to time to research attacks, upload data to Anitian's network and other administrative purposes. Anitian will only require HTTP and HTTPS access to the Internet.
- A key point of contact for questions and project assistance. Anitian prefers to identify a single person where we can direct all project-management related questions and issues, and who can coordinate our activities.

Consultant: Proposal (Description of deliverables and timing)

This may be adjusted at a later date in the development of the project plan but provide estimates.

PROPOSED PROJECT PLAN

Due to the changes in the original project plan, the following plan is merely an estimate. This plan assumes a start date of February 1, 2008. This schedule can be adjusted based on the actual start date.

Deliverable	Description	Date
Initiate Project	Finalize contracts and establish initial project logistics.	Today – 2.1.2008
Discovery Meeting	Meet with key members of the project to gather information and establish project protocols.	1.21.2008
Detailed Project Plan	After establishing initial contacts and goals, Anitian will produce a more detailed project plan with specific steps, expectations, requirements and dates. This will also include a plan for conducting the penetration tests, specifically times and dates for the tests to occur.	2.1.2008
Documentation Review	Review relevant documents and begin building Preliminary Security Assessment Report	1.21.2008 – 2.1.2008
Interviews	Conduct interviews with staff members.	2.4.2008 – 2.8.2008
Write Preliminary Security Assessment Report	Conduct gap analysis and threat modeling. Document all findings in this report.	2.24.2008- 2.29.2008
Technical Analysis & Mock Elections	On-site work with KCE staff to conduct security tests and review all elections procedures.	2.11.2008 – 2.22.2008
Write Security Assessment Report	Using the Preliminary Report as a baseline, augment report with findings from technical analysis and mock elections. Detail recommendations for mitigating or eliminate any credible threats.	2.25.2008 – 3.21.2008
Deliver Draft of Security Assessment Report	Draft version for KCE and Council review.	3.21.2008
Executive Briefing	Meet with KCE and/or Council members to discuss report and Anitian's findings.	3.24.2008 – 3.28.2008

Agency: Requirements for proposal evaluation.

(List required items or criteria necessary to properly evaluate the consultant's proposal)

Required Items:

- Identified experts in computer security, preference given to expertise in voting systems
- Identified expert or subcontract for an elections professional experienced in the administration of elections who shall be retained as part of the project by agreement of King County Elections.
- Ability and capacity to complete the tasks in the prescribed time frames
- Commitment to a process and review that will help build public trust and confidence in the administration of elections
- No conflicts of interest in the arena of voting systems or the elections administration filed
- A draft project plan that will guide this process showing the ability and capacity to complete the tasks in the prescribed time frames specified in the following section on Duration of Work.
- A sample threat assessment report conducted for another customer. Be sure to redact all customer references.
- A list of three references, for whom your organization has conducted a threat assessments in the past two years.
- Any standard template documents routinely used to conduct a security assessment. Including checklists, questionnaires, reference lists, etc.
- A description of the expected process for conducting a non-destructive penetration test on the described system.
- A sample penetration test report conducted for another customer. Be sure to redact all customer references and system specifics.

Section D. Duration of Work**Agency: List important dates including expected start and completion dates.**

Work Order responses are due by close of business October 1, 2007.

Responses will be evaluated and consultant selected by October 8, 2007.

Work orders signed and distributed by October 12, 2007.

Project work may begin as early as October 19, 2007 but at least by November 7, 2007 (dependent on federal certification) and is expected to be completed by December 14, 2007.

Consultant: Proposal

Include estimated work plan, schedule and assignments. Estimate hours and rates.

See work plan defined in previous section for detailed times and dates. Due to the timeline changes, Anitian can agree to completing this project approximately 90 days after inception.

REQUIRED ITEMS

Expertise: Anitian has adequate in-house and contract expertise in the area of information security. We have proposed three experts in information security and have access to three or four more via contract relationships. Anitian is offering King County a choice for elections experts (see next section).

Building Public Trust: Anitian believes the only way to test security is to follow scientific processes that derive conclusions about security from proven facts. We believe this process will ensure public trust because it is free of bias and political agenda. Anitian also believes in conducting practical, realistic security tests based on what the most probable threats are. We specifically avoid sensational or exotic attacks that offer little or no insight into the real threats a client faces. Furthermore, Anitian is an independent firm with over 12 years of experience in information security. We have no ties to any elections companies or organizations. Anitian has no political agenda and does not have any pre-conceived opinions regarding the security or insecurity of elections systems. We believe any system can be secured with effective controls and management.

Furthermore, Andrew Plato, President of Anitian is an eloquent speaker on matters of information security. He provides the key note address at numerous trade events (such as the Interface trade show in Seattle on November 28th.) Mr. Plato can provide testimony regarding Anitian's results before any necessary body. This testimony will be fair, honest and free of any bias.

Samples: Anitian has included sample assessment reports and some standard checklists. Note that these are just samples and may not be completely relevant to this specific project.

Capacity: Anitian has the in-house staff to complete this project. We also have access to additional resources, should it become necessary to utilize other consultants.

