02 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.C.a. 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: Thomas J Misa

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).

02 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.C.a. 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: Jeffrey R Yost

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:
Not Listed

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 10-1

NSF 10-575 **12/17/10**

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

CNS - TRUSTWORTHY COMPUTING

FOR NSF USE ONLY

NSF PROPOSAL NUMBER

1116862

DATE RECEIVED	NUMBER OF COPIES	DIVISION ASSIGNED	FUND CODE	DUNS# (Data Universal Numbering System)	FILE LOCATION
12/17/2010	2	05050000 CNS	7795	555917996	12/20/2010 9:12am S

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

416007513

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

University of Minnesota-Twin Cities

AWARDEE ORGANIZATION CODE (IF KNOWN)

0023879000

ADDRESS OF AWARDEE ORGANIZATION, INCLUDING 9 DIGIT ZIP CODE

200 OAK ST SE
MINNEAPOLIS, MN 55455-5200

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 **TC:Small:Building an Infrastructure for Computer Security History: Phase One -- Mainframes to the Advent of the World Wide Web, 1965-early 1990s**

REQUESTED AMOUNT	PROPOSED DURATION (1-60 MONTHS)	REQUESTED STARTING DATE	SHOW RELATED PRELIMINARY PROPOSAL NO. IF APPLICABLE
$ **437,300**	**36** months	**06/01/11**	

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

☐ BEGINNING INVESTIGATOR (GPG I.G.2)
☐ DISCLOSURE OF LOBBYING ACTIVITIES (GPG II.C.1.e)
☐ PROPRIETARY & PRIVILEGED INFORMATION (GPG I.D, II.C.1.d)
☐ HISTORIC PLACES (GPG II.C.2.j)
☐ EAGER* (GPG II.D.2) ☐ RAPID** (GPG II.D.1)
☐ VERTEBRATE ANIMALS (GPG II.D.6) IACUC App. Date _____
PHS Animal Welfare Assurance Number _____

☒ HUMAN SUBJECTS (GPG II.D.7) Human Subjects Assurance Number _____
Exemption Subsection **2** or IRB App. Date _____
☐ INTERNATIONAL COOPERATIVE ACTIVITIES: COUNTRY/COUNTRIES INVOLVED (GPG II.C.2.j)
_____
☐ HIGH RESOLUTION GRAPHICS/OTHER GRAPHICS WHERE EXACT COLOR REPRESENTATION IS REQUIRED FOR PROPER INTERPRETATION (GPG I.G.1)

PI/PD DEPARTMENT
Electrical and Computer Engineering

PI/PD FAX NUMBER
612-625-8054

PI/PD POSTAL ADDRESS
222 - 21st Avenue South
Charles Babbage Institute - 211 Andersen
Minneapolis, MN 55455
United States

NAMES (TYPED)	High Degree	Yr of Degree	Telephone Number	Electronic Mail Address
PI/PD NAME **Thomas J Misa**	**PhD**	**1987**	**612-624-5050**	**tmisa@umn.edu**
CO-PI/PD **Jeffrey R Yost**	**PhD**	**1998**	**612-624-5050**	**yostx003@tc.umn.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 Authorized Organizational Representative or Individual Applicant 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, lobbying activities (see below), responsible conduct of research, nondiscrimination, and flood hazard insurance (when applicable) as set forth in the NSF Proposal & Award Policies & Procedures Guide, Part I: the Grant Proposal Guide (GPG) (NSF 10-1). 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).

Conflict of Interest Certification

In addition, if the applicant institution employs more than fifty persons, by electronically signing the NSF Proposal Cover Sheet, the Authorized Organizational Representative 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 the NSF Proposal & Award Policies & Procedures Guide, Part II, Award & Administration Guide (AAG) Chapter IV.A; 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 Exhibit II-3 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 Exhibit II-4 of the Grant Proposal Guide.

Certification Regarding Lobbying

The following 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.

Certification Regarding Nondiscrimination

By electronically signing the NSF Proposal Cover Sheet, the Authorized Organizational Representative is providing the Certification Regarding Nondiscrimination contained in Exhibit II-6 of the Grant Proposal Guide.

Certification Regarding Flood Hazard Insurance

Two sections of the National Flood Insurance Act of 1968 (42 USC §4012a and §4106) bar Federal agencies from giving financial assistance for acquisition or construction purposes in any area identified by the Federal Emergency Management Agency (FEMA) as having special flood hazards unless the:
(1) community in which that area is located participates in the national flood insurance program; and
(2) building (and any related equipment) is covered by adequate flood insurance.

