AMENDMENT OF SOLICITATION NUMBER: P1609-008-LC – STAR-Vote: A New Voting System

ISSUED BY: PURCHASING OFFICE 700 LAVACA, SUITE 800 AUSTIN, TX 78701	TEL. NO: (512) 854-9700 FAX NO: (512) 854-9185	DATE PREPARED: **November 29, 2016**
PURCHASING AGENT ASSISTANT: **Lori Clyde**	AMENDMENT NO.: **1**	DATE OF SOLICITATION: **October 6, 2016**

INSTRUCTIONS TO BIDDERS/PROPONENTS:

IMPORTANT: To be considered a responsible and responsive Bidder/Proponent, you must acknowledge receipt of this amendment before the hour and date specified in the solicitation, as amended, by either:

(i) completing the Name and Address block of this amendment, and signing and returning this amendment with your bid/proposal; or

(ii) **(allowable only if the bid/proposal has already been submitted and there are no changes to your bid/proposal)** by completing and executing this amendment as identified in (i) above and faxing it to the Travis County Purchasing Office. **Note if using this method:** you may not submit changes in prices or other competitive information.

Non-receipt of your bid/proposal and this amendment at the designated place within the date and hour specified may result in rejection of your bid or proposal.

The hour and date for receipt of bids or proposals **[ ] is not changed.**
[X] is changed to the following time and date: January 31, 2017 at 2:00 p.m. CST

DESCRIPTION OF CHANGES: Except as provided herein, all terms, conditions, and provisions of the solicitation referenced above as heretofore amended, remain unchanged and in full force and effect.

This Amendment No. 1 is issued to:

1) Change the due date from December 16, 2016 at 2:00 p.m. to January 31, 2017 at 2:00 p.m.

2) Clarify and revise the RFP in accordance with the attached "Questions and Answers for Bid #P1609-008-LC – STAR-Vote: A New Voting System" document provided through BidSync.

   Questions 32, 46, 54, 57, 59, 60, 61, 63, 68, 71, 73, and 84 constitute actual revisions to the RFP requirements.

   The responses to the remaining questions clarify the RFP requirements.

   By signing this Amendment No. 1, Proposer acknowledges and agrees that Proposer has received and reviewed the contents of this Amendment No. 1.

Proposers are required to sign and return this Amendment with their proposal response.

Note to Bidder/Proponent: Complete and execute (sign) your portion of the signature block section below and return to Travis County.

LEGAL BUSINESS NAME: _____ BY: _____ SIGNATURE BY: _____ PRINT NAME TITLE: _____ ITS DULY AUTHORIZED AGENT	☐ DBA ☐ CORPORATION ☐ OTHER DATE:
TRAVIS COUNTY, TEXAS BY: for Bonnie Floyd CYD V. GRIMES, C.P.M., CPPO, TRAVIS COUNTY PURCHASING AGENT	DATE: 12-2-16

Question and Answers for Bid #P1609-008-LC - STAR-Vote: A New Voting System

Overall Bid Questions

Question 1

Do you need to register to attend the Pre-bid conference? If so, who do you register with in the County? **(Submitted: Oct 12, 2016 9:42:48 AM CDT)**

Answer edit

- No, you do not need to register to attend in person. **(Answered: Oct 17, 2016 10:38:56 AM CDT)**

Question 2

Will a call-in conference line be available at the pre-bid conference for others who cannot attend in person? **(Submitted: Oct 15, 2016 8:28:09 AM CDT)**

Answer edit

- On-site is preferable, but a conference line will be available. If you would like to participate via conference call, please email lori.clyde@traviscountytx.gov no later than 3:00 p.m. CT, October 18, 2106 and the conference call information will be sent. **(Answered: Oct 17, 2016 10:38:56 AM CDT)**

Question 3

Can you provide more information about the Risk Limiting Audit (RLA)? Specifically, what form will the RLA take? Is there a whitepaper or technical document that defines the RLA; if so, where can we find it? Which required Elements (as defined in the RFP) are affected by the RLA, and what is each Element's role in the RLA? **(Submitted: Oct 17, 2016 11:28:16 AM CDT)**

Answer edit

- Please see http://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf for description of the RLA. Other resources are also available through an internet search. The RLA is limited to Element B and is supported by each component within Element B through the specifically define data structures of cast vote records, consisting of both the EVRs and PVRs, and the support utilities specified in the RFP requirements. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 4

Can you provide more detail regarding the ADA accessibility requirements for Element C? What specific accessibility features must it include? **(Submitted: Oct 17, 2016 11:29:08 AM CDT)**

Answer

- Accessible features are design dependent and it is the successful proposers responsibility to propose innovative functional design features that comply with ADA and any other applicable state standards for voting and are responsive to the needs of the disability community. Functions such as inserting the ballot in any orientation, use of visual and audio queues and alternative mechanical control(s) are well practiced accessibility features. **(Answered: Oct 18, 2016 5:31:49 PM CDT)** edit

Question 5

Is Element C physically connected to Element B, or is there an air-gap? If physically connected,

who is the responsible party for defining the interface between Elements B and C? **(Submitted: Oct 17, 2016 11:29:56 AM CDT)**

Answer

edit

- Element C is physically connected to the BCS of Element B through the common network shared by the components of the In Person Voting/Tabulation component of Element B. Successful proposers for Elements B & C must submit a proposed interface specification for the interface between Elements B & C and version 1 of the interface specification will be agreed to between the County and proposers during contract negotiations. One of the Element B or C proposers will be assigned responsibility for revision and version control of the interface definition. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 6

What funding source has been allocated for this effort? **(Submitted: Oct 18, 2016 5:16:45 PM CDT)**

Answer

edit

- At the present, $4 million has been budgeted to begin development with follow on County funds anticipated to be requested in budget years thereafter. The County is exploring additional funding sources for this unique governmental project. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 7

What is the estimated cost or desired not-to-exceed limit? **(Submitted: Oct 18, 2016 5:17:12 PM CDT)**

Answer

edit

- No estimated cost has been projected at this time and no not-to-exceed limit set. Successful proposers are aware there is no such thing as unlimited project budgets however and unreasonable cost proposals will not be considered. Cost estimates for individual Elements have been considered by the County based on the level of development or service effort required and the County has reserved the right to selectively award individual Elements based on numerous factors including cost, timeline and overall value to the STAR-Vote system. Awards for all Elements may not be provided as part of this solicitation. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 8

Will a separate solicitation be released for Phase II of this effort? If so, what will Phase II consist of? **(Submitted: Oct 18, 2016 5:17:34 PM CDT)**

Answer

edit

- Phase II will consist of development of the open source versions of the EAC Certified models. A specific time frame has not been determined at this time. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 9

Who is/will be the project manager for this effort? **(Submitted: Oct 18, 2016 5:18:05 PM CDT)**

Answer

edit

- The County will appoint an enterprise-level project manager to manage the integration of the Elements. A specific resource has not been identified at this time. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 10

Does the Department anticipate procuring any services related to the effort? For example: IV&V, QA, Staff augmentation, integration, solicitation prep, etc. If so, what, when and how? **(Submitted: Oct 18, 2016 5:18:43 PM CDT)**

Answer edit

- Travis County is committed to exploring options that will make STAR-Vote a success. At this point, we do not rule out any approach to the project. **(Answered: Oct 18, 2016 5:31:49 PM CDT)**

Question 11

Please confirm that Turn Key bidders can incorporate the Reprivata UL Certified Encrypted Wrapper Solution as part of their overall approach and still be compliant to your bid. The Reprivata UL Certified Encrypted Wrapper covers 1.Voter List database systems
2.Voting Stations and Ballot Box, 3.Vote Tabulation systems to provide an additional layer of encryption according to NSA Mobility Specifications. **(Submitted: Oct 19, 2016 8:59:37 AM CDT)**

Answer

edit

- The proposed Reprivata UL Certified Encrypted Wrapper Solution will be evaluated for its compatibility with the STAR-Vote cryptographic architecture, additional security provided, ease of integration with proposed RFP Elements and cost. Provided the evaluation results in a positive net outcome and adds value to the STAR-Vote system, the Reprivata UL Certified Encrypted Wrapper Solution will be added as a component of the system at contract negotiations. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 12

Can the Government please confirm that Reprivata can submit our proposal explaining the capabilities of our Ul Certified Cyber Encryption solution that is a supporting component to the overall STAR-Vote system, and the cost proposal only. Please confirm that we are not required to follow the instructions delineated in RFP, PART I, SECTION B -REQUIRED DOCUMENTATION (Page 11 of 207).

