INFORMATION ABOUT PRINCIPAL INVESTIGATORS/PROJECT DIRECTORS(PI/PD) and co-PRINCIPAL INVESTIGATORS/co-PROJECT DIRECTORS

Submit only ONE copy of this form **for each PI/PD and co-PI/PD** identified on the proposal. The form(s) should be attached to the original proposal as specified in GPG Section II.B. Submission of this information is voluntary and is not a precondition of award. This information will not be disclosed to external peer reviewers. ***DO NOT INCLUDE THIS FORM WITH ANY OF THE OTHER COPIES OF YOUR PROPOSAL AS THIS MAY COMPROMISE THE CONFIDENTIALITY OF THE INFORMATION.***

PI/PD Name: Peter Neumann

Gender: ☒ Male ☐ Female

Ethnicity: (Choose one response) ☐ Hispanic or Latino ☒ Not Hispanic or Latino

Race: (Select one or more)
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☒ White

Disability Status: (Select one or more)
- ☐ Hearing Impairment
- ☐ Visual Impairment
- ☐ Mobility/Orthopedic Impairment
- ☐ Other
- ☒ None

Citizenship: (Choose one) ☒ U.S. Citizen ☐ Permanent Resident ☐ Other non-U.S. Citizen

Check here if you do not wish to provide any or all of the above information (excluding PI/PD name): ☐

REQUIRED: Check here if you are currently serving (or have previously served) as a PI, co-PI or PD on any federally funded project ☒

Ethnicity Definition:
Hispanic or Latino. A person of Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race.

Race Definitions:
American Indian or Alaska Native. A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.
Asian. A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.
Black or African American. A person having origins in any of the black racial groups of Africa.
Native Hawaiian or Other Pacific Islander. A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.
White. A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

WHY THIS INFORMATION IS BEING REQUESTED:

The Federal Government has a continuing commitment to monitor the operation of its review and award processes to identify and address any inequities based on gender, race, ethnicity, or disability of its proposed PIs/PDs. To gather information needed for this important task, the proposer should submit a single copy of this form for each identified PI/PD with each proposal. Submission of the requested information is voluntary and will not affect the organization's eligibility for an award. However, information not submitted will seriously undermine the statistical validity, and therefore the usefulness, of information recieved from others. Any individual not wishing to submit some or all the information should check the box provided for this purpose. (The exceptions are the PI/PD name and the information about prior Federal support, the last question above.)

Collection of this information is authorized by the NSF Act of 1950, as amended, 42 U.S.C. 1861, et seq. Demographic data allows NSF to gauge whether our programs and other opportunities in science and technology are fairly reaching and benefiting everyone regardless of demographic category; to ensure that those in under-represented groups have the same knowledge of and access to programs and other research and educational oppurtunities; and to assess involvement of international investigators in work supported by NSF. The information may be disclosed to government contractors, experts, volunteers and researchers to complete assigned work; and to other government agencies in order to coordinate and assess programs. The information may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records", 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records", 63 Federal Register 268 (January 5, 1998).

INFORMATION ABOUT PRINCIPAL INVESTIGATORS/PROJECT DIRECTORS(PI/PD) and co-PRINCIPAL INVESTIGATORS/co-PROJECT DIRECTORS

Submit only ONE copy of this form **for each PI/PD and co-PI/PD** identified on the proposal. The form(s) should be attached to the original proposal as specified in GPG Section II.B. Submission of this information is voluntary and is not a precondition of award. This information will not be disclosed to external peer reviewers. ***DO NOT INCLUDE THIS FORM WITH ANY OF THE OTHER COPIES OF YOUR PROPOSAL AS THIS MAY COMPROMISE THE CONFIDENTIALITY OF THE INFORMATION.***

PI/PD Name: Rebecca T Mercuri

Gender: ☐ Male ☐ Female

Ethnicity: (Choose one response) ☐ Hispanic or Latino ☐ Not Hispanic or Latino

Race: (Select one or more)
- ☐ American Indian or Alaska Native
- ☐ Asian
- ☐ Black or African American
- ☐ Native Hawaiian or Other Pacific Islander
- ☐ White

Disability Status: (Select one or more)
- ☐ Hearing Impairment
- ☐ Visual Impairment
- ☐ Mobility/Orthopedic Impairment
- ☐ Other
- ☐ None

Citizenship: (Choose one) ☐ U.S. Citizen ☐ Permanent Resident ☐ Other non-U.S. Citizen

Check here if you do not wish to provide any or all of the above information (excluding PI/PD name): ☒

REQUIRED: Check here if you are currently serving (or have previously served) as a PI, co-PI or PD on any federally funded project ☐

Ethnicity Definition:
Hispanic or Latino. A person of Mexican, Puerto Rican, Cuban, South or Central American, or other Spanish culture or origin, regardless of race.

Race Definitions:
American Indian or Alaska Native. A person having origins in any of the original peoples of North and South America (including Central America), and who maintains tribal affiliation or community attachment.
Asian. A person having origins in any of the original peoples of the Far East, Southeast Asia, or the Indian subcontinent including, for example, Cambodia, China, India, Japan, Korea, Malaysia, Pakistan, the Philippine Islands, Thailand, and Vietnam.
Black or African American. A person having origins in any of the black racial groups of Africa.
Native Hawaiian or Other Pacific Islander. A person having origins in any of the original peoples of Hawaii, Guam, Samoa, or other Pacific Islands.
White. A person having origins in any of the original peoples of Europe, the Middle East, or North Africa.

WHY THIS INFORMATION IS BEING REQUESTED:

The Federal Government has a continuing commitment to monitor the operation of its review and award processes to identify and address any inequities based on gender, race, ethnicity, or disability of its proposed PIs/PDs. To gather information needed for this important task, the proposer should submit a single copy of this form for each identified PI/PD with each proposal. Submission of the requested information is voluntary and will not affect the organization's eligibility for an award. However, information not submitted will seriously undermine the statistical validity, and therefore the usefulness, of information recieved from others. Any individual not wishing to submit some or all the information should check the box provided for this purpose. (The exceptions are the PI/PD name and the information about prior Federal support, the last question above.)

Collection of this information is authorized by the NSF Act of 1950, as amended, 42 U.S.C. 1861, et seq. Demographic data allows NSF to gauge whether our programs and other opportunities in science and technology are fairly reaching and benefiting everyone regardless of demographic category; to ensure that those in under-represented groups have the same knowledge of and access to programs and other research and educational oppurtunities; and to assess involvement of international investigators in work supported by NSF. The information may be disclosed to government contractors, experts, volunteers and researchers to complete assigned work; and to other government agencies in order to coordinate and assess programs. The information may be added to the Reviewer file and used to select potential candidates to serve as peer reviewers or advisory committee members. See Systems of Records, NSF-50, "Principal Investigator/Proposal File and Associated Records", 63 Federal Register 267 (January 5, 1998), and NSF-51, "Reviewer/Proposal File and Associated Records", 63 Federal Register 268 (January 5, 1998).

List of Suggested Reviewers or Reviewers Not To Include (optional)

SUGGESTED REVIEWERS:

Ed Felten, Computer Science, Princeton University,
Princeton, New Jersey
ed@felten.com

Dan Wallach, Computer Science, Rice University,
Houston, Texas
dwallach@cs.rice.edu

Jerry Saltzer, MIT, Cambridge, Massachusetts
(nominally retired from but still active)
saltzer@mit.edu

Avi Rubin, Johns Hopkins University, Baltimore, Maryland
rubin@jhu.edu

Ross Anderson, University of Cambridge, Cambridge, England
Ross.Anderson@cl.cam.ac.uk

Eugene Spafford, CERIAS, Purdue University, W. Lafayette, Indiana
spaf@CERIAS.purdue.edu

Catherine Meadows, Naval Research Laboratory
meadows@itd.nrl.navy.mil

Peter Denning, Computer Science Department, Naval Postgraduate School, Monterey CA
pjd@nps.navy.mil

Dorothy Denning, Computer Science Department,
Naval Postgraduate School, Monterey CA
dedennin@nps.navy.mil

James Horning, NAI Labs
home@horning.net

REVIEWERS NOT TO INCLUDE:

Not Listed

COVER SHEET FOR PROPOSAL TO THE NATIONAL SCIENCE FOUNDATION

PROGRAM ANNOUNCEMENT/SOLICITATION NO./CLOSING DATE/if not in response to a program announcement/solicitation enter NSF 03-2

NSF 02-168 **12/12/02**

FOR CONSIDERATION BY NSF ORGANIZATION UNIT(S) (Indicate the most specific unit known, i.e. program, division, etc.)