By electronically signing the NSF Proposal Cover Sheet, the Authorized Organizational Representative or Individual Applicant located in FEMA-designated special flood hazard areas is certifying that adequate flood insurance has been or will be obtained in the following situations:
(1) for NSF grants for the construction of a building or facility, regardless of the dollar amount of the grant; and
(2) for other NSF Grants when more than $25,000 has been budgeted in the proposal for repair, alteration or improvement (construction) of a building or facility.

Certification Regarding Responsible Conduct of Research (RCR)
(This certification is not applicable to proposals for conferences, symposia, and workshops.)

By electronically signing the NSF Proposal Cover Sheet, the Authorized Organizational Representative of the applicant institution is certifying that, in accordance with the NSF Proposal & Award Policies & Procedures Guide, Part II, Award & Administration Guide (AAG) Chapter IV.B., the institution has a plan in place to provide appropriate training and oversight in the responsible and ethical conduct of research to undergraduates, graduate students and postdoctoral researchers who will be supported by NSF to conduct research.
The undersigned shall require that the language of this certification be included in any award documents for all subawards at all tiers.

AUTHORIZED ORGANIZATIONAL REPRESENTATIVE	SIGNATURE	DATE
NAME **Kevin J McKoskey**	**Electronic Signature**	**Dec 17 2010 2:48PM**

TELEPHONE NUMBER	ELECTRONIC MAIL ADDRESS	FAX NUMBER
612-624-5599	**awards@umn.edu**	**612-624-4843**

* EAGER - EArly-concept Grants for Exploratory Research
** RAPID - Grants for Rapid Response Research

TC:Small:Building an Infrastructure for Computer Security History: Phase One—Mainframes to the Advent of the World Wide Web, 1965-early 1990s

For two decades computer security has received widespread attention in the media—from reports on internet worms, Trojan horses, and identity theft to assessments of pending threats of cyber-terrorism and a future of cyber-warfare. During this time, computer security has become central in computer science, a critical segment of the software industry, and a key focus for national security. As alarming headlines proliferate and a patchwork of band-aids are applied to fundamentally insecure networks that control critical systems (from energy grids to air traffic control), we still know very little about how computer security emerged and developed. Despite its unquestioned importance, minimal scholarship has been conducted (besides cryptography) and few resources have been collected. A significant barrier for understanding computer security is that available documentation is sparse—data that can aid in learning from the past and grasping optimal designs, techniques, protocols, and practices to more effectively address current and future security threats and challenges.

Intellectual Merit: This project, phase one of a two-phase CBI research agenda, proposes to [a] conduct 30 research-grade oral histories with computer security pioneers covering the core areas of the field: government, academia, industry, and criminal justice. Many of the earliest pioneers in computer security are now advanced in their careers and if data and documentation is not collected and preserved now, the opportunity will be forever lost. The project team will [b] produce a knowledge networking wiki to gather further data and provide an additional reference resource. Finally, the team will [c] identify, collect, and provide a permanent public home for archival resources, and [d] publish a series of peer-reviewed articles. Collectively these four components will create a much-needed research infrastructure for computer security history. All of the project components will benefit from the advisory committee of computer security experts that CBI has assembled (see "Project Description" pages 11 and 12).

Broader Impacts: This project is designed to make fundamental contributions to multiple core areas. While we will publish findings to advance knowledge in computer security, the central focus of our project is the creation of a major, permanent research infrastructure for computer security (publicly available oral history transcripts, new archival collections, and a computer security wiki—modeled after the IEEE Global History Network) that will benefit computer security professionals, policymakers, scholars, students, and the broader society. With regard to training, we will carefully mentor a GSRA in the craft of conducting research-grade oral histories in science and technology. Having published on challenges and policy alternatives to advance underrepresented groups in computing (particularly women), the project team will be particularly attuned to documenting and analyzing the role of underrepresented groups in computer security, and disseminating narratives of role models to inspire future scientists.

Key Words: computer security; history of computing; Bell-LaPadula model; Trusted Computer System Evaluation Criteria; Multics; Unix; International Information Integrity Institute (I4)

TABLE OF CONTENTS

For font size and page formatting specifications, see GPG section II.B.2.

*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.