The Reprivata UL Certified Encrypted Wrapper covers 1.Voter List database systems 2.Voting Stations and Ballot Box, 3.Vote Tabulation systems to provide an additional layer of encryption above the application layer of systems. **(Submitted: Oct 19, 2016 9:22:42 AM CDT)** edit

Answer

- Yes, applicable required documentation must be submitted with your response. If your proposal does not address an item, or a subset of an item, on page 11 of the RFP, a brief statement to that effect is sufficient. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 13

Will County provide a list of vendors participating in the Pre-bid conference? **(Submitted: Oct 19, 2016 1:07:26 PM CDT)**

edit

Answer

- Yes, the list will be uploaded to BidSync. **(Answered: Oct 19, 2016 1:15:42 PM CDT)**

Question 14

The County requests three (3) references similar to County for which the Proposer has provided similar goods or services within the last five (5) years. Is the requirement for "similar goods or services" (i.e., elections equipment) applicable only to the EAC certified components (Part A)? If so, what is the corresponding requirement for references for Parts B through E? **(Submitted: Oct 19, 2016 3:50:31 PM CDT)**

edit

Answer

- Element B: software development; Element C: product development; Element D: software security and testing; Element E: human factors evaluation. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 15

Are proposals welcome that span multiple components, including the EAC certified components, where some components (or parts of components) are implemented by subcontractors? **(Submitted: Oct 19, 2016 3:51:58 PM CDT)**

Answer edit

- Yes. The only restriction is that an individual proposal may not include both Elements B and D without sufficient safeguards to isolate these Elements from one another. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 16

We would like some clarification on the statement (in section 4.8.4) that "The County will separately contract for the services of the Red Team. The administrator will independently select the members of the Red Team." Who is "the administrator" in this context? (elsewhere, it refers to the administrator of an individual election) Does this mean that the actual personnel who participate on the Red Team must be selected by the County, above and beyond the award of a contract Part D to a specific firm (or firms)? **(Submitted: Oct 19, 2016 3:53:53 PM CDT)**

Answer

edit

- The referenced paragraph appears in Part I of the RFP so is not a requirement, will not be a part of the contract and appears as legacy language from the prior Request For Information (RFI). The County will separately contract for Element D, Red Team Assurance, and proposals for the contract are expected to include complete staffing to fulfill the requirements given in Part II of the RFP that will become part of the contract. The “administrator” referenced in Part I section E, 4.8.4 is the Election Administrator or his/her designee. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 17

We would like some clarification on the statement (in section 4.10.5) that "Support services must have variety, depth, and reasonable costs." What is meant by "depth" in this context? Is variety truly required, and if so, how is variety measured? **(Submitted: Oct 19, 2016 3:55:30 PM CDT)**

Answer

- The referenced paragraph appears in Part I of the RFP so is not a requirement, will not be a part of the contract and appears as legacy language from the prior Request For Information

(RFI). Part I section E, paragraph 4.0 is titled Desired Operational and Performance Characteristics, and are therefore not requirements of the system and can be considered background information that may contain items that cannot be measured. As "desired characteristics", information in Part I section 4.0 should be considered by proposers when addressing the requirements in Part II of the RFP and to the degree the proposal supports the desired intent, scoring will be higher for the Subjective Evaluation as given in Part I, section C, paragraph 4.0. Proposers are free to define the terms given in Part I section E paragraph 4.0 and incorporate these characteristics in their proposals as appropriate. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

edit

Question 18

How flexible is the County likely to be on the intellectual property requirements and, in particular, what concern is County attempting to address by acquiring all intellectual property rights to the developed system?

For example, if a proposer developed the entire system (parts B and C) under a suitable open source license (like that being considered by County for its potential consortium), and commited to FRAND licensing terms for the system to County and any other county that wanted to use it, but kept the intellectual property rights for itself, would that address the County's concern? **(Submitted: Oct 19, 2016 3:59:07 PM CDT)**

Answer

edit

- No, all intellectual property rights in and to the STAR-Vote development efforts for Elements B and C will be transferred to the County upon their creation. The County will consider licensing the intellectual property back to the proposer under FRAND licensing terms to meet proposer's undisclosed objectives and only if such a license is deemed to provide the County with additional benefit. It should be noted, however, that the County intends to develop an intellectual property position and licensing model that is modeled on best practices in the commercial Open Source arena for product development and maintenance during execution of the RFP contracts, and any FRAND licensing opportunities must be compatible with the County's resulting model. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 19

Since the decrypted content of spoiled/challenged ballots does not represent any voter's intent, what is the concern that has led County to not offer the decrypted content on the public bulletin board? **(Submitted: Oct 19, 2016 4:01:19 PM CDT)**

Answer

edit

- At this time, the Texas Secretary of State will not allow populating the public bulletin board with decrypted content, and this requires the public to access the bulletin board from the County network, accessible at the County offices as described in the RFP. The County's intent is to continue discussions, negotiations and provide demonstrations to the TX SOS so that future implementations may support population of the public bulletin board on public networks in Texas **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 20

In places (like section 3.8) where the use of 1-D barcodes is mandated, what is the concern that led to such specificity in the requirement (as opposed to a more general requirement for a computer-readable format, such as a QR code or an OCR font)? **(Submitted: Oct 19, 2016 4:02:26 PM CDT)**

Answer

edit

- The referenced paragraph appears in Part I of the RFP so is not a requirement, will not be a part of the contract and appears as legacy language from the prior Request For Information (RFI). Proposers should provide best-in-class solutions when responding to the requirements in Part II of the RFP, justifying alternate implementations as appropriate. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 21

Are the per-polling-place limits (specified in requirement 2.6.1.5) of 4 BCSs and 40 voting stations arbitrary, or based on some specific concern or external requirement? **(Submitted: Oct 19, 2016 4:03:46 PM CDT)**

Answer

edit

- The specified limits were determined based on practical limitations of polling place facilities, traffic flow within the polling place and the ability of poll worker to manage polling locations. The limitations specified in Appendix B paragraph 2.6.1.5 are the minimum requirements with no upper limit. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 22

Requirements 5.1, 5.2, 5.12, 5.13, 5.14, 6.0, 6.1 and 6.6 all ask for "a file specification" (and some ask for "a preferred interface for importing data from a third-party system", or similar additional information). Is this meant to be a complete file specification (along the lines of a full Google Protocol Buffer description or a JSON schema definition) and a specific interface, or a general description of the type of specification and the type of interface. **(Submitted: Oct 19, 2016 4:05:24 PM CDT)**

Answer

edit

- The objective of these requirements is to obtain from proposers a file specification with as much detail as possible, which can range from a general description to a complete schema definition. The submitted file specifications will be used during contract negotiations to define the development starting point for each interface. The successful proposers responsible for either side of the interface will be a part of contract discussions to define the interface and agree to its definition and the development effort required to implement the interface. The County recognizes the some interfaces will be more defined than others and the intent is to capitalize on any prior knowledge that successful proposers have with respect to each interface. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 23

One of the components that is mandated to have an open source reference implementation is the Polling Location Network Traffic Inspector (hereafter, PLTI) Module (requirement 3.1.4.1). Who is expected to use the PLTI, and how is it intended to work?