CCR - ITR SMALL GRANTS

FOR NSF USE ONLY

NSF PROPOSAL NUMBER

0313351

DATE RECEIVED	NUMBER OF COPIES	DIVISION ASSIGNED	FUND CODE	DUNS# (Data Universal Numbering System)	FILE LOCATION
				009232752	

EMPLOYER IDENTIFICATION NUMBER (EIN) OR TAXPAYER IDENTIFICATION NUMBER (TIN)

941160950

SHOW PREVIOUS AWARD NO. IF THIS IS
☐ A RENEWAL
☐ AN ACCOMPLISHMENT-BASED RENEWAL

IS THIS PROPOSAL BEING SUBMITTED TO ANOTHER FEDERAL AGENCY? YES ☐ NO ☒ IF YES, LIST ACRONYM(S)

NAME OF ORGANIZATION TO WHICH AWARD SHOULD BE MADE

SRI International

AWARDEE ORGANIZATION CODE (IF KNOWN)

4007712000

ADDRESS OF AWARDEE ORGANIZATION, INCLUDING 9 DIGIT ZIP CODE

333 Ravenswood Avenue
Menlo Park, CA 94025-3493

NAME OF PERFORMING ORGANIZATION, IF DIFFERENT FROM ABOVE

PERFORMING ORGANIZATION CODE (IF KNOWN)

ADDRESS OF PERFORMING ORGANIZATION, IF DIFFERENT, INCLUDING 9 DIGIT ZIP CODE

IS AWARDEE ORGANIZATION (Check All That Apply) (See GPG II.C For Definitions)
☐ SMALL BUSINESS ☐ MINORITY BUSINESS
☐ FOR-PROFIT ORGANIZATION ☐ WOMAN-OWNED BUSINESS

☐ IF THIS IS A PRELIMINARY PROPOSAL THEN CHECK HERE

TITLE OF PROPOSED PROJECT **ITR: Integrity and Accountability in Electronic Election Systems**

REQUESTED AMOUNT	PROPOSED DURATION (1-60 MONTHS)	REQUESTED STARTING DATE	SHOW RELATED PRELIMINARY PROPOSAL NO. IF APPLICABLE
$ **499,942**	**36** months	**09/01/03**	

CHECK APPROPRIATE BOX(ES) IF THIS PROPOSAL INCLUDES ANY OF THE ITEMS LISTED BELOW

☐ BEGINNING INVESTIGATOR (GPG I.A)
☐ DISCLOSURE OF LOBBYING ACTIVITIES (GPG II.C)
☐ PROPRIETARY & PRIVILEGED INFORMATION (GPG I.B, II.C.6)
☐ HISTORIC PLACES (GPG II.C.9)
☐ SMALL GRANT FOR EXPLOR. RESEARCH (SGER) (GPG II.C.11)
☐ VERTEBRATE ANIMALS (GPG II.C.11) IACUC App. Date _____
☐ HUMAN SUBJECTS (GPG II.C.11)
Exemption Subsection _____ or IRB App. Date _____
☐ INTERNATIONAL COOPERATIVE ACTIVITIES: COUNTRY/COUNTRIES INVOLVED (GPG II.C.9)
_____
☐ HIGH RESOLUTION GRAPHICS/OTHER GRAPHICS WHERE EXACT COLOR REPRESENTATION IS REQUIRED FOR PROPER INTERPRETATION (GPG I.E.1)

PI/PD DEPARTMENT
Computer Science Laboratory

PI/PD POSTAL ADDRESS

Menlo Park, CA 940253493
United States

PI/PD FAX NUMBER
650-859-2844

NAMES (TYPED)	High Degree	Yr of Degree	Telephone Number	Electronic Mail Address
PI/PD NAME **Peter Neumann**	**PhD**	**1961**	**650-859-2375**	**neumann@csl.sri.com**
CO-PI/PD **Rebecca T Mercuri**	**PhD**	**2001**	**215-645-5000**	**rmercuri@brynmawr.edu**
CO-PI/PD				
CO-PI/PD				
CO-PI/PD				

Electronic Signature

CERTIFICATION PAGE

Certification for Authorized Organizational Representative or Individual Applicant:

By signing and submitting this proposal, the individual applicant or the authorized official of the applicant institution is: (1) certifying that statements made herein are true and complete to the best of his/her knowledge; and (2) agreeing to accept the obligation to comply with NSF award terms and conditions if an award is made as a result of this application. Further, the applicant is hereby providing certifications regarding debarment and suspension, drug-free workplace, and lobbying activities (see below), as set forth in Grant Proposal Guide (GPG), NSF 03-2. Willful provision of false information in this application and its supporting documents or in reports required under an ensuing award is a criminal offense (U. S. Code, Title 18, Section 1001).

In addition, if the applicant institution employs more than fifty persons, the authorized official of the applicant institution is certifying that the institution has implemented a written and enforced conflict of interest policy that is consistent with the provisions of Grant Policy Manual Section 510; that to the best of his/her knowledge, all financial disclosures required by that conflict of interest policy have been made; and that all identified conflicts of interest will have been satisfactorily managed, reduced or eliminated prior to the institution's expenditure of any funds under the award, in accordance with the institution's conflict of interest policy. Conflicts which cannot be satisfactorily managed, reduced or eliminated must be disclosed to NSF.

Drug Free Work Place Certification

By electronically signing the NSF Proposal Cover Sheet, the Authorized Organizational Representative or Individual Applicant is providing the Drug Free Work Place Certification contained in Appendix A of the Grant Proposal Guide.

Debarment and Suspension Certification

(If answer "yes", please provide explanation.)

Is the organization or its principals presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from covered transactions by any Federal department or agency? Yes ☐ No ☒

By electronically signing the NSF Proposal Cover Sheet, the Authorized Organizational Representative or Individual Applicant is providing the Debarment and Suspension Certification contained in Appendix B of the Grant Proposal Guide.

Certification Regarding Lobbying

This certification is required for an award of a Federal contract, grant, or cooperative agreement exceeding $100,000 and for an award of a Federal loan or a commitment providing for the United States to insure or guarantee a loan exceeding $150,000.

Certification for Contracts, Grants, Loans and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, ''Disclosure of Lobbying Activities,'' in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements and that all subrecipients shall certify and disclose accordingly.

This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

AUTHORIZED ORGANIZATIONAL REPRESENTATIVE	SIGNATURE	DATE
NAME **Richard L Herz**	**Electronic Signature**	**Dec 12 2002 6:42PM**

TELEPHONE NUMBER	ELECTRONIC MAIL ADDRESS	FAX NUMBER
650-859-2004	**richard.herz@sri.com**	**650-859-6171**

*SUBMISSION OF SOCIAL SECURITY NUMBERS IS VOLUNTARY AND WILL NOT AFFECT THE ORGANIZATION'S ELIGIBILITY FOR AN AWARD. HOWEVER, THEY ARE AN INTEGRAL PART OF THE INFORMATION SYSTEM AND ASSIST IN PROCESSING THE PROPOSAL. SSN SOLICITED UNDER NSF ACT OF 1950, AS AMENDED.

PROJECT SUMMARY

We are in the midst of a very ill-advised craze to replace conventional election systems with *self-auditing fully electronic voting machines* that have essentially *no external accountability.* Unfortunately, all of the existing self-auditing fully electronic voting systems provide absolutely no meaningful assurance that votes cast are correctly recorded and counted. The developers and purveyors insist that we must trust them, despite the almost total lack of accountability and a total lack of nontamperable audit trails, and despite the developers' insistence on closed-source proprietary software and interfaces that can in many cases allow software developers and local election officials to alter the software and the voting configurations with no evidence thereof. The opportunities for accidents and fraud are basically unchecked. (For a long time, but especially in the past two years, election system developers and vendors have been increasingly lobbying procurement agencies and election officials, extolling the wonders of their products. Many of their claims relating to properties of their systems are clearly unsubstantiated, and in some cases seriously false.)

The work proposed herein will explore various alternatives for providing significant integrity and independent accountability, including mechanisms and approaches that can surmount the fundamental inadequacies of self-auditing fully electronic voting systems. It addresses various issues throughout the development cycle and subsequent system use, including requirements, system principles, auditing, independent oversight, evaluation, certification, and the relevance of open-source and proprietary software in the context of systems that must be trustworthy beyond reproach. In many respects, the problems associated with attempting to obtain truly trustworthy electronic voting systems represent a paradigmatic difficult case, because of the requirements for a reviewable development process, high system integrity, strong independent accountability, confidentiality of votes, ability to defend against challenges of system/ballot integrity and accountability, defense against denial-of-service attacks, and defense against threats by insiders (including developers and election officials) as well as outsiders (several of the existing machines have external interfaces that are largely omnipotent with respect to the software and the data, and therefore totally subvertible). Overall, achieving integrity and accountability in operational electronic voting systems is an end-to-end problem in which there are numerous potential weak links. In order to have any credibility whatsoever, all of these weak links must be either removed or carefully monitored. As a consequence, the proposed work constructively encompasses issues of system architecture and in some cases network architecture, software engineering, security, privacy, pseudoanonymity, and operational practice. The results of this effort will also be directly applicable to various other applications in which accountability and integrity must be balanced with needs such as privacy, confidentiality, and pseudoanonymity, such as monitoring proper use of sensitive databases without compromising the desired privacy that might otherwise result from the monitoring itself. Participation of graduate students is included.

In addition to the research content, the proposed work will include relevant reports, articles, and a book; educational materials suitable for courses in computer security and political science and for use by election personnel; interactions on standards efforts with NIST, the Federal Election Commission, and the new Election Assistance Commission; and suggestions for design features that can enhance and support voter usability.

TABLE OF CONTENTS

For font size and page formatting specifications, see GPG section II.C.

*Proposers may select any numbering mechanism for the proposal. The entire proposal however, must be paginated. Complete both columns only if the proposal is numbered consecutively.

PROJECT DESCRIPTION

When we refer here to *voting systems,* we actually encompass all of the systems involved in casting and recording ballots, tabulating votes, and distributing the results. (We will not deal extensively with problems in recording registrations and distributing voter records – except in the context of Internet voting; although those problems are of course also a vital part of the voting process, they are generally external to the systems for casting and tabulating votes.) Thus, we consider much more than just the vote-casting machines, although those systems are certainly at the heart of the problem and represent many of the concerns for overall system integrity and accountability.