TC:Small:Building an Infrastructure for Computer Security History:
Phase One—Mainframes to the Advent of the World Wide Web, 1965-early 1990s

In May 2009 the White House issued *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, a top-level review by cyber-security experts with input from industry, academia, the civil liberties and privacy communities, international partners, and the Legislative and Executive Branches. This report, framed by President Barack Obama's speech on the topic on May 29, 2009, created a new cyber-security coordinator reporting to the National Security Advisor and collaborating with the administration's top economic advisors. In December 2009 Howard A. Schmidt was named to this post. Schmidt had advised the Bush Administration and prior to that was Chief Information Security Officer at Microsoft—co-founding its Trustworthy Computing Security Strategies Group.

The concluding appendix of *Cyberspace Policy Review* contains a timeline diagram entitled "History Informs Our Future" (C-13) that juxtaposes technology milestones with selected privacy and security laws. This chart seemingly pairs the PC modem in 1977 and the Foreign Intelligence Surveillance Act of 1978, for example, but does not explain how these and other events might connect. Much as computer security has often been an afterthought in the design and construction of computing systems and networks, the history of computer security typically has been an afterthought of completed policy evaluations and recommendations. Brief lists of milestones are ineffective surrogates for historical analysis and assessment of evolving technologies, system design decisions, and security laws, policies, and practices. A thorough appraisal of the scientific, technical, and institutional history of computer security is urgently needed.

This project affirms that history should, in fact, inform our future, that it is vital to understanding today's problems and challenges, and that a narrow window exists to collect resources to understand the emergence of computer security. Many in the first generation of computer security pioneers—scientists with the insight to see the vulnerabilities to security and privacy resulting from the advent and growth of time-sharing and computer networking, and the ingenuity to develop technologies, processes, and procedures to try to mitigate risk—are now advanced in their careers. If their knowledge, memories, insights, and documents are not collected, preserved, and made available to the research community, an opportunity may be forever lost to understand the emergence of computer security and trustworthy computing, and the salient educational and policy lessons it can provide.

As such, our research is divided into two phases, with this proposal outlining the **first phase** (1965 to early 1990s): computer security in the time-sharing and networked mainframe and mini-computing era. This includes challenges posed to computer security with the widespread use of time-sharing systems in government, corporations, and universities, as well as the increasing use of the ARPANET, regional networks, and later the Internet, by the defense, university, and other

communities. We plan to conduct a **second phase** project that will directly build upon data and findings from the first phase (and hence only be possible after completion of phase one). It will focus on computer security in the age of ubiquitous networked computing of the Web era (early 1990s-2010)—from the near universal use of the Web for communication, work, commerce, entertainment, and leisure to the impending shift from IPv4 to IPv6. The phase one project will focus on computer security in the U.S., which led early computer security efforts, while phase two must be more international in scope.

In short, our research will analyze how work in the field of computer security has sought to meet the growing threats to trustworthy operation of computers in the mainframe, minicomputer, and early networked age. It will investigate not only the technical side of the field—the theories, models, methods, and tools and how they changed over time—but also evolving priorities, strategies, politics, economics, and values associated with security, reliability, privacy, and usability. The project will further understanding and knowledge of computer security and trustworthy computing, and more broadly, create an infrastructure of data for research on these topics by others.

The primary components of our project (to build a publicly accessible infrastructure for understanding the emergence of computer security) are a **major oral history initiative** and a **knowledge networking wiki**. The Charles Babbage Institute (CBI), the foremost archival repository and research center on computer history worldwide, has long been among the international leaders in research-grade oral histories for science and technology. We have also effectively used wikis (on multiple projects) to advance historical research and understanding. The project team will **collect archival resources** (such as unpublished reports, correspondence, and grey literature). Finally, the team will analyze this data and **publish peer-reviewed scholarship** on the emergence of computer security and trustworthy computing.

In addition to original research, this project will create a major, permanent infrastructure of resources/data for computer scientists and engineers, policy-makers, historians, and others to study computer security and trustworthy computing—greatly augmenting future opportunities to learn from the past.