From our perspective, it seems that allowing anybody to attach a PLTI to an air-gapped STAR-Vote network would render said network no longer air-gapped, unless the PLTI is in fact an entire computer system with its own trusted boot mechanism that has gone through security audit procedures. Moreover, it seems that 1) the PLTI would need to be in a position to intercept all traffic on the air-gapped network, which essentially requires it to be a router itself, as standard Ethernet switches (as would be expected to be used in the air-gapped network) do not let devices on individual ports "spy on" each other's network traffic; and 2) all the information that might conceivably be captured by a PLTI should also be recorded by every device on the air-gapped network as part of the operation of the Network and Logging Layer. **(Submitted: Oct 19, 2016 4:12:33 PM CDT)**

edit

Answer

- The Polling Location Network Traffic Inspector (PLTI) open source reference module is not used during an election. The PLTI module is used for system testing, maintenance and to allow development of additional or alternate functions or features for the In Person Voting/Tabulation module by third-parties **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 24

What is the concern that led to the restriction that the public bulletin board will only be made available in person at County offices, rather than more generally on the Internet?

This restriction seems to unnecessarily restrict the set of people who can verify the integrity of the election, by 1) requiring them to physically visit the County offices, and 2) requiring them to potentially stay there a significant amount of time to perform the verification. It also seems like it would hinder the development of apps for third-party verification. It is possible that County intended for members of the public to be able to visit County offices and download the bulletin board data to, e.g., a USB stick; but that seems effectively the same as making signed data files available via the Internet, with all the added security drawbacks of allowing members of the public to attach random USB devices to a County system. **(Submitted: Oct 19, 2016 4:16:03 PM CDT)**

edit

Answer

- See response to Question 19. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 25

In Section 3.14, the description of hash chaining says that "even a voter who votes after the altered electronic record is created and checks his or her ballot can detect whether tampering has occurred"... but it is not clear that is the case without the ability for the voter to run their own integrity checking tool over potentially the entire set of bulletin board data, as they need to follow the hash chain back to its beginning (or until they find where the tampering occurred). What mechanism is proposed for allowing voters to run such a tool? **(Submitted: Oct 19, 2016 4:17:53 PM CDT)**

Answer

edit

- The referenced paragraph appears in Part I of the RFP so is not a requirement, will not be a part of the contract and appears as legacy language from the prior Request For Information (RFI). As a new, unique and highly innovative system, not all procedural details have been defined for certain aspects of the system. The County's minimum intent is to build the infrastructure that enables public verification and work with governmental agencies and interested public populations to define the procedural processes to support independent verification in the future. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 26

What is Section 8.0 of Part IV reserved for? **(Submitted: Oct 19, 2016 4:18:25 PM CDT)**

Answer

edit

- Section 8.0 is not applicable to this solicitation. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 27

The precinct hardware configuration closely resembles in a number of significant respects, a

voting system under US patent. Has the County satisfied itself that there are no intellectual property issues with the preferred precinct architecture? **(Submitted: Oct 20, 2016 6:34:07 AM CDT)**

Answer edit

- The County has reviewed existing patents and other intellectual properties and is satisfied there are no present issues; however, the County is continuing to evaluate the intellectual property landscape. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 28

Can you provide the schedule for Phase 1? **(Submitted: Oct 20, 2016 6:37:29 AM CDT)**

Answer

- The project schedule for the RFP will be finalized during contract negotiations and will be based on the responses from successful proposers. The County recognizes the different Elements will have different development timelines and the County will work with the successful proposers to synchronize the schedules. Proposers should submit 'best effort' timelines with the understanding that individual development efforts may be extended based on dependencies on other Elements. It is the County's objective to complete all development within a two-year period. **(Answered: Nov 4, 2016 5:13:16 PM CDT)** edit

Question 29

Homomorphic encryption methods are contemplated for the voting system resulting from this RFP. The federal standards leading to EAC certification for voting systems (VVSG, all versions) require encryption methods carry FIPS 140-2 testing and qualification by the federal government. The State
of Texas requires EAC certification. No homomorphic encryption algorithm carries a FIPS 140-2 designation, thus a system with this form of encryption cannot achieve EAC (federal) and subsequent Texas certification. How does the County plan to deal with this? **(Submitted: Oct 20, 2016 6:39:03 AM CDT)**

edit

Answer

- True, but there are other techniques that have the capability to blanket the homomorphic encryption methods in FIPS qualified methods that the County is investigating. Furthermore, the County intends to submit STAR-Vote as an experimental system under the Innovation Class of voting systems that has been directed to be included in VVSG 2007, which will allow deviation from the FIPS requirement if necessary. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 30

We have some questions about the requirement for "Emergency Paper Ballots", which reads as follows: "In the case of an emergency, such as a power outage or an incident that causes the evacuation of a polling location, Election Judges are instructed to use emergency paper ballots. If this occurs, the paper ballots are deposited in a special ballot box and are managed at the Counting Station using an emergency paper ballot process using the the By-Mail Scanning and Resolution module."

Where and when are the blank emergency paper ballots created? In how many different ballot styles, and in what quantities, do they need to be available at each polling place? Is it desired that they have unique PIDs and PCIDs, similar to those desired for mail ballots? **(Submitted: Oct 20, 2016 7:51:10 PM CDT)** edit

Answer

- The blank emergency paper ballots are produced by the EAC Certified By-Mail product that is part of Element A. The Election Administrator is responsible for specifying the quantities and ballot styles to be available for emergency use and, for the distribution of the emergency paper ballots. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 31

Is it permissible for two separate groups within the same company, or two distinct subsidiaries of the same company, to build the system (parts A/B/C) and perform the red team function (part D), provided there are no overlapping personnel and a sufficient firewall (as between the corporate advisory and brokerage sides of investment banks, or between the editorial and advertising departments in news organizations) is maintained? **(Submitted: Oct 20, 2016 7:56:18 PM CDT)**

Answer

edit

- Yes, this is permissible provided the firewall is adequately described in the proposal and the County determines that the firewall will provide sufficient separation between the two groups. Any proposal submitted with Elements B and Element D with a firewall in the same proposal will be subject to a Pre-Award Survey as given in Part I, Section C, paragraph 2.0 to verify the organizational, operational and procedural aspects of the firewall. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 32

1. Referring to the two RFP clauses shown below: A) Is the vendor relinquishing ownership rights on the source code for the EAC-certified products procured as part of the RFP? B) If there is any additional development or modification made on the EAC-certified system (and/or system components) to customize the system for the County or other counties in a consortium, what does the County own and what does the vendor own? A quick response to these questions is requested, so that we may decide whether to respond to the RFP.

2.1. paragraph 2: Travis County (or a consortium of other STAR-Vote™ counties) must retain all intellectual property and proprietary rights in and to the STAR-Vote™ Elements B, C (only the custom software/firmware for existing hardware) and all legally protectable elements and components of it. This ownership position excludes any rights in Element A, the EAC-Certified products, procured as part of this RFP.

4.15.2: The system must not use any technology, standard, or data format that would preclude Travis County (or a consortium of counties) from retaining exclusive rights to the system's source code if it chooses to do so. **(Submitted: Oct 21, 2016 2:02:43 PM CDT)**

Answer

edit

- The referenced paragraph appears in Part I of the RFP so is not a requirement, will not be a part of the contract and appears as legacy language from the prior Request For Information (RFI). An Addendum to the RFP is being accumulated and will include a new paragraph 4.9 added to Part II, section 4.0, stating the following:

  4.9 Ownership of the EAC Certified Modules of Element A is retained by the proposer. The successful proposer shall provide a sample licensing agreement for the use of the EAC Certified Module with the STAR-Vote system independent of any County or State where STAR-Vote may be implemented now and in the future. The successful proposer agrees the final terms of the license will be determined as part of the contract negotiations. If any of the

submitted EAC Certified Modules require modification to meet the STAR-Vote requirements, the successful proposer is responsible for making such modifications and gaining EAC and Texas certification for the changes. The successful proposer retains ownership of any changes and any such changes are automatically included in the license for use by STAR-Vote. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 33