There are enormous risks of undetectable and unprovable fraud in today's self-auditing fully electronic voting systems, not to mention undetectable and unprovable accidents. In the absence of any meaningful voter-verifiable independent accountability, it is a simple matter for trusted insiders (developers, programmers, administrators) as well as knowledgeable local election officials to tamper with the systems so that votes are not correctly recorded and not correctly counted. (See Inside Risks columns by Neumann [25], Rebecca Mercuri [13, 14, 17, 18], and Mercuri/Neumann jointly [20], in issues of the *Communications of the ACM,* all on the inside back page. Even though Neumann edits this *CACM* series, all of these articles were subjected to review by his ACM Committee on Computers and Public Policy. Also, see Mercuri's article on auditing audit trails [19] in her *CACM* Security Watch series.)

In addition, Neumann has written numerous articles on the subject of actual irregularities in electronic as well as conventional voting systems. These have appeared in the ACM Risks Forum (www.risks.org) and in regular issues of the *ACM Software Engineering Notes.* His *Illustrative Risks* document [29] contains an index to many of those items. In some of these cases reported in the RISKS archives, election results were subsequently determined to be incorrect, sometimes seemingly accidentally (of which there are surprisingly many cases) but sometimes with strong suspicions of fraud (although internal fraud is very difficult to prove in the absence of meaningful accountability, particularly in self-auditing fully electronic systems). Whenever results were suspected to have been wrong (for example, because of divergence from exit polls, or because of evident malfunctions), it is often impossible to distinguish between errors that appear to be accidental and results that might have been caused by intentional internal manipulation. In such cases, the integrity of the election process tends to be left in doubt long after the election itself seems to have been resolved.

As elaborated upon in the biography section and noted in the Merit Review Criteria subsection of the Project Description, Neumann and Mercuri both have been involved in analyzing election system technology for many years. In addition, Dr. Neumann was a participant in two workshops that led to the Caltech/MIT Voting Technology Project final report [1]. Dr. Mercuri was a contributor to the George Washington University Democracy Online Project [6], and testified for Congress on this topic.

The U.S. Government is spending at least $4 billion in Federal funds in new (and supposedly improved) election equipment; however, this is only the tip of an iceberg, because many of the new systems require substantial support, training and services, plus additional ongoing costs. However, this may not be lead to real improvements because of the prevailing environments in which oversight and accountability of the computer systems are almost nonexistent. Clearly, alternatives are

needed.

At present, two basic methods have been proposed for providing much greater integrity and independent voter-verified accountability as an *augmentation* to electronic systems.

- For over a decade, Rebecca Mercuri has urged the use of a voter-verified independent hard-copy machine-readable records. This concept is discussed in greater detail below. If the machine-readable record is used for official tabulations, her method obviates the need to trust the electronic machines (which nevertheless can provide an effective human interface and instant unofficial results).

- Under a different approach, David Chaum (www.chaum.com) has outlined a redundancy-check paper (or other nonelectronic) receipt mechanism (Secret-Ballot Receipts and Transparent Integrity, unpublished memorandum, available at www.vreceipt.com) that can provide substantial assurance of correct results (within a particular probabilistic measure), also with voter verifiability, even if the voting machines themselves are not completely trustworthy, while at the same time ensuring voter privacy. The Chaum approach provides additional assurances that offset the basic weakness of having to trust the vote-casting systems. The Chaum approach still requires some measure of trustworthiness in the voting process (which need not be electronic), and thus is therefore somewhat weaker than the Mercuri Method.

Various cryptographic approaches have also been proposed, but they all suffer from the untrustworthiness of the system environments in which they are implemented. In the absence of a voter-verified completely independent nonsubvertible medium (e.g., paper, film, or perhaps even once-writable memory under suitable circumstances of assured trustworthiness), today's systems provide essentially *zero* accountability as to the integrity of computerized voting. (Note also that in typically nonsecure systems, audit trails can relatively easily be tampered.) Voting on such a machine is thus logically equivalent to LasVegas-style gambling over the Internet using an off-shore computer system that is completely controlled by organized crime.

Background

The lack of integrity and accountability in the voting process is a very old problem. Many of the old and new problems surfaced in 1985 in a series of articles by David Burnham in *The New York Times* (July 29 and 30, August 4 and 21, and December 18, 1985). In Neumann's RISKS section of the July 1986 issue of the *ACM Software Engineering Notes* (volume 11, number 3), there was an analysis of voting system risks based on a talk by Eva Waskell summarized by Ron Newman, enumerating a wide range of problems such as spaghetti code, the same memory locations being used interchangeably for multiple races, undocumented GOTOs, the use of the COBOL ALTER verb that allows self-modifying code, calls to undocumented and unknown subroutines, bypassable audit trails, and so on. In 1988, Ronnie Dugger [9] wrote a long article in *The New Yorker* that discussed many of the problems then perceived. Perhaps most important is a 1988 report by Roy G. Saltman [37] at the National Bureau of Standards (now NIST) that discussed the risks to elections, laying out numerous recommendations on what needed to be done to avoid them. Then, the 1988 Senate race in Florida (in the same four counties using the punch-card equipment that was problematic in the 2000 Presidential election) resulted in 210,000 votes mysteriously disap-

pearing when compared with the totals for the Presidential race — representing a startling 14% of the number of voters whose votes were apparently not counted in those counties.

In the last 20 years, the situation has been growing progressively worse, particularly with the advent of the development of unmonitorable electronic systems. Essentially all of the warnings of Burnham, Dugger, and Saltman from the 1980s have gone unheeded; although the electronic systems make it appear that everything is running smoothly, there has been almost no progress in system integrity and accountability in commercially available voting systems. Even the minimal audit trails that do exist are easily compromised, so that there is little or no integrity even in the little accountability that might seem to exist.

As a further illustration of the lack of progress, contrast the situation today with what Neumann wrote in 1990, in an Inside Risks column in the *CACM* (very slightly edited here for continuity):

***** BEGIN 1990 ARTICLE: *****

Risks in Computerized Elections, Peter G. Neumann
ACM Communications of the ACM, November 1990 [25]

Introduction. Errors and alleged fraud in computer-based elections have been recurring Risks Forum themes. The state of the computing art continues to be primitive. Punch-card systems are seriously flawed and easily tampered with, and still in widespread use. Direct recording equipment is also suspect, with no ballots, no audit trails, and no real assurances that votes cast are properly recorded and processed. Computerized elections are being run or considered in many countries, including some notorious for past riggings; thus, the risks discussed here exist worldwide.

Erroneous results. Computer-related errors occur with alarming frequency in elections. Last year there were reports of uncounted votes in Toronto and doubly counted votes in Virginia and in Durham, North Carolina. Even the U.S. Congress had difficulties when 435 Representatives tallied 595 votes on a Strategic Defense Initiative measure. An election in Yonkers, New York, was reversed because of the presence of leftover test data that accumulated into the totals. Alabama and Georgia also reported irregularities. After a series of mishaps, Toronto has abandoned computerized elections altogether. Most of these cases were attributed to "human error" and not "computer error", and were presumably due to operators and not programmers; however, in the absence of dependable accountability, who can tell?

Fraud. If wrong results can occur accidentally, they can also happen intentionally. Rigging has been suspected in various elections, but lawsuits have been unsuccessful, particularly in the absence of incisive audit trails. In many other cases, fraud could easily have taken place. For many years in Michigan, manual system overrides were necessary to complete the processing of noncomputerized precincts, according to Lawrence Kestenbaum. The opportunities for rigging elections are manifold, including the installation of trapdoors and Trojan horses, child's play for vendors and knowledgeable election officials. Checks and balances are mostly placebos, and easily subverted. Incidentally, Ken Thompson's oft-cited Turing lecture [39] reminds us that tampering can

occur even without any source-code changes; thus, code examination is not enough.

Discussion. The U.S. Congress has the constitutional power to set mandatory standards for Federal elections, but has not yet acted. Existing standards for designing, testing, certifying, and operating computerized vote-counting systems are inadequate and voluntary, and provide few hard constraints, almost no accountability, and no independent expert evaluations. Vendors can hide behind a mask of secrecy with regard to their proprietary programs and practice, especially in the absence of controls. Poor software engineering is thus easy to hide. Local election officials are typically not sufficiently computer literate to fully understand the risks. In many cases, the vendors run the elections.

Reactions in RISKS. John Board at Duke University expressed surprise that it took over a day for the doubling of votes to be detected in eight Durham precincts. Lorenzo Strigini reported last November on a read-ahead synchronization glitch and an operator pushing for speedier results, which together caused the computer program to declare the wrong winner in a city election in Rome, Italy. Many of us have wondered how often errors or frauds have remained undetected.

Conclusions. Providing sufficient assurances for computerized election integrity is a very difficult problem. Serious risks will always remain, and some elections will be compromised. The alternative of counting paper ballots by hand is not promising. But we must question more forcefully whether computerized elections are really worth the risks, and if so, how to impose more meaningful constraints.

NOTE: The Virginia, Durham, Rome, Yonkers, and Michigan cases were discussed in *ACM Software Engineering Notes, 15*, 1, January 1990, 10-13. [Many subsequent cases have appeared in later issues, continuing to the present.]

***** END 1990 ARTICLE: *****

In the 2000 and 2002 elections, numerous cases were reported that raise suspicions regarding the electronic systems: more votes counted than cast; touch-screen choices for one particular candidate showing up on the screen for another candidate on multiple voting machines; vendor personnel "fixing" software on the fly; exit polls radically differing from the official tallies; the failure of the networks' exit-poll systems, blocking the only semblance of independent checks on the integrity of the electronic systems; and so on.

In light of the 2002 election problems, it is clear that the situation is still deplorable, particularly with respect to self-auditing fully electronic election systems. Furthermore, the situation seems to be getting worse, due to the proliferation of self-auditing voting equipment and software that has an even greater potential for global fraud or errors affecting many systems simultaneously, with virtually no controls over auditability and no legislation that resolves what to do in the case of equipment failure, inability to recover data, different results provided on multiply redundant recording mechanisms, and so on.