References: Anitian has provided five references (see below) for our own work. The elections consultants we are presenting have also provided their own references. Please note, one of our top references is the CISO for King County.

ELECTIONS EXPERTS

Anitian has contacted all three of the firms King County recommended for sub-contracting. After conducting thorough interviews with each firm, Anitian felt the both Al Davison from Elections Management Solutions, Inc. and Bill O'Neill from Shamrock Associates, Inc. were the most qualified.

KCE has expressed a desire to include Al Davidson as the selected elections expert.

Consultant: Proposal

Include estimated work plan, schedule and assignments. Estimate hours and rates. Anitian agrees with this decision. This revised work order assumes that Al Davidson will be the subcontracted elections expert.

DESCRIPTION OF SECURITY TESTING

Security testing will be performed during the Technical Analysis and Mock Election phase of this project. Security testing for this project will be specialized to handle the unique elections environment. Anitian considers testing to include both technical and non-technical processes. For example, Anitian will likely conduct security and vulnerability scans on key election components (a technical test), as well as testing how election processes are followed (a non-technical test).

Security testing will involve the following general steps:

- **Planning & Hypothesis:** Based on the gap analysis process, Anitian will focus on the most likely ways to effectively compromise the KCE processes and systems. We will plan out the attacks and tactics in advance to ensure efficient use of testing time.
- **Reconnaissance:** The next step is to monitor activity and conduct non-invasive scans. In this step, Anitian will watch how processes are performed or scan systems to see what is running on those systems. The goal of this phase is to determine if what we have planned and hypothesized as probable exploit vectors is accurate. If reconnaissance reveals that our plans were inaccurate, we will revise our tests accordingly.
- **Technical Threat Testing:** Using a combination of commercial and open-source security testing tools, Anitian will determine what, if any, threats are valid in the KCE environment. This will involve conducting vulnerability scans, validating results and executing sample exploits to determine the security posture of the KCE environment.
- **Non-Technical Threat Testing:** Using a variety of methods, the elections expert will walk through a variety of simulations and hypothetical scenarios to determine how KCE staff (and the elections systems) respond to possible threats. These tests will be previously defined in the Preliminary Security Assessment Report.

Since most of these tests (both technical and non-technical) will be performed against a non-production environment, the tests themselves pose very little risk to the operational elections systems. However, Anitian may conduct tests on the main KCE network (with the approval of KCE staff) and those tests do carry some, albeit small, risk of interfering with normal operations. Anitian will make every reasonable effort to eliminate or minimize any disruption to production environments.

SAMPLE REPORTS

Samples of Anitian's reports are included with this work order.

REFERENCES:

Below are some references for Anitian's work. Each of the elections experts also

Consultant: Proposal

Include estimated work plan, schedule and assignments. Estimate hours and rates. submitted their own references which are included as attachments.

King County	Ralph Johnson	Chief Information Security Officer	206-205-9230
PEMCO Insurance	Kip Boyle	Chief Information Security Officer	(206) 628-6339
EthicsPoint	Nick Murphy	Chief Information Officer	(971) 250-4112
Homer Electric Association	Marvin Super	Director, Information Technology	(907) 235-3311
Mentor Graphics	Sean Boyle	Information Security Manager	(503) 685-1542

Section E. Key Personnel

Please list the key personnel you will include in the project and their name, role and hourly rate. Attach resumes of all key personnel to the end of this document. Please do not insert them after this table. Key personnel cannot be changed without concurrence of the county.

<i>Consultant: Proposed Personnel List – (resumes must be attached)</i>		
Name	Role	Hourly Rate
Andrew Plato, CISSP, CISM	Executive Sponsor	Included
Adam Gaydosh, CISSP, CISA, GIAC	Senior Security Analyst	Included
John Van Boxtel, CISSP, CCNA	Senior Security Engineer	Included
Al Davidson	Elections Expert	Included

Section F. Payment

Agency: King County Acceptance Criteria. The following criteria must be met prior to King County approving payment.

- Timely submission of report pursuant to King County Council Motion 2007-0402 (Section D) “Within 10 calendar days after completion of the security testing by third party experts, a report of the results prepared by the third party experts shall be simultaneously provided to the executive, the council, the citizens’ election oversight committee, the public and the media.”
- Completion of an acceptable report detailing identified threats, vulnerabilities and mitigation strategies for each threat/vulnerability combination.
- Report must be well organized and clearly written and understandable to King County elections staff.

Each deliverable must be met and approved as described prior to payment approval.

Work Order

(Consultant and agency will revise based on final negotiation)

<i>Consultant Proposed Payment Schedule</i>		
Deliverable	Cost	Due Date
Security Assessment Work (mandatory) Includes the following:	\$ 57,950.00	
- Project Plan	Included	10.31.07
- Initial Security Assessment Report	Included	11.19.07
- Security Test Plan	Included	12.05.07
- Security Testing Report	Included	12.10.07
- Final Security Assessment Report	Included	12.14.07
OPTION 1: Elections Expert, Al Davidson	\$ 36,750.00	
FIXED PRICE w OPTION 1:		\$94,700.00
<i>Cost of all deliverables must equal fixed price total. \$</i>		