2) If we propose one or more EAC certified products, and these require modifications for Texas-specific certification and/or for interface updates to interact with other products and we make those updates, do we retain the rights to the product (as a whole, inclusive of both the EAC certified and the new code specific to this project) after deployment? A quick response to these questions is requested, so that we may decide whether to respond to the RFP. **(Submitted: Oct 21, 2016 2:02:55 PM CDT)** edit

Answer

- See response to Question 32. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 34

How do we submit our Documentation showing our UL Cyber Assurance Program UL 2900 Certification and the backup UL Certification Backup Test Report to for you to use to evaluate and for other vendors to use to utilize to wrap their applications to make them more secure? We want submit the information but do not know how to do this. There is no other Open Source UL CAP Certified and approved software that allows all interested parties to review the functionality and the testing that was conducted. Hallmarks of a CoT software Technological Implementation include:
¬ Cloaking of the private IP Address space (RFC 1918)
¬ Use of NSA Suite B level of Encryption or an equivalent alternative
¬ NSA Mobility Access Capabilities Package Architecture
¬ Rigid adherence to NIST CSF Tier 3
¬ Rigid control over DNS within the Encrypted Core
¬ Rigid control over Security Credentials and the issuing Certificate Authority
¬ Submission to qualified 3rd party (UL) testing and assurance.
The CoT Technological Solution utilizes a multi-layered encryption software approach consistent with NSA standards for National Security Systems (NSS). This creates a secure encrypted connection while cloaking the IP accessibility of the edge devices connected to a Community of Trust. Traffic from all the edge devices inside the Community of Trust is policed and anomalous or suspicious traffic is captured and stored in the Central Privacy Authority Intrusion Database. While inside the Community of Trust, Viruses, Trojans and any sort of Malware will be unable to communicate with outside entities and attempts to do so will be flagged for investigation. **(Submitted: Oct 22, 2016 1:16:24 PM CDT)** edit

Answer

- It is recommended that you submit a description of an implementation of your proposed software to provide a security wrapper for the Element B network and devices, including the BCS, Voting Terminals and Ballot Box/Scanner. Please include a description of the hardware requirements and/or the devices that would need to host the product. As this type of product, and potential security advantages, were not contemplated in the RFP, the requirements in the Appendices do not directly apply but should be considered when drafting a description of your implementation. Any information you can provide that allows Element B to securely operate wirelessly is also of interest. It is also recommended that you include evidence of the certifications/testing/approvals carried by your product for governmental standards. If a favorable review results from the County's security and cryptographic team, the potential

inclusion of your system into STAR-Vote will be discussed as part of the contract negotiations. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 35

Can we set a working session with the group who created this package and possibly some bidders (your call) who are willing to look at how our open source multi-layered encryption can be provided to improve security but also the bundled product may allow existing modules to be offered as open source when combined with our solution and then this is the one that is open source while their standard product is protected and proprietary s a stand alone solution. Reprivata provides our software at nominal cost to allow Travis County to provide it to all bidders. This create an open source version that is wrapped in our multi-layere encryption solution that is UL Certified CAP 2900 software. It could fix a business problem and a technical problem and make the solution less expensive because of the architecture and business model. We think it could help the vendors respond to the needs of the project but not cannibalize their existing revenue models and reduce the amount of custom work if they use our software to wrap their software inside the encrypted core. **(Submitted: Oct 23, 2016 8:01:59 AM CDT)**

edit

Answer

- Due to the rules of the closed competitive solicitation process, the County is not allowed to communicate with prospective proposers outside the transparent process provided by BidSync while the closed competitive process is open. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 36

Section 8.10.2 lists Google Protocol Buffer as the interface protocol between Element B and Element C. Does this include use of the proto3 version for C# compatibility? **(Submitted: Oct 26, 2016 11:35:25 AM CDT)**

Answer

edit

- Yes, you may propose the use of the Google Protocol Buffer proto3 for the interface between Element B and C. Please note, however, that the final interface specification will be determined during contract discussions that include the County and the successful proposers for Elements B and C. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 37

Will the 8-1/2” wide paper stock used for the PVR output from element B be flat sheet, fan fold, cut sheet or rolled thermal paper? Has the thickness (weight) of the thermal paper stock been specified, and if so, what is the specification? **(Submitted: Oct 26, 2016 11:37:03 AM CDT)**

Answer

edit

- Flat sheet paper is preferred for usability concerns but other formats will be considered if properly justified. When using rolled thermal paper, curling of the output paper is undesirable so if proposed, please address this historical performance artifact. No paper weight has been specified but the paper should have sufficient rigidity to be fed into the Ballot Box/Scanner with a single hand. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 38

The RFP calls for insurance documentation within 10 calendar days after award and before beginning work. The Pre-proposal conference agenda calls for evidence of current insurance coverage to be submitted with the proposal. Please clarify the insurance documentation that is required to be submitted with the proposal? For reference, here are the sections from the two documents:

RFP page 12, Section 3.4 Attachment 10 - Insurance documentation within ten (10) calendar days after award and before beginning work

Pre-proposal conference:

OTHER REQUIRED DOCUMENTATION (para 3.0, page 31-32)
Submit the following documents with the proposal in accordance with these paragraphs: edit

Evidence of current insurance coverage (para 3.4, page 12). **(Submitted: Oct 31, 2016 3:28:26 PM CDT)**

Answer

- Vendors should submit their standard insurance certificate showing insurability with their proposal response. The insurance certificate that is submitted 10 days after award should include all of the requirements listed in Attachment 10. **(Answered: Nov 28, 2016 5:17:57 PM CST)**

Question 39

Regarding Element C, the requirements are silent on the need for the scanning device to print any reports such as POST, Open Polls, Close Polls, or a Scanned PVR Report. Are there unstated requirements for the scanning system to maintain state data (example: number of PVR scanned), and then print the state information onto a thermal printer at polls close? **(Submitted: Nov 3, 2016 9:46:13 AM CDT)**

Answer edit

- The intent is for Element C to download data to the BCS of Element B such that the BCS can produce the required reports for the In Person Voting. Alternate approaches will be considered where the final configuration will be defined during contract negotiations as part of the interface definition between Element B and Element C. Element C is expected to maintain complete, time-stamped electronic records of all activities that it performs during an election. **(Answered: Nov 4, 2016 5:13:16 PM CDT)**

Question 40

The VVSG 1.1 requirements state that a voting system's display must have at least an 85 pixel per inch pitch, at least 700 cm^2 of display area, and an antireflective coating. Thus, the screen is required to have a diagonal dimension of over 15", regardless of whether it has a 16:9 or 4:3 aspect ratio. The RFP requirements call for a structure similar to a tablet that is lightweight, portable, and has a long battery life; a minimum 5-point multi-touch touchscreen; and a system that must not depend on hardware with non-Intel processors. To the best of our knowledge, there are no current COTS devices that fulfill all these requirements out of the box. Since the goal of the VVSG 1.1 requirement is readability, and the higher pixel density on many modern tablets makes them significantly more readable than older tablets of the same size, are you willing to relax the screen size requirement of VVSG 1.1 to admit the possibility of using the wide array of 12"-14" Intel tablets that exist on the market. **(Submitted: Nov 4, 2016 4:18:44 PM CDT)** edit

Answer

- Yes, the County will accept alternate hardware configurations outside the requirements stated in the RFP provided the deviation is justified and the proposed hardware meets the effective objectives of the original requirements and VVSG 1.1. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 41

Mandating a minimum 5-point multi-touch touchscreen (Requirement 9.5.2) may significantly impact the cost and availability of devices for the voting system. Should this be a desirable requirement, rather than a mandatory one, if all accessibility and usability goals can be met with a less capable touchscreen? **(Submitted: Nov 4, 2016 4:20:05 PM CDT)**

Answer edit

- Yes, the County will accept alternate hardware configurations outside the requirements stated in the RFP provided the deviation is justified and the proposed hardware meets the effective objectives of the original requirements and VVSG 1.1. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 42

Must the audio jack (Requirement 9.5.3) permit only one-way data flow (to the listener), or must it support on-headphone volume control? The former tightens the security profile of the device; the latter facilitates better usability and familiarity, especially to disabled voters. **(Submitted: Nov 4, 2016 4:20:32 PM CDT)**