Not only have the new unauditable electronic systems introduced more security risks and operational difficulties, but they have in many cases (especially in the touch-screen systems) become

more difficult (rather than easier) to use for some members of the general population, as well as for other special populations (such as the palsied, those with shaking hands). They have demonstrated increased start-up, maintenance, and monitoring costs, well beyond those for other, more traditional, balloting methods. For example, it now takes Broward County in Florida two hours (instead of one) to start up their voting machines at the beginning of each election, and they are required to use county employees rather than the regular poll-working staff, because of the complexity of the machines. This cost Broward an additional $2.5 million just to run the November 2002 election, in addition to something on the order of $18 million they spent on the new machines, and with less auditability (some 103,000 votes turned up two days after the election). Such unexpected and ongoing add-on costs are expected to increase as these systems proliferate.

It also needs to be understood that voting over the Internet entails even greater risks, as noted in [32, 36]. The lack of assured trustworthiness is an even more serious obstacle when dealing with the Internet. Essentially everything is a potential weak link, including the file servers that would provide allegedly trustworthy voting software, the Web servers and back-end systems that would accept and count the votes, malicious insiders and random intruders altering software and data, analogs of the Ken Thompson Trojan horse [39], rest-home administrators casting votes for all of their inhabitants, penetrators casting large numbers of unauthorized votes from untraceable off-shore systems, and many other scenarios that enhance the ease of election fraud through technology — rather than eliminating it or greatly reducing it. Internet voting also provides increased opportunities for vote-selling, monitoring, harassment, and control of ballots by other people than the voter. These problems are especially salient in a country that has suffered from voter disenfranchisement, especially of minorities, throughout its entire history.

Previous Research on This Problem

Neumann's 1995 book, *Computer-Related Risks* [26], discusses some of the problems (pages 171–174) and outlines some criteria for computer-based voting, including system integrity, data integrity and reliability, voter authenticity, voter anonymity and data confidentiality. system accountability, system disclosability, system availability, system reliability, interface usability, documentation and assurance, other criteria such as trusted paths and personnel integrity (pages 245–253). It also points out that any such enumeration is intrinsically incomplete.

Dr. Mercuri's Ph.D. thesis (noted below) picks up from there and considers a much more detailed set of requirements and criteria in terms of protection profiles under the Common Criteria framework [11]. It also defines with considerable care the approach that we refer to here as the Mercuri Method, involving an independent voter-verified, nontamperable, but yet private, audit record that can enable trustworthy voting systems even if the primary computer systems are not trustworthy [15, 16]. (See also a recent book chapter by Mercuri and Neumann [21].)

The Mercuri Method and the Chaum Secret-Ballot Receipts are examples of the principle of minimizing what must be trustworthy, thereby reducing the number and scope of the weak links. This principle is explored extensively in Neumann's ongoing work [30] for DARPA's Composable High-Assurance Trustworthy Systems program. His effort also considers the general problem of making more-trustworthy systems out of less-trustworthy subsystems, which is highly relevant here, and addresses reliability, survivability, performance, and other requirements in addition to security.

Inklings of Progress

Indeed, the Mercuri Method is currently incorporated into the electronic voting systems of Avante International Technology, specifically in Vote-Trakker EVC308 and its successor versions, with plans to retrofit it into earlier models. It has also has been used experimentally with considerable reported success in some of machines in the 2002 Brazilian elections [35], although the correctness of about only 3% of the votes was actually checked (that is, the consistency between the electronic tabulations and the paper records).

Synopsis of Dr. Mercuri's Thesis

The subject of electronic voting and vote tabulation involves a unique combination of technological, computational, and sociological problems that produce a set of constraints upon the systems used for ballot entry and vote counting.

This document identifies the various types of voting systems; the hierarchy of constraints under which they are required to operate; and the numerous checks and balances that need to be provided in order to ensure accuracy and integrity. The thesis work involved a detailed assessment of the limitations of electronic vote tabulation systems using the framework of the ISO's Common Criteria. A minimal voting system was described, along with a procedure by which existing and proposed voting systems may be evaluated for potential flaws.

The result demonstrated the existence of a category of systems for which the Common Criteria can be deemed inadequate. The Criteria provides for assessment of system dependencies, but does not account for counter-indications.

Specifically, the requirement for ballot privacy creates an unresolvable conflict with the use of audit trails in providing security assurance.

This result has broad implications within other commercial arenas, particularly those involving anonymous data delivery. Other results involved an appraisal of possible election risks (such as global denial of service and Trojan horse attacks) that are enhanced by the deployment of electronic balloting systems, along with recommendations of considerations that can assist in reducing these vulnerabilities. A discussion of some issues related to the 2000 Florida Presidential election, recount, and litigation is included.

Elements of the Proposed Effort

The proposed effort is expected to address the following items, each in as much detail as permitted by the funding level and time available, and each involving Neumann and Mercuri. Graduate students would be involved in many of these items as well, as appropriate.

1. Pursue research on system requirements, principles, and architectures that can provide meaningful system integrity and independent accountability, with particular interest in, but not totally restricted to, electronic vote casting and electronic vote tabulation. This section of the proposal outlines many of the issues we will consider. Our expertise, background, and previous work (especially [15]) form an excellent starting point.

2. Internet voting will also be considered to the extent that trustworthiness could be assured without having to trust massive portions of the Internet, its attached systems, and its users, perhaps using some of the alternative architecture concepts of Neumann's CHATS project [30]. Although unconstrained schemes for voting over the Internet have been widely condemned as too risky, we will consider whether there are any highly constrained approaches that could be acceptable, for example, limited to certain physical locations.

3. Continue to explore realistic evaluation criteria such as those developed in Dr. Mercuri's doctoral thesis [15], identify weaknesses therein, and iterate on the criteria, providing detailed analyses of the approach and its potential limitations.

4. Provide graduate students with experience in this research area and guidance on potential thesis topics involving relevant problems.

5. Continue to write articles and papers, speak with media, and give talks relating to the risks of self-auditing fully electronic voting systems.

6. Write a book on the risks in electronic elections and what can be done to minimize those risks.

7. Prepare educational materials that can be useful as components in courses on computer security, system architecture, political science, democratic principles, and so on.

8. Work with the National Institute of Standards and Technology, the Federal Election Commission, and the Election Assistance Commission established under the Help America Vote Act of 2002, to offer help in the ongoing effort to dramatically improve the existing standards, necessary components, and oversight. (Mercuri and Neumann both participated in the review of the FEC's 2002 draft standards, but were disappointed that their analyses were only marginally addressed. In addition, Mercuri testified at the early hearings of the Voting Rights Act bills and was instrumental in ensuring that an audit-trail capacity requirement appeared in the final legislation.)

9. Ensure that the resulting recommended approaches will address concerns of voter usability needs, and are capable of being sensibly administered by local election officials and poll workers, without compromising the desired accountability.

10. Develop educational materials that would be useful for government election officials, vendors, and certification authorities, particularly with respect to safeguarding from risks during the development, certification, procurement, deployment, use, and maintenance of the election systems.

11. Develop recommendations for enhancing the procurement process, for example, canonical requirements and evaluation procedures, and general guidance.

12. Explore the tradeoffs among anonymity, semi-anonymity (as in the British approach of recovery by the Government of certain individuals' votes, subject to suitable warrants), marginal anonymity (as in handling of absentee ballots), and so on, within the context of electronic voting, and examine their implications.

13. Explore the tradeoffs between open-source software and proprietary closed-source in the context of electronic voting systems. (For example, see [28] for a general summary.)

14. Examine the viability of escrowing voting system source code, along with the possible benefits and risks.

15. Summarize other tradeoffs, such as those between electronic systems and more conventional (e.g., paper-based) election methods; tradeoffs among legislation, regulation, and litigation, in terms of what defines a vote; how a meaningful recount might be performed when there is no accountability; how recounts can be avoided through significantly increased integrity and accountability; and other relevant issues.

16. Examine the applicability of various approaches to providing significantly greater assurance, such as the use of formal methods in analyzing carefully constrained system architectures.

17. Overall, whether or not the proposed effort is successful in characterizing practical alternatives for major improvements in election integrity and accountability, some conclusions must be drawn relating to the various tradeoffs among other technologies, including optically-read paper ballots and other lower-tech approaches.

The proposed project focuses ostensibly on integrity and accountability in electronic voting systems – as part of complete systems, not as individual components or software in isolation of the operational environments. Many of the results will be directly relevant to other applications within a large family of auditable systems requiring some balance of accountability together with anonymity and privacy. Indeed, the complexity of the paradigmatic security and privacy problems considered in the proposal is prototypically relevant much more broadly, as noted below in the subsection on merit review criteria – under broader impacts of the proposed activity.

Overall, we believe that caution is advisable regarding the rather misguided belief that technology is an easy fix for some of the past problems. High-tech electronic systems are not necessarily better than the more conventional alternatives, a conclusion reached (for example) by the Caltech/MIT study [1]. Indeed, in the absence of meaningful accountability, they may be much worse from the viewpoint of total election system integrity, even though highly popular with election officials because of their speed and avoidance of recounts (even if the results are wildly incorrect). Thus, we expect to characterize many of the potential causes of failure and intentional misuse, along with the associated risks.

Management Plan

The proposed effort will be done by Dr. Peter Neumann and Professor Rebecca Mercuri, as Co-Principal Investigators. They have collaborated extensively on a *pro bono* basis for the past 15 years regarding voting systems, and will be able to communicate by e-mail, Internet, telephone, and in person (on the East coast during the academic years, with protracted joint work largely on the West coast during the summers). During the academic year 2003-3004, she will be on sabattical from Bryn Mawr — during which time she anticipates being associated informally with Princeton.