Overview: The Need to Document Computer Security

Computer security is fundamentally concerned with safeguarding information on, and control of, computers and computer networks—protecting against unauthorized individuals or groups accessing, misusing, disabling, or destroying computer systems. In the early post-World War II era of digital mainframe computers, computer security was focused primarily on the physical security of computing machinery at government laboratories, major corporations, and other organizations. Computer security used guards, locks, surveillance cameras, and identification procedures—largely the same tools used to protect and secure other environments. Redundancy of data was also fundamental to security protocols to prevent loss from enemy attack, accidents,

or natural disasters (floods, fires, tornados, earthquakes). Notions of computer security began to broaden significantly in the 1960s when computer networking (e.g. SAGE) opened up entirely new risks resulting from unauthorized access to and interception of data, and new methods of introducing malicious software. The growing use of time-shared systems by the mid-1960s and the spread of the ARPANET in the 1970s only heightened the potential threats.

Visionary scientists, such as RAND computer scientist Willis Ware, led the earliest attempts to analyze computer security. Much of this work was dedicated to understanding the depth of the problem in operating time-shared computer systems in secure environments (largely in the military) where individuals had different security clearance levels. Much of the early research was funded by the Department of Defense (DOD), which was dependent on secure computer systems. Computer security research was also funded and/or conducted by the National Security Agency (NSA), and National Bureau of Standards (NBS)/National Institute of Standards and Technology (NIST), as well as by corporations and universities.

Forward-looking firms in the rapidly growing time-sharing industry recognized the importance of security and privacy measures for their systems. For example, Allen-Babcock Computing, Inc. developed Remote Users of Shared Hardware (RUSH) to provide otherwise-missing security options for early distributions of IBM's OS/360. Security measures of the RUSH monitor included a "login" statement with three levels of protection; longer keys for write as compared with read-only capabilities; and ensuring that users in Remote Job Entry mode could not read files other than their own (Babcock 1967). The firm's emphasis on their security measures at the 1967 Spring Joint Computer Conference, and the near absence of reports, articles, and papers on the topic by others, suggests that ABC's RUSH was atypical. Most time-sharing firms serving the scientific and business markets were yet to fully implement security features. By the early 1970s, strong privacy and access controls were becoming increasingly common for time-sharing firms, particularly those with DoD contracts (Hoffman 1971).

Computer consultant James Anderson (1972) led a panel commissioned by Air Force Major Roger Schell to create a comprehensive research and development plan for multi-user computer systems dealing with various levels of classified and unclassified information through terminals in both secure and insecure environments. Anderson's 130-page report defined the problem and proposed creation of a "security kernel" (in essence a small, secure operating system with both software and hardware components), to isolate security functions and avert the need for security throughout the entire operating system. In effect, the plan dictated that all security functions pass through the kernel.

In 1976, nonprofit research corporation MITRE's David Elliott Bell and Leonard J. LaPadula, under contract from the Air Force's Electronic Data Systems Division, completed a report building upon the secure kernel concept and Air Force work funded at Case Western Reserve University in the early 1970s to establish an approach based on mathematical modeling of computer security. This work soon became known as the Bell-LaPadula Model.

This model was a fundamental basis for establishing Department of Defense standards (also used in other areas of government and industry) in the DoD's "Trusted Computer System Evaluation Criteria" (TCSEC), issued by the National Security Agency's National Computer Security Center in 1983 and updated in 1985. This publication was so influential it was soon commonly referred to simply as the "Orange Book." Subsequent specialized computer security books, each with a different color cover, collectively became known as the "Rainbow Series." The Orange Book (and Rainbow Series) was the most fundamental tool to designate levels of computer security controls. For roughly a decade, the Orange Book was the standard in the classified community, prior to the adoption in the 1990s of international standards, referred to as the Common Criteria (which contained elements of both North American and European standards).

Concurrent with the research and development of computer security by the DoD and its contractors, research on computer security was also conducted at a number of leading universities. Multics at MIT was the earliest and most significant computer-security project conducted in an academic setting. In the mid-1960s computer scientists at Project MAC (an ARPA-funded research center), along with General Electric and Bell Labs, developed Multics, an influential time-sharing system that extended MIT's pioneering Compatible Time-Sharing System (CTSS). Notably, to combat CTSS's problems with accidental overwriting, "Multics was designed from the start for security" (Karger and Schell 2002). Security features were built into both hardware and software, most notably since PL/I (the language Multics was written in) featured automatic string truncation that intrinsically limited buffer overflow errors. In the late 1960s the Air Force contracted with Honeywell to replicate the paper-based DoD classified access structure for electronic documents using Multics. While Roger Schell led a team that demonstrated significant vulnerabilities of Multics as part of a security evaluation and enhancement project in the early 1970s, Multics was both a time-sharing breakthrough and major computer security achievement. Indeed, a 30-year retrospective indicated that "**lessons learned** from the vulnerability assessment are **highly applicable today** as governments and industry strive (unsuccessfully) to 'secure' today's weaker operating systems through add-ons, 'hardening', and intrusion detection schemes" (Karger and Schell 2002). Multics was the primary example for TCSEC's stringent B2 category. It also had lasting influence through UNIX, a descendent operating system developed by researchers at Bell Labs.