Answer edit

- Yes, the County will accept alternate hardware configurations outside the requirements stated in the RFP provided the deviation is justified and the proposed hardware meets the effective objectives of the original requirements and VVSG 1.1. Please discuss possible mitigation strategies for any impact on loss of security. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 43

Element B requirement 5.11 states: “Equipment in the polling location must remain operational on battery power for at least four hours. A full precinct must be able to be operated by the power provided by a typical gas-power generator supplying about 2000 watts.” The relationship between the battery life requirement and the maximum power supplied by a typical generator is unclear. Is the battery life measurement meant to start from a state where the batteries are fully charged? Must the full precinct’s equipment always use a total of less than about 2000W, or merely be able to do so when running on generator/battery power? **(Submitted: Nov 4, 2016 4:20:49 PM CDT)** edit

Answer

- Assume the battery life measurement starts from a fully charged battery and that the system draws 2000W or less only when operating on battery power. The system refers to all equipment in the polling location required to conduct voting operations. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 44

Element B requirement 5.13 states: “Propose a bi-directional data interface between the Ballot Control Station (BCS) and the Ballot Box/Scanner (Element C).” Is this meant to be a physical data interface (a specific type of physical connection), or a communication protocol similar to that used by the other components on the STAR-Vote air-gapped network? **(Submitted: Nov 4, 2016 4:21:11 PM CDT)**

Answer edit

- The bi-directional interface between the Ballot Control Station (BCS) and the Ballot Box/Scanner (Element C) is a real-time communication channel operating on the physically connected polling place network in order to meet the data interchange requirement for the vote casting process. The connection can either be direct or through off-the-shelf networking equipment. **(Answered: Nov 18, 2016 7:06:22 PM CST)**

Question 45

In Appendix B, point 2.5.1.4.4 states that the COTS operating system must "Not be changed in a way that would invalidate its qualification as COTS". What types of changes would you consider to invalidate such qualification? **(Submitted: Nov 4, 2016 4:21:34 PM CDT)**

edit

Answer

- A custom compiled version of the operating system that cannot be purchased by the general public. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 46

Requirement 2.1.3.5 and its sub-requirements, and requirements 2.1.3.6 and 2.1.3.7, seem as though they may be incorrectly formatted; in particular, it seems that requirements 2.1.3.5.3 through 2.1.3.7 should all be one level higher up in the hierarchy than they are. Perhaps there was a formatting error? Please review and advise. **(Submitted: Nov 4, 2016 4:21:52 PM CDT)**

Answer

edit

- Correct. The RFP contains a numbering error in Appendix B In-Person Voting/Tabulation and the following numerical corrections will be added to an Addendum to the RFP:
  Appendix B
  IS: 2.1.3.5.3; NOW: 2.1.3.6
  IS: 2.1.3.5.4; NOW: 2.1.3.7
  IS: 2.1.3.6; NOW: 2.1.3.8
  IS: 2.1.3.7; NOW: 2.1.3.9 **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 47

Requirement 2.5.1.4.6 says that the OS used must "Support Measured Boot or equivalent technologies enabled by a hardware or firmware Trusted Platform Module (TPM)". It does not say that Measured Boot or equivalent technologies must actually be used in the delivered product. Is it County's intention that Measured Boot or equivalent technologies must be used? **(Submitted: Nov 4, 2016 4:22:07 PM CDT)**

Answer

edit

- It is the County's intention to provide assurance that when the Operating System (OS) boots, it's running code that hasn't been compromised. The assurance can be provided by Measured Boot, Secure Boot or other proposed equivalent techniques with a proven level of assurance. The County prefers the proposed method be commercially available off-the-shelf. **(Answered: Nov 18, 2016 7:06:22 PM CST)**

Question 48

With respect to Requirement 8.3.1, we presume that the _system_, not just the _code_, must be robust. Please advise. **(Submitted: Nov 4, 2016 4:22:46 PM CDT)**

Answer

edit

- Yes. The system and software must be robust. Appendix D lists the software requirements and Appendix F contains the hardware requirements and collectively, these Appendices require a robust system. **(Answered: Nov 18, 2016 7:06:22 PM CST)**

Question 49

Requirement 8.7.1 mentions “assemblies”, but other portions of the RFP properly underspecify the means by which component-based development and deployment take place. We presume that you mean “...assemblies or similar component abstractions.”. Please advise. **(Submitted: Nov 4, 2016 4:23:08 PM CDT)**

Answer

edit

- Requirement 8.7.1 is part of the Software Specification appendix and therefore the requirement is referring to software assemblies. The use of the term “assemblies” was not intended to convey any architectural construct but rather software code blocks that are generally created as part of software development using software development best practices. The term “similar component abstractions” may be used interchangeable with the term “assemblies”. **(Answered: Nov 18, 2016 7:06:22 PM CST)**

Question 50

The use of network runtime monitors, like that which is permitted in Requirement 8.7.7, is a complex and delicate issue. Do you have any more specific guidance as to what type of monitoring and auditing you intend to allow (or to perform) on the system? **(Submitted: Nov 4, 2016 4:24:40 PM CDT)**

Answer

edit

- Refer to Question 23 for the use of network monitoring. The RFP calls for successful proposers to recommend and justify hardware components for Element B, and this should also include any hardware reference in Appendix D paragraph 8.7.7. The type of monitoring and auditing would be for the communication traffic that is exchanged between the components of the In Person Voting process. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 51

We presume that you want proposals to identify the underlying algorithm that fulfills requirements 9.1.1 through 9.1.4, not a full formal specification of said algorithm. E.g., saying “we agree that it looks like ElGamal over EC is fine” is good enough. Please clarify. **(Submitted: Nov 4, 2016 4:24:55 PM CDT)**

Answer

edit

- Appendix E, paragraphs 9.1.1 through 9.1.4 specifies the properties the algorithm must possess. Naming the proposed algorithm and describing how it satisfies the required properties is sufficient. The County assumes that any proposed algorithm has a proven history and is supported by a publicly available body of knowledge that will allow the County’s cryptographic resources to review the suitability of the algorithm for STAR-Vote. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 52

With respect to Requirement 9.1.7, we presume that you want proposals to identify all algorithms that will likely be useful (but not necessarily used) in the design and implementation of the system. Please clarify. **(Submitted: Nov 4, 2016 4:25:12 PM CDT)**

Answer

edit

- Yes. Anywhere that encryption is required by the RFP, the proposed encryption algorithm should be named. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 53

With respect to Requirement 9.2, we presume that a plurality election scheme, possibly with multiple seats available, is the only scheme that need be supported by this initial implementation. Should proposers reflect upon other schemes deployed in the USA? **(Submitted: Nov 4, 2016 4:25:28 PM CDT)**

Answer edit

- The requirement in Appendix E, paragraph 9.2 is an explanation of Homomorphic Encryption and the example provided is clearly labeled as "illustrative", which should not be interpreted as a definition of the types of contests supported. Requirements for supported contest types are defined elsewhere in the RFP. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 54

There seems to be a typo in the first paragraph of Requirement 9.3. There is a missing application of 'E'. Please advise. **(Submitted: Nov 4, 2016 4:26:01 PM CDT)**

Answer

- Correct. The following change will be added to the RFP Addendum: edit
  IS: "Commitment Consistency, the second property of the selected encryption system, means that given that you have an encryption of n, ¬_k (n), if another party…"
  NOW: "Commitment Consistency, the second property of the selected encryption system, means that given that you have an encryption of n, E ¬_k (n), if another party…" **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 55

Is encoding the receipt described in Requirement 9.3 as a large natural number a mandatory requirement? We expect that, with usability testing, there may be other means by which to encode the hash that are more useful and usable by voters. **(Submitted: Nov 4, 2016 4:26:17 PM CDT)**

Answer edit

- The County will consider alternate methods used to produce the hash value for a voter receipt provided it maintains the same level of cryptographic strength. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 56

