Subject: Statement of Work
Date: Tuesday, March 30, 2004 8:29 PM
From: R. Mercuri <notable@mindspring.com>
To: "Peter G. Neumann" <neumann@csl.sri.com>, Donna LinnÈ <linne@csl.sri.com>, Donna Linné <donna.linne@sri.com>, Alicia Siciliano <alicia@csl.sri.com>

Attached is my 3-page "Statement of Work" document (Microsoft Word) for the project, with the plain text version below. Actually if we do win this grant, I'm especially looking forward to creating the incident reporting facility. ;-)

I think the only other thing pending for this proposal is my "other funding" statement, but since basically there I don't have any (government funding, that is), then I guess that wraps it up if you can handle that on your end. I hope you received my faxed signed budget sheets.

If there's anything else I've forgotten, please let me know. I'm hoping this is NOW over (but for the residual shouting), thanks for all your patience and assist, and good working with all of you, as always.

Rebecca Mercuri.

Statement of Proposed Work
ACCURATE NSF Project
Notable Software, SRI contractor
Rebecca Mercuri, Co-PI

My involvement with the ACCURATE project team will focus primarily on three aspects: standards efforts, transparency and trust investigation, and incident reporting. Communication of my findings will be made within the group and, as well, conveyed via the World Wide Web, published in technical papers, and reported in lectures and media communications. I plan to direct the efforts of a few graduate assistants for some aspects of this work. I will also establish rapport with the other investigation teams to discuss their projects and results.

Standards Efforts

I have played an active role in the IEEE Voting Systems Standards working group, with the FEC in development of their 2002 VSS, and with NIST in their HAVA-related activities. Each of these teams is developing "working" standards that will be used to certify a subsequent crop of voting systems, but they are not intended to be static documents. Rather, these are recognized as requiring ongoing revision to continue to adequately reflect changes both in computer and election technology, as well as evolution to accommodate current thinking in voting legislation and practices.

My efforts in this regard, will be to provide valuable resources for these standards bodies. For example, where paper is used (whether produced by hand in the case of optically scanned ballots, or by machine using DRE/touchscreen equipment), issues regarding readability, longevity, retention, independent auditability and so on, shall be addressed. Methodologies for assessing the accuracy of the original vote totals as well as accounting for disparities (when such occur) in independent recounts, will be developed. Interrelationships among election system requirements, such as the inherent conflicts between full auditability, full anonymity, and the ability to provide an independent way of insuring that display mechanisms are trustworthy and accurately reflect ballot contents, will be examined. Development of a generic set of requirements that provides high accuracy in recounts, is also an area for investigation.

The IEEE has recently initiated a subgroup of its voting systems standards effort that pertains to data transfer. In particular, they are attempting to define a non-proprietary protocol that can be used across platforms and between equipment vendors in order to define ballot layouts. I plan to provide assistance to this project in the following ways: developing methods of ensuring that ballot layouts accurately display and collect data appropriately in the individual election contests; assessing the usability of the layout engines as well as the ballot templates; and providing controls to demonstrate that the ballots reflect what was programmed. Aspects of data transfer that the IEEE group is not presently considering, which my research might encourage, would include security, reliability, and auditability controls for the ballot templates as well as for the vote data and totals, as well as ensuring appropriate distribution of upgrades to systems and applications software. True accuracy and reliability metrics, involving field data rather than shake-and-bake equipment failure rates, can be developed. The IEEE working group has considered the production of a "best practices" document in terms of balloting system design. This could be extended to cover end-to-end practices, as well as comparative

merits of particular implementation features. Such issues as the cost and time benefits/tradeoffs could be considered. A standard could be recommended for ballot identification (that would not reveal the identity of the voter or be used for vote selling) in order to prevent alteration, removal, or substitution of ballots (whether on paper or in electronic format), along with high-reliability recovery techniques to be used for recounts or if/when data loss problems occur. Standards impacts related to multiple language ballots and accessibility can also be addressed.

Transparency and Trust in Election Systems

The current debate involving the availability (or lack thereof) of voter verified ballots from which to perform a recount with fully automated voting systems stems from two fundamental concepts made evident by Florida's 2000 U.S. Presidential election:

1. Voters must be able to confirm that they have cast their ballot as they intended to vote.

2. There must be an undisputable way of determining the vote totals following the election.

The major voting system manufacturers currently maintain that proprietary machines can be trusted to collect and tabulate ballots electronically, and that these results can accurately determine election outcomes. But a growing body of scientists has endorsed the need for independently verifiable elections, and legislators (such as former Princeton physicist and now US Representative Rush Holt) have introduced federal and state bills that would mandate the availability of paper audit trails.

Yet many fear the return to paper-based elections, not only due to their chad-filled past, but also because of issues of whether or not people can be trusted as well as (or better than) computers to collect and count ballots. Elections are sociological phenomena for which technological solutions are being applied, whether this be paper and pencil, punchcard, or touchscreen. These technologies necessarily result in a disparity between the expectations for the voting system and what performance is actually capable of being delivered. For example, election officials are quick to assert that "every vote counts" even though it has long been known that between 3-5% of votes may not be cast or recorded in many elections, no matter what form of balloting technology was

actually used. Cryptographers, such as David Chaum claim that it is possible, using mathematical techniques, to provide total assurance of election results using methods that are independently verifiable. Still, all cryptographic technology involves trusted agents as well as a degree of obscurity, so there may be some lingering doubt as to the integrity of the outcome. A computational solution that could be acceptable to the scientific community may not be sufficiently error-free or transparent enough to instill confidence in the voting public. The Mercuri Method involving the use of a paper audit trail, could be expanded to include cryptography and barcodes to ensure that the ballots remain in the box, and to allow for independent development of non-proprietary and open-source solutions for end-of-day tallying directly from the ballots that the voters had verified.

The question at hand is to determine a methodology for counterbalancing transparency and trust in voting systems. This component of the ACCURATE proposal will use the election scenario as a test bed for developing theories in this regard. Inherent conflicts between anonymity and auditability will be examined. The result would likely take the form of a hierarchical structure in which levels of transparency and trust can be ascertained. This model would then be explored using real-world settings, and concrete remedies would be provided to equipment vendors and members of the election community in order to assist them in mitigating exposure to risks. Results, having potential expansion to other trusted application areas beyond voting, would be published broadly, in order to obtain feedback and so that others can make use of this research.

Incident Reporting

Currently, there is no central repository for reports of election irregularities or equipment failures, and were there to be such a repository, there is nobody charged with analysis of such reports. This is true both at the state and national levels. Incident collection and reporting is further hampered by the restrictive non-disclosure agreements that have been signed between voting equipment vendors and purchasing authorities making it a third-degree felony to disclose the cause of an equipment-related election problem, even if such has resulted in court hearings.

For this part of the ACCURATE project, I plan to direct the creation of an incident reporting and analysis facility that will operate in a similar fashion to Carnegie Mellon's CERT Coordination Center as a central repository for the

collection and distribution of voting equipment anomalies. Types of incidents could include: inability to open or close polling places on time; other break-downs and denial-of-service occurrences; detection of deployment or distribution of uncertified software or components; excessive MTBF rates; anomalous vote tally reports. Using this data, categories of failures and vulnerabilities could be developed, correlation with particular product models and vendors could be identified, and true reasons for failures could be assessed.

This repository would be of tremendous use by those having direct (such as equipment purchasers, election officials, vendors, maintenance personnel) or auxiliary (media, legislators, attorneys, political scientists, usability experts, computer and engineering professionals) involvement with the election process. The incident reporting data could be used to support and motivate many of the other aspects of the ACCURATE research project.