For the academic year 2004-2005, there is a likelihood of her being considered for a Radcliffe Fellowship. The proposed funding includes full-time summer support for Dr. Mercuri and graduate students (most likely one graduate student each summer, although we might have two one summer and none another summer, depending on when the project begins), with suitable travel support.

Cost Sharing

No cost sharing is required in this proposed effort. However, because Dr. Mercuri's nine-month academic-year salary will be paid while she is on sabbatical from Bryn Mawr College the first year, and anticipating her being on leave under a prospective fellowship the second year, while still being able to work extensively on the proposed effort, considerable financial leverage is expected to be available to enhance the effectiveness of the NSF funding, in addition to providing leverage with respect to her time availability and intellectual involvement in the proposed work. Similarly, Dr. Neumann receives some support from SRI for his ACM and other related activities that address the problems of electronic voting systems.

International Collaborations

There are no anticipated explicit international collaborations in the proposed research, although we are cognizant of efforts in other countries. In particular, Mercuri briefed the United Kingdom Cabinet Office in October 2002, and is tracking electronic elections in other countries as well (e.g., Germany, Brazil). Furthermore, her work was instrumental in the retrofit of the voting systems used in 3 percent of the 2002 Brazilian election [35].

Technology Transfer and Legislative Improvements

There are, of course, potential spin-offs of this work into the commercial marketplace. As noted above, Dr. Mercuri's past work has already had an impact on Avante's product line and has inspired the Brazilian experiment (with machines provided by National Semiconductor, running Microsoft and Unisys software). It is hoped that the proposed work will help goad some of the election system developers into adopting some of the resulting approaches – perhaps along with improved NIST and FEC standards and Federal and State legislation mandating greater integrity and accountability. Note that Dr. Mercuri has already directly influenced the inclusion of audit-trail requirements in the Help America Vote Act and new California and Florida election codes.

Prior NSF Results

There are no prior NSF results of ours directly related to the proposed topic, because we have received no prior funding in this area. An earlier NSF-funded paper by Neumann [24] is relevant to system trustworthiness in general, but is largely superseded by more recent work noted below.

Merit Review Criteria

The intellectual merit of the proposed activity is manifold.

- This project is based on the Principal Investigators' many years of experience in the design of trustworthy systems and the analysis of nontrustworthy systems, treated as systems in the large. It will apply advanced concepts in system and network architecture, requirements formulation, and software engineering. It will take direct advantage of the results of Neumann's current DARPA project on designing systems in which the necessary assurable trustworthiness can be dramatically isolated.

- The results of the work will provide extensive materials for teaching and study relating specifically to the problems of electronic election systems.

- The research will provide considerable leverage for federal, state, and local government entities desiring to improve the integrity of their election process.

- The problems considered are enormously important for the preservation of our democratic form of government.

- The proposers are both extremely well qualified to perform the proposed activity, with a combined experience approaching 40 years relating to the integrity of the election process and approaching 70 years relating to the development and analysis of trustworthy systems.

- The proposed effort is unconstrained in its willingness to consider new alternatives in addition to the Mercuri Method and the Chaum Mechanism outlined herein. If ever thinking out of the box was in order, it is with respect to the problems considered here. However, all of the alternatives considered will be examined for their practical feasibility and their ease of use.

There are numerous broader impacts of the proposed activity.

- As noted in the project summary, the results of this effort will also be directly applicable to various other applications in which accountability and integrity must be balanced with needs such as privacy, confidentiality, and pseudoanonymity, such as monitoring proper use of sensitive databases without compromising the desired privacy that might otherwise result from the monitoring itself. Examples include the maintenance of medical information, genetic records, financial transactions, and other cases in which accuracy and integrity are required along with some form of anonymity.

- The results of the work will provide extensive materials for teaching about trustworthy systems and system architecture, and be of considerable interest to others such as departments of political science and schools of public administration, offering a well-developed analysis of the paradigmatic security and privacy problems represented by electronic election systems.

- When considered in the large, from registration to vote casting to computing the results, today's election systems have had a debilitating and perhaps unexpected effect in disenfranchising many citizens, particularly minority and disabled voters. The recent efforts to facilitate sight-impaired voters have also introduced some new and very serious potential security risks. The proposed work should help significantly in alleviating these problems, and also provide increased awareness for advocates of increased voter education.

- The results will be disseminated broadly, through articles, at least one book, conference papers and panel appearances, and Internet Web documents.
- The benefits to society could be enormous if the research is adopted by a combination of developer altruism and legislative efforts in democratic nations to encourage developer participation in adopting the results. In that the U.S. is looked at as a leader in technology and voting rights, we have a responsibility to the world, not just our own country.
- The proposed effort is strongly motivated by a desire to integrate research and education, to significantly increase the awareness levels of the voting populace and of students who will become voters. The pervasive nature of the security and privacy problems raised by electronic voting system integrity and accountability could have a much greater personal appeal than many of the more subtle ways in which our lives interact with security and privacy issues.

List of All Personnel Associated with the Proposal

Peter G. Neumann, Principal Scientist, Computer Science Laboratory, SRI International, 333 Ravenswood Avenue, Menlo Park, California, 94025-3493. His Harvard University doctoral thesis advisor (1957-1961) was Professor Anthony G. Oettinger (still active). Collaborators in the past 48 months relevant to the proposal area include Rebecca Mercuri (below) and Lauren Weinstein. Other collaborators in the past 48 months include Drew Dean and Sami Saydjari (working on Neumann's DARPA Composable High-Assurance Trustworthy Systems project, at SRI), and Phillip Porras (EMERALD and misuse detection generally, at SRI), in capacities related to trustworthy systems and other research areas in general but not to voting machines in specific. Porras is the only one of the three with whom he has coauthored papers, although Dean and Saydjari were contributors to the DARPA CHATS project. Patrick Lincoln heads SRI's Computer Science Laboratory, so in some sense he can also be called a colLaborator (unless that is stretching a pun too far). In addition, Neumann chairs the ACM Committee on Computers and Public Policy, whose members include Peter Denning, Sy Goodman, Jim Horning, Rob Kling, Nancy Leveson, David Parnas, Jerry Saltzer, Barbara Simons, and Lauren Weinstein, although they act more as a review board for Neumann's ACM activities (including referees for the CACM Inside Risks articles) rather than strict-sense collaborators.

Rebecca T. Mercuri, Assistant Professor in the Department of Mathematics (Computer Science Division), Bryn Mawr College, 101 North Merion Avenue, Bryn Mawr College, Pennsylvania, 19010-2899. Her University of Pennsylvania thesis external advisor was Peter G. Neumann. Her committee also included Penn professors Norman Badler, David Farber, Mitch Marcus, and Lyle Ungar. Her primary collaborator in the past 48 months relevant to the proposal area has been Peter G. Neumann, although in the complete absence of any funding. (Lauren Weinstein coauthored one item with them on Internet voting, also in the absence of any funding.) Essentially all of their collaboration has been pro bono for both of them. Her other collaborators in the past 48 months included co-authors Maria Hristova, Ananya Misra, and Megan Rutter, students at Bryn Mawr, albeit in an essentially unrelated area.

Bibliography

[1] Caltech MIT Voting Technology Project. Voting what is what could be. Technical report, Caltech and MIT, July 2001.

[2] D.D. Clark et al. *Computers at Risk: Safe Computing in the Information Age*. National Research Council, National Academy Press, 2101 Constitution Ave., Washington, D.C. 20418, 5 December 1990. Final report of the System Security Study Committee.

[3] R.C. Daley and P.G. Neumann. A general-purpose file system for secondary storage. In *AFIPS Conference Proceedings, Fall Joint Computer Conference*, pages 213–229. Spartan Books, November 1965.

[4] K.W. Dam and H.S. Lin, editors. *Cryptography's Role In Securing the Information Society*. National Research Council, National Academy Press, 2101 Constitution Ave., Washington, D.C. 20418, 1996. Final report of the Cryptographic Policy Study Committee, ISBN 0-309-05475-3.

[5] D. Dean. *Formal Aspects of Mobile Code Security*. PhD thesis, Computer Science Department, Princeton University, January 1999. (http://www.cs.princeton.edu/sip/pub/ddean-dissertation.php3).

[6] Democracy Online Project. A debate on computerized voting: A new solution for a new generation of voters. Technical report, George Washington University, Washington DC, January 2001.

[7] D.E. Denning, D.L. Edwards, R. Jagannathan, T.F. Lunt, and P.G. Neumann. A prototype IDES: A real-time intrusion-detection expert system. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, 1987.

[8] D.E. Denning and P.G. Neumann, editors. General security policy. In *Multilevel Data Management Security*, Washington D.C., 1983. Chapter 3 of the Report of the 1982 Summer Study, National Academy of Sciences, Air Force Studies Board, Marvin Schaefer, Chairman.

[9] R. Dugger. Annals of democracy (voting by computer). *New Yorker*, November 7, 1988.

[10] R.J. Feiertag and P.G. Neumann. The foundations of a Provably Secure Operating System (PSOS). In *Proceedings of the National Computer Conference*, pages 329–334. AFIPS Press, 1979.

[11] International Standards Organization. *The Common Criteria for Information Technology Security Evaluation, Version 2.1, ISO 15408*. ISO/NIST/CCIB, 19 September 2000. (http://csrc.nist.gov/cc).