Related to Requirement 10.5.7, about accessibility devices, must the voting system have a voter-accessible USB port to permit arbitrary voter-supplied accessibility equipment to be used? This is another instance where security and accessibility/usability are in conflict. Ensuring that such a port is secure and robust is non-trivial. **(Submitted: Nov 4, 2016 4:26:35 PM CDT)**

Answer

edit

- The proposal may identify specific accessibility devices to be used with the voting terminal to limit the security exposure. The County will provide these specific devices for use in the polling locations, connected to the voting terminal without exposing ports for arbitrary devices. The interfaces/devices must remain "standards-compliant accessibility devices via

industry-standard technologies" so that the County can provide alternate devices as needed. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 57

The text in requirement 10.5.11 does not make sense. Perhaps there was a formatting error? Please review and advise. **(Submitted: Nov 4, 2016 4:26:48 PM CDT)**

Answer

- There is a formatting error in Appendix F, paragraph 10.5.11 that will be corrected in an Addendum as follows:
  IS: 10.5.11 The ability to be used in a parallel distribution of software and System Images, backup, data retrieval and clearing the memory; type and brand of touch screen display;
  NOW: 10.5.11 The ability to be used in a parallel distribution of software and System Images, backup, data retrieval and clearing the memory;
  10.5.12 Type and brand of touch screen display;
  The current paragraphs 10.5.12 through 10.5.29 are incremented by one and NOW run from 10.5.13 through 10.5.30. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

edit

Question 58

Can we presume that all voting locations are ADA compliant (in particular, we are wondering about this with respect to issues such as being able to wheel a voting station, including printer, paper, etc., to the curb for curbside voting)? **(Submitted: Nov 4, 2016 4:27:01 PM CDT)**

edit

Answer

- This is a correct assumption, all polling locations are required to be ADA compliant by statute. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 59

Requirement 10.8.1 is blank in the RFP. Is there a missing requirement, or is this a typographical error? **(Submitted: Nov 4, 2016 4:27:17 PM CDT)**

Answer

- Appendix F, paragraph 10.8.1 has a typographical error that will be corrected in an Addendum as follows:
  IS: 10.8.1
  NOW: 10.8.1 Run on rechargeable battery power for a minimum of 4 hours. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

edit

Question 60

Requirement 10.8.7 is missing part of its text. We presume it is identical to requirement 10.6.7. Please advise. **(Submitted: Nov 4, 2016 4:27:33 PM CDT)**

Answer

- Correct. Appendix F paragraph 10.8.7 has a typographical error that will be corrected in an Addendum as follows:
  IS: 10.8.7 Provide a cost justification for
  NOW: 10.8.7 Provide a cost justification for the initial purchase and ongoing operation;
  (Answered: Nov 18, 2016 7:06:23 PM CST)

edit

Question 61

In the case of the Ballot Box/Scanner Option 2 (section 10.9): Travis County should note that it is not only the software that should be open source and your property; significant parts of scanner technology are implemented in firmware. Thus both must be stipulated as witnessing ownership transfer and transparency. **(Submitted: Nov 4, 2016 4:27:44 PM CDT)**

Answer

- The County is aware that scanning heads typically have resident firmware to manage the electro-mechanical operation of the paper transport mechanism and generation of image data, independent of the application. This firmware can be isolated from the application logic that manages the functionality of the Ballot Box/Scanner (the "election specific functions"). The County also recognizes there are Original Equipment Manufacturers (OEMs) that manufacture scanning heads for use for different applications across different industries and these OEM products are used for current election products. The OEM products include the electro-mechanical component and resident firmware. To account for the state of the industry, minimize the development risk and allow the use of OEM scanning head products, the following paragraph will be added to the RFP in an addendum:
  NOW: 10.9.1.22 The incorporation of Original Equipment Manufacturer (OEM) scanning hardware, which includes the electro-mechanical components and resident firmware, is permitted to meet the STAR-Vote Ballot Box/Scanner requirements in this RFP given the following conditions:
  10.9.1.22.1 The OEM scanner head is a complete assembly that includes the electro-mechanical components and resident firmware for operation of the paper transport mechanism and generation of image data that is marketed and sold by the OEM as a single part number and revision level. This allows the OEM product to be designated as COTS hardware.
  10.9.1.22.2 The application software must be designed so that alternate OEM scanning heads from different OEMs can be substituted for the proposed scanning head.
  10.9.1.22.3 The County does not require ownership of OEM COTS products but must have a license or purchase order in the County's name for the continued use of the OEM product for STAR-Vote. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

edit

Question 62

Mandating the use of non-volatile memory for (some underspecified amount of) caching of messages is overly proscriptive (unless "non-volatile memory" is to be taken to mean "any non-volatile storage medium"). Other storage mechanisms should suffice. Moreover, without some kind of upper bound in a non-functional requirement, this is difficult to fulfill for developers and enforce for the client. Please advise. **(Submitted: Nov 4, 2016 4:28:07 PM CDT)**

Answer

- The County is unable to find a specific requirement for caching messages in non-volatile memory. The requirement with the closest reference is 10.9.1.3 where the first sentence references the device becoming disconnected from the network but retaining power. In this instance, maintaining the messages in volatile memory is not an issue. The second sentence notes that power may be lost and the objective is for no messages pending transmission to be lost due to a power loss. The County recommends that any messages that have not been sent be written off to non-volatile memory as part of the power down sequence of the device. Additional reference requirements from the RFP are needed if the question has not been answered satisfactorily. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

edit

Question 63

Requirement 10.9.1.6 states that the ballot box must "have the ability to 'accept' or 'reject' each page physically via the feed mechanism once a Ballot Control Station has indicated over the network

that the page should be accepted or rejected", and requirement 10.9.1.8 states that the ballot box must "have a feed speed that accepts voter ballot pages without delay". These two requirements seem impossible to reconcile, because a delay is required to verify the acceptability of each ballot page if it is to be rejected using the feed mechanism. Would an alternative mechanism for accepting or rejecting ballots be acceptable (e.g., routing them to either the sealed ballot box or to a return tray, like the coin return in a vending machine)? Would some amount of delay be acceptable? We suggest that perhaps a statement of the goals to be achieved by the ballot box's accept/reject mechanism, rather than specific requirements about feed mechanism and delay, would allow for a wider range of viable solutions to be proposed. **(Submitted: Nov 4, 2016 4:28:28 PM CDT)**

Answer edit

- The County will entertain alternate approaches. However, the voter may not have access to 'accepted' ballots. We apologize for the apparently contradictory requirements. In this instance, the use of the term 'accept' in paragraphs 10.9.1.6 and 10.9.1.8 have two different meanings. In paragraph 10.9.1.6, 'accept' is used in the context of the 'accept and reject' process employed by the Ballot Box/Scanner while operating in partnership with the BCS. This requirement indicates an elapse time exists for the BCS to provide a response for the disposition of the current ballot. The context of paragraph 10.9.1.8 relates to the feed speed of the voter inserting his or her ballot and that Ballot Box/Scanner must receive or 'consume' the ballot without delay. This language will be updated in an RFP addendum as follows:
  IS: 10.9.1.8 Have a feed speed that accepts voter ballot pages without delay;
  NOW: 10.9.1.8 Have a feed speed that consumes voter ballot pages without delay;
  (Answered: Nov 18, 2016 7:06:23 PM CST)

Question 64

Is having ballots fall into a secure ballot box, as described in 10.9.2, mandatory? E.g., would a device that lifts or otherwise moves the ballot into the secure ballot box be acceptable? **(Submitted: Nov 4, 2016 4:28:58 PM CDT)**

edit

Answer

- The County will consider alternate solutions. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 65

Is permitting PVRs to stack neatly, as described in 10.9.2.2, a mandatory requirement? Mandating such is a security risk insofar as a voter's privacy can be violated by a malicious observer. **(Submitted: Nov 4, 2016 4:29:13 PM CDT)**

Answer edit

- The intent of paragraph 10.9.2.2 is for the efficient storage of the ballots in the Ballot Box, as 'neatly' is simply descriptive and not specifically defined. The Ballot Box is locked and sealed and not accessible to observers, which protects the voter's privacy. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 66