Our project team will carefully study the security models and practices of Multics and UNIX, along with important work done in the 1970s and 1980s at University of California-Berkeley, Carnegie Mellon University, University of Michigan, and other universities.[1] We will also analyze the emergence of key computer security products of the 1970s and 1980s such IBM's RACF (Resource Access Control Facility), SKK's ACF2 (Access Control Facility), and CGA's Top Secret product—security monitors with access control and auditing functions.

[1] Relevant existing CBI oral histories include R. M. Fano, F. J. Corbató, J. B. Dennis, Michael Dertouzos, Edward Feigenbaum, B. A. Galler, Richard Crandall, R. Adrion, J. F. Traub, and Allen Newell.

Despite historical outlines by sociologist Donald MacKenzie (1997, 1999, 2001) and historian (co-PI) Jeffrey Yost (2007), much remains to be learned of the technical, scientific, political, economic, and social elements of these and other computer security standards (such as the Data Encryption Standard), how they were implemented by institutions and the computer industry, what institutional structures, policies, and practices facilitated this work, and many other topics in the history of computer security and trustworthy computing.

Research Questions

Here are some detailed research questions that will help guide our work:

- What research results were achieved by K.G. Walter and colleagues at Case Western in the early 1970s and how, specifically, did this work influence Bell and LaPadula?
- What changing roles did National Security Agency (NSA), NBS/NIST, and DoD have in evolving computer security standards? How has computer security developed in different settings, and to what extent have the military models (Bell-LaPadula and TCSEC) influenced those in civilian government, industries, healthcare, and education?
- What aspects were addressed by security models subsequent to Bell-LaPadula, such as the Biba, Clark-Wilson, and Brewer-Nash integrity models and their implementations?
- To what extent did "common standards" gain wide usage, and to what extent did institutions, companies, and agencies seek individual or "appropriate standards"?
- What has been the impact of notable "security entrepreneurs" such as Willis Ware, Bernard Peters, Stephen Walker, and others? How did they gain and maintain credibility in the field, and how might their examples offer pertinent lessons for today?
- How has computer crime changed over time, and what lessons might this have for prevention/reduction of computer crime in the future?
- How did computer firms (IBM, DEC, GE, Honeywell and others) manage issues of security, efficiency, usability, and convenience in designing and building hardware, operating systems, and applications? How did the computer/software security industry emerge and change over time?
- What was the nature of cooperative organizations such as International Information Integrity Institute (I4)? How did security efforts outside the government relate to the National Computer Security Center? What lessons can be learned from these efforts and how they were coordinated and conducted across organizational boundaries?
- What discussions/debates took place and how was security perceived and acted upon (or not) in the development of company-specific proprietary computer networks as well as ARPANET, MILNET, CSNET, BITNET, regional networks, and NSFNET?
- What was the political economy of the Data Encryption Standard (1976-2002) and what are the weights of the various factors that played into this evolving standard?

These are some of the **core questions** that we expect our ongoing research to shed light upon. This research will advance understanding of the emergence of computer security far beyond existing studies, as the following literature review makes clear.

Literature Review

Surprisingly little historical research on computer security has been published to date. Ciphers and codebreaking are the only topics that have received extensive attention. This includes David Kahn's landmark *Codebreakers* (1967), and more recent studies focused on cryptography and cryptanalysis during World War II—detailing work at Bletchley Park and the breaking of the Enigma code—Copeland (2005, 2006, 2007), Hodges (2000), and Hinsley and Stripp (1993). Snyder (1980) provides a useful short survey of contributions of cryptologic organizations (primarily the NSA) to early computer technology. There have also been a number of popular books on ciphers and encryption, such as Singh (1999), West (1999), and Levy (2001). The NSA's Center for Cryptologic History sponsors a biennial historical symposium.

Some recent studies have focused on cryptography in different national settings, such as de Leeuw (2007) on the Dutch Republic, Black (2007) on Great Britain, and Bauer (2007) on Germany as well as earlier settings such as the European Renaissance (Strasser 2007).