[12] R. Jagannathan, T.F. Lunt, D. Anderson, C. Dodd, F. Gilham, C. Jalali, H.S. Javitz, P.G. Neumann, A. Tamaru, and A. Valdes. System Design Document: Next-generation Intrusion-Detection Expert System (NIDES). Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, 9 March 1993.

[13] R. Mercuri. Voting-machine risks. *Communications of the ACM*, 35(11), November 1992. *Inside Risks* column.

[14] R. Mercuri. Corrupted polling. *Communications of the ACM*, 36(11), November 1993. *Inside Risks* column.

[15] R. Mercuri. *Electronic Vote Tabulation Checks and Balances*. PhD thesis, Department of Computer Science, University of Pennsylvania, 2001. (http://www.notablesoftware.com/evote.html).

[16] R. Mercuri. A better ballot box: New electronic voting systems pose risks as well as solutions. *IEEE Spectrum*, pages 46–50, October 2002.

[17] R. Mercuri. Florida 2002: Sluggish systems, vanishing votes. *Communications of the ACM*, 45(11), November 2002. *Inside Risks* column.

[18] R. Mercuri. Uncommon criteria. *Communications of the ACM*, 45(1), January 2002. *Inside Risks* column.

[19] R. Mercuri. On auditing audit trails. *Communications of the ACM*, 46(1), January 2003. *Security Watch* column.

[20] R. Mercuri and P.G. Neumann. System integrity revisited. *Communications of the ACM*, 44(1), January 2001. *Inside Risks* column.

[21] R. Mercuri and P.G. Neumann. Verification for electronic balloting systems. In *Secure Electronic Voting, Advances in Information Security, Volume 7*. Kluwer Academic Publishers, Boston, Massachusetts, 2002.

[22] P.G. Neumann. *Funktionale Prefixcodes als Grundlage der praktischen Verschulüsselung*. Thesis for Dr rerum naturum degree, Department of Mathematics and Physics, Technische Hochschule, Darmstadt, Germany, June 1960.

[23] P.G. Neumann. *Efficient Error-Limiting Variable-Length Codes*. PhD thesis, Department of Applied Mathematics, Harvard University, May 1961. Published as report BL-28, Theory of Switching, The Computation Laboratory, Harvard University.

[24] P.G. Neumann. On the design of dependable computer systems for critical applications. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, October 1990. CSL Technical Report CSL-90-10.

[25] P.G. Neumann. Risks in computerized elections. *Communications of the ACM*, 33(11):170, November 1990. *Inside Risks* column.

[26] P.G. Neumann. *Computer-Related Risks*. ACM Press, New York, and Addison-Wesley, Reading, Massachusetts, 1995. ISBN 0-201-55805-X.

[27] P.G. Neumann. Practical architectures for survivable systems and networks. Technical report, Final Report, Phase Two, Project 1688, SRI International, Menlo Park, California, June 2000. (http://www.csl.sri.com/neumann/survivability.html).

[28] P.G. Neumann. Robust nonproprietary software. In *Proceedings of the 2000 Symposium on Security and Privacy*, pages 122–123, Oakland, California, May 2000. IEEE Computer Society. (http://www.csl.sri.com/neumann/ieee00.ps and http://www.csl.sri.com/neumann/ieee00.pdf).

[29] P.G. Neumann. Illustrative risks to the public in the use of computer systems and related technology, index to RISKS cases. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, 2003. The most recent version is available online in html form for browsing at http://www.csl.sri.com/neumann/illustrative.html), and also in .ps and .pdf form for printing in a much denser format.

[30] P.G. Neumann. Principled assuredly trustworthy composable architectures. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, April 2003. Emerging draft final report, SRI Project 11459, updating the first-year Interim Report, June 29, 2002, http://www.csl.sri.com/neumann/chats4.html; also chats4.ps and chats4.pdf.

[31] P.G. Neumann, R.S. Boyer, R.J. Feiertag, K.N. Levitt, and L. Robinson. A Provably Secure Operating System: The system, its applications, and proofs. Technical report, Computer Science Laboratory, SRI International, Menlo Park, California, May 1980. 2nd ed., Report CSL-116.

[32] P.G. Neumann, R. Mercuri, and L. Weinstein. Internet and electronic voting. *ACM Software Engineering Notes*, 26(2):8, March 2001. Earlier version in the Risks Forum, volume 21 number 14.

[33] P.G. Neumann and P.A. Porras. Experience with EMERALD to date. In *Proceedings of the First USENIX Workshop on Intrusion Detection and Network Monitoring*, pages 73–80, Santa Clara, California, April 1999. USENIX. http://www.csl.sri.com/neumann/det99.html.

[34] P.A. Porras and P.G. Neumann. EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances. In *Proceedings of the Nineteenth National Computer Security Conference*, pages 353–365, Baltimore, Maryland, 22-25 October 1997. NIST/NCSC.

[35] H. Riebeek. Brazil holds all-electronic national election. *IEEE Spectrum*, pages 25–26, November 2002.

[36] A. Rubin. Security considerations for remote electronic voting. *Communications of the ACM*, 45(12):39–44, December 2002.

[37] R.G. Saltman. Accuracy, integrity, and security in computerized vote-tallying. Technical report, National Bureau of Standards (now NIST) special publication, Gaithersburg, Maryland, 1988.

[38] M. Schaefer et al. *Multilevel Data Management Security*. Air Force Studies Board, National Research Council, National Academy Press, 1983. Final report of the 1982 Multilevel Data Management Security Committee.

[39] K.L. Thompson. Reflections on trusting trust. *Communications of the ACM*, 27(8):761–763, August 1984.

[40] C. Wang. *A Security Architecture for Survivable Systems*. PhD thesis, Department of Computer Science, University of Virginia, January 2001. (http://www.cs.virginia.edu).

BIOGRAPHY for Peter Neumann

Peter G. Neumann (Neumann@CSL.sri.com, http://www.csl.sri.com/neumann) received three degrees from Harvard: AB in Mathematics cum laude in 1954, SM in Applied Mathematics in 1955, and PhD in 1961. (There was no computer science department in those days.) He also received a Dr rerum naturarum from the Technische Hochschule, Darmstadt, Germany, in 1960, while on a Fulbright from 1958 to 1960. Anthony G. Oettinger and Alwin Walther were the advisors for his Harvard [23] and Darmstadt [22] doctoral theses, respectively.

He was an Adjunct Professor at the University of Maryland in the fall of 1999, where he taught a course of his own creation on survivable systems and networks. He was also a visiting Mackay Lecturer at Berkeley throughout the 1970–1971 academic year, and before that at Stanford in the spring quarter of 1964. He was also a teaching fellow and research assistant at Harvard for most of his graduate residence from 1954 to 1958.

He has worked in the computer field since 1953, when he was a summer student at the Naval Ordnance Lab in White Oak, Maryland. In the Computer Science Lab at Bell Telephone Labs at Murray Hill, New Jersey, throughout the 1960s, he was involved in research in computers and communications; during 1965 through 1969, he participated extensively in the design, development, and management of Multics, jointly with MIT and Honeywell, and led the Multics efforts at Bell Labs.

In the Computer Science Laboratory at SRI since 1971, where he is now Principal Scientist, he has been concerned with computer systems having stringent requirements for security, reliability, human safety, and high assurance (including formal methods). He has been technically involved in electronic voting systems in one way or another for the past 20 years. He was part of the SRI team that wrote the requirements for the New York City Election Project's desired electronic voting systems, helped evaluate the proposals, and later was called on to examine the source code of the selected system (under nondisclosure agreements to the City and the developer). His analysis and testimony apparently had some influence on the Board of Elections canceling the contract. Since then, he has been a strong critic of voting machines that provide little or no accountability, testifying for the California Assembly (January 17, 2001, http://www.csl.sri.com/neumann/calass.pdf) and the Houston City Council (July 9-10 2001), and generally advising on the risks involved in trusting unaccountable computers in elections.

His most relevant recent publications include a book, *Computer-Related Risks* [26] (which incorporates the paper [25]), a report [27] on architectures for highly survivable and secure systems and networks, and the emerging report [30] for DARPA's Composable High Assurance Trustworthy Systems program, available on his Web site. All of these publications are directly relevant to the proposed work. In particular, the book includes a set of requirements for electronic voting machines that later became the basis for Rebecca Mercuri's doctoral thesis (see below), in which she elaborated extensively on those requirements and the difficulties of fulfilling them. The CHATS report considers architectures that localize the need for trustworthiness. He has also discussed the risks of electronic voting extensively in the ACM Risks Forum (www.risks.org) and in his quarterly columns in the ACM SIGSOFT *Software Engineering Notes.*

Other work is also relevant, but less specifically so. For example, in addition to being heavily involved in the design and development of a very secure system, Multics (e.g., the file-system design [3]), he was principal investigator for the Provably Secure Operating System design (1973-

1980) [10, 31], whose strongly typed architecture led to Honeywell and Secure Computing Corporation systems, under the sponsorship of NSA. He has been involved in SRI's work on anomaly and misuse detection for the past 20 years, including IDES [7] and NIDES [12], and more recently co-authored two basic papers on EMERALD [34, 33], the latter given the best-paper award at the First USENIX Workshop on Intrusion Detection and Network Monitoring. He was an original member of the SeaView team that produced a multilevel-secure database management system based on a security kernel but not requiring any MLS trustworthiness in the DBMS, based on a recommendation of the National Academy of Sciences summer study group co-chaired by him and Dorothy Denning [8]. All of those efforts address integrity and accountability. His NSF-funded 1990 paper [24] is noted above.