Are additional security mechanisms that provide evidence of the integrity and (unmentioned in this requirement) provenance of the ballot box welcome? This is implicitly mentioned in requirement 10.9.2.10. **(Submitted: Nov 4, 2016 4:29:32 PM CDT)**

Answer edit

- Yes. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 67

What is the underlying reason for the magic number 12” as the maximum distance in Requirement 10.10.7? **(Submitted: Nov 4, 2016 4:29:45 PM CDT)**

Answer

edit

- The maximum 12” dimension in paragraph 10.10.7 is primarily a practical design consideration to require a relatively compact device for use, transportation and storage. Another consideration is to provide voter privacy that becomes more difficult as the dimension increases. Alternate distances will be considered provided the aforementioned characteristics are specifically addressed. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 68

We presume that the duplicate requirement in 10.10.39 is a typographical error; is this correct? **(Submitted: Nov 4, 2016 4:30:00 PM CDT)**

Answer

edit

- Yes, paragraph 10.10.39 contains a typographical error that will be corrected in an Addendum to the RFP as follows:
  IS: 10.10.39 Have the ability to be programmed so that a voter’s PVR is completely deleted from the memory of the Reader upon completion of the reading process. Have the ability to be programmed so that a voter’s PVR is completely deleted from the memory of the Reader upon completion of the reading process.
  NOW: Have the ability to be programmed so that a voter’s PVR is completely deleted from the memory of the Reader upon completion of the reading process. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 69

Requirement 2.6.2.10 states “After the voter has received a Voting Ticket or at the time the voting process is disrupted at the Voting Station, provide a means of determining the status of the Voting Ticket. This must be made available to the voter in a printed copy.” It is unclear what “at the time the voting process is disrupted at the Voting Station” means (e.g., what sort of disruption is envisioned? hardware/software failure? voter error? both?). It is also unclear when and by whom/at what station this must be made available to the voter in a printed copy; our assumption is that this would be done at the BCS, but we would like clarification. **(Submitted: Nov 4, 2016 4:30:15 PM CDT)**

edit

Answer

- Section 2.6 is titled “Ballot Controller Station (BCS) Module” and therefore, paragraph 2.6.2.10 defines functionality provided by the BCS. The BCS is required to produce the Voting Ticket report that is given to the voter. The BCS that generated the Voting Ticket is responsible for producing the Voting Ticket status report. The voting process disruption at the Voting Station can stem from any cause, which is irrelevant for production of the Voting Ticket report. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 70

Requirement 2.6.2.11 states that a voting station must monitor and log “all network messages”. We presume that this does not include network messages used to populate the logs of machines that join the network mid-election with historical information about the election, as it seems that including such messages would lead to a “message log loop” when a device is added or recovers from a connectivity loss: the log information sent to the device to fill in its logs would be logged (again) by every other device, and those additional log entries would then need to be sent to the

device being added, etc., resulting in the device being added never being up to date with the other devices' logs. Is this a correct presumption on our part? **(Submitted: Nov 4, 2016 4:30:39 PM CDT)**

Answer

edit

- Appendix B, section 2.6 is titled "Ballot Controller Station (BCS) Module" and therefore, paragraph 2.6.2.11 defines functionality provided by the BCS, not the Voting Station. The purpose of logging all messages is to create a unified audit trail of all device activity within the polling location and storing the audit log on all devices. Storing this log on all devices on the network creates a redundant storage mechanism to protect the log. When a device is added to the network mid-election, the redundantly stored log data from other devices operating in the polling location is copied to the new device so that it stores the same information as the other devices. An illustrative solution for this is for the BCS to have a 'new device' communication mode where the BCS communicates directly with the newly added device to bring it up to date with audit data. If the foregoing does not answer the question regarding "message log loop", additional explanation is required to address the question more specifically. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 71

Requirement 2.6.2.12.4.1 states that, when a ballot page is spoiled, the BCS must "look up the Voting Ticket number used by the voter to create the ballot being spoiled. Using this, look up the number of Voting Tickets this voter has been previously issued." However, there appears to be no corresponding requirement for a voting station or the BCS to maintain an association between a Voting Ticket number and the PCIDs of the ballot created using that Voting Ticket. Must such an association be broadcast to the network when the voting station prints a ballot? **(Submitted: Nov 4, 2016 4:31:22 PM CDT)**

Answer

edit

- The stated observation in the question regarding an explicit association between the Voting Ticket number and PCID is not contained in the RFP. However, the requirements for reporting the Voting Ticket status in 2.6.2.10 and the verification requirements in 2.6.2.11.2.2 imply a temporary relationship be maintained. To specify these requirements more definitively, the following changes will be added to an RFP Addendum:
  NEW: 2.6.2.4.4 The Voting Ticket number is to be stored in non-volatile memory until the voting session associated with the Voting Ticket number is completed.
  IS: 2.6.2.11.2.1 Decrypt the PCIDs using the BCS's private key, and store the ballot's PCIDs, the associated page numbers, and the audit crypto hash, zi, in a ballot lookup table, indexed by the PCID. This table must be stored in Volatile Memory and must not be committed to Non-volatile Memory;
  NOW: 2.6.2.11.2.1 Decrypt the PCIDs using the BCS's private key, and store the ballot's PCIDs, the associated page numbers, and the audit crypto hash, zi, in a ballot lookup table, indexed by the PCID. This table must be stored in Volatile Memory and must not be committed to Non-volatile Memory. When a paper ballot cast message is received by the BCS, the BCS checks whether the corresponding PCID is stored in the temporary table and broadcasts the associated zi value together with the action that needs to be taken (cast, spoiled, provisional, re-issue). The PCID entry is then removed from the temporary table. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 72

Requirement 2.6.2.14 states that in the event of a BCS failure, the software on a Voting Station must "be able to accommodate being reconnected to a Polling Location Network for which an election has already begun and effectively enable the continuation of that election." What is the

desired behavior with respect to the Voting Station's existing message logs, both in terms of its own behavior and whether it should provide those logs to other Voting Stations on the new network, when this occurs? **(Submitted: Nov 4, 2016 4:31:41 PM CDT)**

Answer edit

- Appendix B, section 2.6 is titled "Ballot Controller Station" so the requirement in paragraph 2.6.2.14 is for a problem with the BCS and its continuation of the election, provided the device recovers. Refer to Question 70 for a response regarding Voting Station message logs. If the BCS goes off-line and then is reconnected to the network, the desired behavior for the message log of the BCS is for it to be updated with communication traffic that occurred while the BCS was off-line. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 73

Requirement 2.6.3.6 states that after the polls close, the BCS software must "provide a mechanism for deleting information related to a past election from the BCS". We presume that such deletion must not occur before the ballot manifest is finalized and the information has been properly archived; is that presumption correct? What are the complete conditions that must be met before election information may be deleted from the BCS? **(Submitted: Nov 4, 2016 4:31:59 PM CDT)**

Answer edit

- Requirements 2.6.3.6 and 2.6.3.7 are out of temporal order. Deletion of past elections can only occur after the election has been certified by the Election Administrator. To clarify this condition, an Addendum to the RFP will contain the following update:
  IS: 2.6.3.6 Provide a mechanism for deleting information related to a past election from the BCS.
  NOW: 2.6.3.6 Provide a mechanism for deleting information related to a past election from the BCS only after the election has been certified and at the direction of the Election Administrator. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 74

Requirement 2.7.3.2.2.2 says that a Voting Station must generate "unique Page Identifiers (PIDs) for each page of the voter's PVR", and a subrequirement requires this to be done with a cryptographic random number generator. In what context are the PIDs required to be unique? (i.e., should they be unique among all PIDs created by that Voting Station? unique among those created by all Voting Stations on the same airgapped network? unique among those created by all Voting Stations participating in the election?) **(Submitted: Nov 4, 2016 4:32:16 PM CDT)**