Dr. Neumann served on doctoral thesis committees for Jeff Ullman at Princeton (1960s), Drew Dean at Princeton (1999, relating to formal aspects of mobile code security [5]), Lenny Foner at MIT (1999, relating to security and privacy in a data-sharing environment), Chenxi Wang at the University of Virginia (2001, on obfuscation to hinder reverse engineering [40]), and most recently Rebecca Mercuri at the University of Pennsylvania (2001, *Electronic Vote Tabulation: Checks & Balances* [15], most relevant to the present proposal, in its treatment of the integrity and lack of integrity in the electronic voting-system process [15]). He was technically Dr. Mercuri's External Advisor, but in reality her principal advisor on this subject.

He has been on three National Academy of Sciences studies, relating to multilevel secure databases (1982 [38]), Computers at Risk (1989–1990 [2]) and U.S. cryptographic policy (1994–1996 [4]). He is a member of the U.S. General Accounting Office Executive Council on Information Management and Technology. He is also a member of the National Science Foundation Computer Information Science and Engineering Advisory Board.

For the ACM, he was founder of SIGSOFT's Software Engineering Notes in 1976 and editor for 18 years; Chairman of the ACM Committee on Computers and Public Policy (since 1985); co-chairman of the ACM Advisory Committee on Security and Privacy (created in 2001); and a Contributing Editor for CACM (since 1990) for the monthly 'Inside Risks' column. In 1985 he created, and still moderates, the ACM Forum on Risks to the Public in the Use of Computers and Related Technology, which is one of the most widely read of the serious online computer newsgroups. His RISKS-derived book (*Computer-Related Risks,* Addison-Wesley, 1995) is in its fifth printing, and is now also available in Japanese.

His Website (http://www.CSL.sri.com/neumann) includes testimonies for Senate and House committees, on risks in the critical infrastructures, cryptography, URLs for the Risk Forum, and other items.

He is a Fellow of the American Association for the Advancement of Science, the ACM, and the Institute of Electrical and Electronics Engineers. He has received the ACM Outstanding Contribution Award for 1992, the first SRI Exceptional Performance Award for Leadership in Community Service in 1992, the Electronic Frontier Foundation Pioneer Award in 1996, the ACM SIGSOFT Distinguished Service Award in 1997, the CPSR Norbert Wiener Award in October 1997, for "deep commitment to the socially responsible use of computing technology", and the National Computer Systems Security Award in 2002.

BIOGRAPHY for Rebecca Mercuri (SRI Proposal Number ECU 02-475)

Rebecca Mercuri (www.notablesoftware.com/evote.html, mercuri@acm.org) is an Assistant Professor in the Department of Mathematics (Computer Science Division), Bryn Mawr College. She received her Ph.D. from the School of Engineering and Applied Science at the University of Pennsylvania in 2001, after receiving an M.S.Eng. there in 1990. Earlier degrees include an M.S. in Computer Science from Drexel University (1989), a B.S. in Computer Science from the Pennsylvania State University (1979), and a B.S. in Music from the University of the Arts (1977). Prior to her employment at Bryn Mawr in 2000, she spent 20 years in industry, both as an independent contractor with Notable Software, Inc., the consulting firm she founded, and as a regular employee. Positions included Visiting Member of Technical Staff, AT&T Bell Labs; Associate Member of Technical Staff, RCA David Sarnoff Research Center; independent contractor at Intel, Federal Aviation Administration, Philadelphia Stock Exchange; and subcontractor for the U.S. Departments of Defense and Education, and for Merck, Inc.

Her research interests focus on interactive real-time systems, with an emphasis on digital multimedia and computer-related risks and security issues. Dr. Mercuri has been acclaimed as one of the leading experts on electronic vote tabulation – she has published more than a dozen papers (and her doctoral thesis [15]) on this subject, and testified in Florida election hearings in 2000 and 2002. She also provides expert witness and election consultation services worldwide.

She organized and chaired a session on Security and Auditability of Electronic Vote Tabulation Systems for the 1993 National Computer Security Conference in Baltimore, sponsored by NIST and NSA. She also organized and chaired a session on Electronic Voting: Threats to Democracy, for the Third Conference on Computers, Freedom, and Privacy, in March 1993. In addition, she was an invited panelist on voting-system topics, for the annual conference of Computer Professionals for Social Responsibility (October 1996), a National Press Club session (January 2001), the 27th Asilomar Microcomputer Workshop (April 2001), and the 24th Annual Conference of the Council on Government Ethics and Laws (September 2002).

Her comments and theories have been quoted by the *Wall Street Journal, The Economist, Scientific American, The New York Times, U.S. News and World Report*, the Associated Press, National Public Radio, and other major news services. She writes a quarterly column on computer security in *Communications of the ACM,* and is a frequent guest columnist to *CACM*'s Inside Risks. She has received awards from the National ACM and Region 1 of the IEEE for her service as co-founder and long-time board member of the Princeton ACM/IEEE Computer Society. Dr. Mercuri was elected to membership in Upsilon Pi Epsilon, the Computer Science honor society.

The five most relevant publications (apart from her doctoral thesis, which is clearly most relevant of all) are:

- Rebecca Mercuri, A Better Ballot Box?, *IEEE Spectrum,* October 2002, pp. 446–50 [16].
- Rebecca Mercuri, Computer Security: Quality Rather than Quantity, Security Watch column, *Communications of the ACM,* 45, 10, pp. 11–14, October 2002.
- Rebecca Mercuri, Humanizing Voting Interfaces, *Usability Professionals' Association Conference Proceedings*, July 11, 2002.
- Peter Neumann, Rebecca Mercuri, Lauren Weinstein, Internet and Electronic Voting,

ACM Software Engineering Notes (SIGSOFT), 26, 3, p. 8, March 2001 [32].
• D.D. Seligmann, Rebecca T. Mercuri, and John T. Edmark, Providing Assurances in a Multimedia Interactive Environment, *Proceedings of ACM SIGCHI '95*, May, 1995.

Other publications worthy of note here, with considerable general relevance even if not specifically addressing electronic voting systems, include the following:

• R.T. Mercuri, On Auditing Audit Trails, Security Watch column, *Communications of the ACM*, January 2003 [19].
• R.T. Mercuri, Physical Verifiability of Computer Systems, *Proceedings of the Fifth International Computer Virus and Security Conference*, March 1992.
• R.T. Mercuri, In Search of Academic Integrity, *Communications of the ACM*, 40, 5, pp. 11-14, May 1998.

All of these and other publications are available on her Web site.

Dr. Mercuri has no current research support, all previously funded projects having been concluded. She is currently listed as one of nine proposed co-principal investigators (with members of Princeton University's Sociology, Computer Science, and Electrical Engineering Departments) in an NSF IGERT proposal on Pervasive Information Systems.

SUMMARY PROPOSAL BUDGET YEAR 1

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **Bryn Mawr College**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Rebecca T Mercuri**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Rebecca T Mercuri - Co-PI**	**0.00**	**0.00**	**3.00**	$ **23,867**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**3.00**	**23,867**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**23,867**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**4,773**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**28,640**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**8,300**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**1,200**	
TOTAL OTHER DIRECT COSTS				**1,200**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**38,140**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Salary (Rate: 21.0000, Base: 23867)**					
TOTAL INDIRECT COSTS (F&A)				**5,012**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**43,152**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.C.6.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **43,152**	$

M. COST SHARING PROPOSED LEVEL $ **10,024** AGREED LEVEL IF DIFFERENT $

PI/PD NAME: **Rebecca T Mercuri**

ORG. REP. NAME*: **Richard herz**

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

 ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

SUMMARY PROPOSAL BUDGET YEAR 2

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **Bryn Mawr College**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Rebecca T Mercuri**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Rebecca T Mercuri - Co-PI**	**0.00**	**0.00**	**3.00**	$ **24,822**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**3.00**	**24,822**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**24,822**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**4,964**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**29,786**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**8,300**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**1,200**	
TOTAL OTHER DIRECT COSTS				**1,200**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**39,286**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Salary (Rate: 21.0000, Base: 24822)**					
TOTAL INDIRECT COSTS (F&A)				**5,213**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**44,499**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.C.6.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **44,499**	$

M. COST SHARING PROPOSED LEVEL $ **10,425** AGREED LEVEL IF DIFFERENT $

PI/PD NAME: **Rebecca T Mercuri**

ORG. REP. NAME*: **Richard herz**

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

 ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

SUMMARY PROPOSAL BUDGET YEAR 3

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION: **Bryn Mawr College**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Rebecca T Mercuri**

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Rebecca T Mercuri - Co-PI**	**0.00**	**0.00**	**3.00**	$ **25,815**	$
2.					
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**3.00**	**25,815**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**25,815**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**2,237**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**28,052**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**8,300**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**1,200**	
TOTAL OTHER DIRECT COSTS				**1,200**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**37,552**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **Salary (Rate: 21.0000, Base: 25815)**					
TOTAL INDIRECT COSTS (F&A)				**5,421**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**42,973**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.C.6.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **42,973**	$

M. COST SHARING PROPOSED LEVEL $ **10,842** AGREED LEVEL IF DIFFERENT $

PI/PD NAME: **Rebecca T Mercuri**

ORG. REP. NAME*: **Richard herz**

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

 ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

SUMMARY PROPOSAL BUDGET

Cumulative

FOR NSF USE ONLY		
PROPOSAL NO.	DURATION (months) Proposed	Granted
AWARD NO.		

ORGANIZATION
Bryn Mawr College

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Rebecca T Mercuri

A. SENIOR PERSONNEL: PI/PD, Co-PI's, Faculty and Other Senior Associates (List each separately with title, A.7. show number in brackets)	NSF Funded Person-mos. CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Rebecca T Mercuri - Co-PI**	**0.00**	**0.00**	**9.00**	$ **74,504**	$
2.					
3.					
4.					
5.					
6. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	**0.00**	**0.00**	**0.00**	**0**	
7. (**1**) TOTAL SENIOR PERSONNEL (1 - 6)	**0.00**	**0.00**	**9.00**	**74,504**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL ASSOCIATES	**0.00**	**0.00**	**0.00**	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	**0.00**	**0.00**	**0.00**	**0**	
3. (**0**) GRADUATE STUDENTS				**0**	
4. (**0**) UNDERGRADUATE STUDENTS				**0**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**74,504**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**11,974**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**86,478**	
D. EQUIPMENT (LIST ITEM AND DOLLAR AMOUNT FOR EACH ITEM EXCEEDING $5,000.)					
TOTAL EQUIPMENT				**0**	
E. TRAVEL 1. DOMESTIC (INCL. CANADA, MEXICO AND U.S. POSSESSIONS)				**24,900**	
2. FOREIGN				**0**	
F. PARTICIPANT SUPPORT COSTS					
1. STIPENDS $ **0**					
2. TRAVEL **0**					
3. SUBSISTENCE **0**					
4. OTHER **0**					
TOTAL NUMBER OF PARTICIPANTS (**0**) TOTAL PARTICIPANT COSTS				**0**	
G. OTHER DIRECT COSTS					
1. MATERIALS AND SUPPLIES				**0**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**0**	
3. CONSULTANT SERVICES				**0**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**3,600**	
TOTAL OTHER DIRECT COSTS				**3,600**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**114,978**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE)					
TOTAL INDIRECT COSTS (F&A)				**15,646**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**130,624**	
K. RESIDUAL FUNDS (IF FOR FURTHER SUPPORT OF CURRENT PROJECTS SEE GPG II.C.6.j.)				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **130,624**	$

M. COST SHARING PROPOSED LEVEL $ **31,291** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Rebecca T Mercuri

ORG. REP. NAME*
Richard herz

FOR NSF USE ONLY		
INDIRECT COST RATE VERIFICATION		
Date Checked	Date Of Rate Sheet	Initials - ORG

C ***ELECTRONIC SIGNATURES REQUIRED FOR REVISED BUDGET**

Budget Justification Page

Salary - Co-PI will spend 3 summer months and 1 month during the academic year working on this project. Summer salary is requested and the 1 month academic year salary will be covered by Bryn Mawr College. Salary is calculated based on annual academic salary and incremented by 4% annually.

Fringe Benefits - Fringe benefits are calculated at 20% on summer salary and 26% on academic year salary. Academic year fringe benefits will be covered by Bryn Mawr College.

Travel - Co-PI will make four trips per year to SRI in California during the year with several weeks spent on-site at SRI. Calculation is made for living quarters ($1500/mo.) and car rental ($500/mo). In addition, airfare is calculated at a maximum of $800 per trip. Co-PI will also attend at least one conference per year for the purpose of presentation. The cost for the conference is calculated at $1500/yr.

Other Supplies - Co-PI will need a high speed link, phone line, and data line to her home for this project. The cost is estimated at $100/mo.

Indirect Costs - Indirect Costs are calculated at 21% (off-campus rate)of salaries and wages.

Current and Pending Support

(See GPG Section II.D.8 for guidance on information to include on this form.)

The following information should be provided for each investigator and other senior personnel. Failure to provide this information may delay consideration of this proposal.

Investigator: **Peter Neumann**	Other agencies (including NSF) to which this proposal has been/will be submitted.

Support: ☒ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title: **Architectural Frameworks for Composable Survivability and Security**

Source of Support: **DARPA/SPAWAR**

Total Award Amount: $ **1,076,438** Total Award Period Covered: **06/29/01 - 06/28/03**

Location of Project: **Menlo Park, CA**

Person-Months Per Year Committed to the Project. Cal:**4.00** Acad: **0.00** Sumr: **0.00**

Support: ☒ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title: **Discerning Attacker Intent**

Source of Support: **MPO**

Total Award Amount: $ **1,082,678** Total Award Period Covered: **04/18/00 - 04/17/03**

Location of Project: **Menlo Park, CA**

Person-Months Per Year Committed to the Project. Cal:**0.50** Acad: **0.00** Sumr: **0.00**

Support: ☐ Current ☒ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title: **ITR: Integrity and Accountability in Electronic Election Systems**

Source of Support: **NSF**

Total Award Amount: $ **499,942** Total Award Period Covered: **09/01/03 - 09/01/06**

Location of Project: **Menlo Park, CA**

Person-Months Per Year Committed to the Project. Cal:**2.00** Acad: **0.00** Sumr: **0.00**

Support: ☐ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title:

Source of Support:

Total Award Amount: $ Total Award Period Covered:

Location of Project:

Person-Months Per Year Committed to the Project. Cal: Acad: Sumr:

Support: ☐ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title:

Source of Support:

Total Award Amount: $ Total Award Period Covered:

Location of Project:

Person-Months Per Year Committed to the Project. Cal: Acad: Summ:

*If this project has previously been funded by another agency, please list and furnish information for immediately preceding funding period.

Current and Pending Support

(See GPG Section II.D.8 for guidance on information to include on this form.)

The following information should be provided for each investigator and other senior personnel. Failure to provide this information may delay consideration of this proposal.

Investigator: **Rebecca Mercuri**

Other agencies (including NSF) to which this proposal has been/will be submitted.

Support: ☐ Current ☒ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title: **ITR: Integrity and Accountability in Electronic Election Systems**

Source of Support: **NSF/SRI International**

Total Award Amount: $ **130,624** Total Award Period Covered: **09/01/03 - 08/31/06**

Location of Project: **Menlo Park, CA**

Person-Months Per Year Committed to the Project. Cal: **0.00** Acad: **0.00** Sumr: **3.00**

Support: ☐ Current ☐ Pending ☒ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title: **NSF IGERT - Pervasive Information Systems**

Source of Support: **NSF/Princeton University**

Total Award Amount: $ **250,000** Total Award Period Covered: **09/01/03 - 08/31/08**

Location of Project: **Bryn Mawr, PA**

Person-Months Per Year Committed to the Project. Cal: **2.00** Acad: **2.00** Sumr: **0.00**

Support: ☐ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title:

Source of Support:

Total Award Amount: $ Total Award Period Covered:

Location of Project:

Person-Months Per Year Committed to the Project. Cal: Acad: Sumr:

Support: ☐ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title:

Source of Support:

Total Award Amount: $ Total Award Period Covered:

Location of Project:

Person-Months Per Year Committed to the Project. Cal: Acad: Sumr:

Support: ☐ Current ☐ Pending ☐ Submission Planned in Near Future ☐ *Transfer of Support

Project/Proposal Title:

Source of Support:

Total Award Amount: $ Total Award Period Covered:

Location of Project:

Person-Months Per Year Committed to the Project. Cal: Acad: Summ:

*If this project has previously been funded by another agency, please list and furnish information for immediately preceding funding period.

FACILITIES, EQUIPMENT & OTHER RESOURCES

FACILITIES: Identify the facilities to be used at each performance site listed and, as appropriate, indicate their capacities, pertinent capabilities, relative proximity, and extent of availability to the project. Use "Other" to describe the facilities at any other performance sites listed and at sites for field studies. USE additional pages as necessary.

Laboratory:

Clinical:

Animal:

Computer: **The proposed research will be conducted using the computational facilities of the Computer Science Laboratory (CSL) and the System Design Laboratory (SDL), SRI International, Menlo Park, California. CSL/SDL supports its own research facility consisting of over 100 workstations, and over 30 file servers (providing over two**

Office:

Other: _____

MAJOR EQUIPMENT: List the most important items available for this project and, as appropriate identifying the location and pertinent capabilities of each.

OTHER RESOURCES: Provide any information describing the other resources available for the project. Identify support services such as consultant, secretarial, machine shop, and electronics shop, and the extent to which they will be available for the project. Include an explanation of any consortium/contractual arrangements with other organizations.

Continuation Page:

COMPUTER FACILITIES (continued):

terabytes of storage) and CPU servers including several multiprocessor machines. Most of the computing facility is running Linux, with dedicated machines running FreeBSD, SunOS, Solaris, AIX and Digital UNIX. Several personal computers are available running Windows. A printing service is maintained providing high-quality monochrome and color printing. All of the servers, workstations and printers are connected to a high-capacity Cisco switch providing 200MB links to offices, and by multiple redundant links to the Internet. Telecommuting access is also supported, by means of dedicated high-speed ISDN and DSL links to staff homes.

Nona C. Smith, Director
Office of Sponsored Ressearch
Bryn Mawr College
101 North Merion Avenue
Bryn Mawr, PA 19010-2899
610 526-5298 FAX: 610 526-5165

B R Y N M A W R

STATEMENT OF INTENT

It is the intent of Bryn Mawr College of Bryn Mawr, Pennsylvania to enter into a sub-granting agreement with SRI, a non-profit corporation in Palo Alto, California upon the receipt by the SRI of a grant from the National Science Foundation funding Dr. Peter Neumann's proposal entitled "ITR: Integrity and Accountability in Electronic Election Systems." It is understood that the sub-granting agreement will be based on the budget submitted by Dr. Rebecca T. Mercuri (as included in the proposal) in the amount of $130,624 to support Dr. Mercuri's component of the above named project.

The appropriate programmatic and administrative personnel of each institution involved in this grant application are aware of the National Science Foundation's Grant Policy regarding consortiums and are prepared to establish the necessary inter-institutional agreement(s) consistent with that policy.

DATE:

December 10, 2002

BRYN MAWR COLLEGE

Nona C. Smith

Nona C. Smith,
Director of Sponsored Research
Bryn Mawr College