Answer edit

- The intent is for the PIDs to be unique to the election. Paragraph 2.7.3.2.2.2.1 recommends the use of "Universally Unique Identifiers (UUIDs) if deemed feasible" and paragraph 2.7.3.2.2.2.2 indicates "The PIDs must be created via a cryptographic random number generator". Implementing these two techniques effectively guarantees the PIDs will be unique to an election. The probability of creating a duplicate PID is extremely low and if implemented correctly, the County will accept this as providing an election-unique PID. Alternate implementation will be considered, however. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 75

Requirement 2.7.7.3.3 states that a Voting Station "must not allow the voter or anyone but the Administrator to access any other software or disable demonstration mode." Does the County envision a particular mechanism for authenticating the Administrator to the Voting Station in such a

scenario, or is that left open for specification by proposers? **(Submitted: Nov 4, 2016 4:32:35 PM CDT)**

edit

Answer

- Please recommend and propose an appropriate access control. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 76

Requirement 2.8.8 states that the Data Integration/Validation Module must provide a means for an administrator to specify that a specific polling location's data that failed validation be sent to the tabulator regardless. We presume that such a decision on the part of an administrator must be logged in some fashion; does the County have a particular mechanism in mind for that? **(Submitted: Nov 4, 2016 4:32:54 PM CDT)**

Answer

edit

- Please recommend and propose an appropriate access control.
  As a rule that applies to every component or module in the STAR-Vote system, any action performed by a user/operator must generate a time-stamped record of the action and the record stored in an audit log maintained by the component or module. For this particular instance, yes, the action must be logged. The county does not have a prescribed mechanism for this action but an illustrative example is for the default condition to be that the failed validation not to be sent and the Administrator must override the default by entering a password or some other authentication means. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 77

Requirement 2.10.7.1.2 states that tallies must be exportable "as a hard-coded PDF report". What is meant by "hard-coded" in this context? **(Submitted: Nov 4, 2016 4:33:08 PM CDT)**

Answer

edit

- In this instance, "hard-coded" is interpreted as a "non-editable" PDF report. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 78

Requirement 4.2.5 states that at the polling location, the system must "make use of an attached 2-D barcode scanner to read the barcode containing the Election Data Integrity Hash from BCS printouts". The Election Data Integrity Hash (and, indeed, all other data to be presented as barcodes) was specified elsewhere to be a 1-D barcode. What type of barcode should the Election Data Integrity Hash actually be, or should that be left to the proposer to suggest? **(Submitted: Nov 4, 2016 4:33:27 PM CDT)**

edit

Answer

- Proposers should provide best-in-class solutions when responding to the requirements in Part II of the RFP, justifying alternate implementations as appropriate for stated barcode requirements. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 79

Requirement 4.3.10 states that the Bulletin Board Module must be able to provide "a complete dump of an audit log from each polling location." Since the audit logs of all the devices at the polling location will be different (but should be consistent with one another - a fact that should be checkable after the election), how should it be decided which audit log to dump? (additionally,

should the system offer the option to dump all of them?) **(Submitted: Nov 4, 2016 4:33:45 PM CDT)**

Answer edit

- The intent is for there to be a single audit log for the entire polling location by broadcasting audit entries for a device to all other devices on the network, and for any device added to the network to be updated with the audit log at the time the device is connected. The result of this operational feature is a single audit log for the entire polling location, which is dumped to the Bulletin Board Module. Refer to Question 70 for further description. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 80

Requirement 8.1.1 states that every aspect of the software must be "designed using coding best practices." Is this meant to refer to the VVSG guidelines on such, or does County have another specific set of best practices to refer proposers to? **(Submitted: Nov 4, 2016 4:34:02 PM CDT)**

Answer edit

- The minimum coding best-practices requirement is the VVSG guidelines. Other, more current commercial best-practices exist and, to the degree these are followed or utilized, should be stated in your proposal. **(Answered: Nov 18, 2016 7:06:22 PM CST)**

Question 81

Requirement 8.9.3.3 states that the Network and Logging Layer "transmits well-formed messages from a device's software to all connected STAR-Vote™-compatible devices". Is this meant to be (1) a broadcast of signed, but not encrypted messages (except to the extent that individual message components are required to be encrypted by the rest of the protocol), or (2) a transmission of message content individually encrypted to the various recipients on the network, or (3) whichever of these possibilities is deemed most appropriate by the proposer? **(Submitted: Nov 4, 2016 4:34:19 PM CDT)**

edit

Answer

- The correct interpretation of Appendix D paragraph 8.9.3.3 is the first option (1) as stated in the question, where the messages from each device are signed by the originating device and contain encrypted components within the message that are required to be encrypted as specified by other requirements given in the STAR-Vote specification. The overall message is not required to be encrypted. **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 82

Requirement 8.9.3.6 states that the Network and Logging Layer "logs all messages received automatically, and ensures good ordering of the message log through retention of a hash chain." Does "good ordering" in this context mean merely that the order that messages appear in a component's message log accurately reflects the order in which they were actually received by that component, or does it mean something more sophisticated at a system level about the ordering of messages as observed by all components? **(Submitted: Nov 4, 2016 4:34:51 PM CDT)**

Answer

- The proper interpretation of Appendix D, paragraph 8.9.3.6 is that the "ordering" of messages must be identical across all devices connected to the network such that the audit logs stored by each device are identical, as stated in early responses to RFP Questions 70 and 79. This ordering technique requires that the communication protocol must resolve any conflicts

edit

or race conditions that are created by messages being sent from different devices at the same instance in a deterministic manner. The message must include the hash of the prior message in the hash chain, thus ensuring that remote recipients of the message are storing hashes of other machines' logs. The intent of this design is to implement a form of "timeline entanglement" that enables a variety of high-level integrity checks that can be performed during and after the completion of an election. Further background on timeline entanglement can be found at:

https://www.usenix.org/conference/11th-usenix-security-symposium/secure-history-preservation-through-timeline-entanglement **(Answered: Nov 18, 2016 7:06:23 PM CST)**

Question 83

Requirement 8.9.3.9.3 states that messages “must not be modified at the software level prior to logging”. What does “at the software level” mean in this context, given that low-level operating system networking code, which must of necessity modify messages upon receipt from the network hardware interface before presenting them to the network and logging layer, is also software. **(Submitted: Nov 4, 2016 4:35:04 PM CDT)**

Answer

- The requirement of Appendix D, paragraph 8.9.3.9.3 applies only to STAR-Vote code and does not apply to standard networking protocols provided by the operating system or hardware used to facilitate networked communication. In this context, “message” refers to the complete data packet sent from one device to another and the intent is to ensure that messages are not preprocessed by the STAR-Vote software before storage, and to encourage the vendor to immediately write messages when received. Further, the logging and networking layers must operate in unison so if a message is to be transmitted on the network, it is added to the log as-is. This requirement is not meant to restrict the packet formatting and other processing that occurs in the networking software stack. **(Answered: Nov 18, 2016 7:06:22 PM CST)**

edit

Question 84

Requirement 8.9.4.3.3 states that the Audit Plaintext Commitment File must include, for each entry, “the decrypted Audit Plaintext Reference Key for that vote.” What is an Audit Plaintext Reference Key? The term does not appear anywhere else in the RFP. **(Submitted: Nov 4, 2016 4:35:25 PM CDT)**

Answer

- The “Audit Plaintext Commitment Key” given in Appendix D, paragraph 8.9.4.3.3 is a legacy term from the RFI. The term is defined in Appendix D, paragraph 8.10.3.1.3 and referenced in Appendix B, paragraph 2.10.5.1. To specify this requirement more definitively, the following change will be added to an RFP Addendum:

  Appendix D, paragraph 8.9.4.3.3;

  IS: The decrypted Audit Plaintext Reference Key for that vote; and

  NOW: The decrypted hash of the Race Identifier (RID) combined with the Page Identifier (PID) for the page of the PVR on which this race is displayed. This hash must then be encrypted with the Election Public Key; and **(Answered: Nov 18, 2016 7:06:22 PM CST)**

edit

Print Close