Certain computer security specialists have included historical discussion while writing on contemporary issues. Examples include Donn Parker's path-breaking book on computer crime (1983), Bruce Schneier's influential overview of digital security (2000), and Whitfield Diffie's recounting of his work with Martin Hellman on public key encryption (Diffie 1988).

Computer scientists specializing in computer security research have used history to frame or understand contemporary opportunities and challenges (Ware 1989, 1997; Spafford 1991; Landwehr 1993; Roberts 1993; Solomon 1993; Ruthberg and Tipton 1993; Murray 1994; Highland 1997; Hruska 1998; Gligor 1999; McLean 1999; Weisschuh 2000; Hofmeyr 2003; Brassard 2005; Dent 2009; Michael, Voas, and Laplante 2009).

Science studies scholars have rarely addressed the topic of computer security except for sociologist Donald MacKenzie (1996, 1997, 2001: chapter 5). An interest in formal verification led MacKenzie to the question of proof in mathematics, the use of mathematical models to design secure computing systems, and efforts to automate the process of evaluating whether these systems conformed to the mathematical models. While insightful, MacKenzie's work traces one particular thread (formal verification). Further, as with most individual investigations, it did not generate publicly available resources for future study of computer security.

Co-PI Yost is the only historian (other than MacKenzie) to publish on the history of computer security. His survey of computer security standards (2007) includes the first scholarly treatment of the origins of the software security industry. He also published a study of medical informatics

and privacy (2004). Yost has conducted CBI oral histories with security pioneers James Bidzos, Martin Hellman, Donn Parker, and Willis Ware.

Over the past few decades computer security has become a fundamental area of research in the field of computer science. Likewise, the computer security industry has grown immense. As such, computer security should play a much larger role in the history of computer science (e.g. operating systems and networking), as well as studies of the computer and software industries. In surveys (Campbell-Kelly and Aspray, 1996; Ceruzzi 1998; Campbell-Kelly 2003; Yost 2005) computer security is, at best, briefly mentioned. (Specialist studies of software and hardware say little more.) The results of this project will put computer security in the mainstream history of computer science and computing.

The project will also contribute more broadly to the history of science and technology, adding substantively to the existing literature on science, technology, and risk management; technology and crime; standards setting; and the management of complex technological systems.

Moving beyond the historical literatures, there are considerable published and unpublished source materials. While these are of unquestioned value to understanding the emergence of computer security, they provide only a fragmented and incomplete picture, one that can be enriched and clarified through this project's oral history initiative, project wiki, collection of primary resources, and scholarly publications.

Owing to the institutional settings of early computer security research (DOD, NSA, System Development Corporation, RAND, and MITRE), many reports were not published. They circulated only within the computer security research community. Matt Bishop (a member of our project advisory committee) led a project to disseminate seminal unpublished papers. These range from key papers advancing knowledge and practice toward the development of DOD computer security standards in TCSEC to fundamental papers on public key encryption by Rivest, Shamir, and Adelman. See <csrc.nist.gov/publications/history>.

Clearly more analysis of the emergence of computer security and a permanent infrastructure for its study are needed.

Project Components

We have used oral histories, research/publications, and archival collection development successfully on multiple NSF- and DARPA-funded projects. Oral histories provide access to key individuals and often create opportunities for new documentary and archival collections with high research value. These collections, once processed and made publicly available, then add to the permanent research infrastructure. On several recent projects we have used a knowledge networking wiki—a tool that creates a public forum for presenting results and soliciting feedback from the scientific community.

1. Oral History

The Charles Babbage Institute (CBI) is among the international leaders in conducting and disseminating research-grade oral histories in the history of science and technology. When conducted and used with care, oral histories complement available written records and provide research data unavailable through any other means.

Computer security experts (scientists from academia, industry, and government) will advise project staff on the most critical individuals to interview. (This advisory committee is discussed on pages 11 and 12). The committee consists of nine leading computer security pioneers, all of whom have consented to be interviewed for this project. Additional computer security pioneers have already consented to oral histories, such as Dorothy Denning (Professor of Defense Analysis at Naval Postgraduate School, and former Director of the Georgetown Institute for Information Assurance). The interviews will cover the four fundamental settings for computer security research and application—government, academia, industry, and criminal justice. CBI's reputation as the leader in oral history in the computing field, and the support and connections of the advisory committee, will assist us in successfully interviewing the most important individuals.

We will conduct 30 carefully chosen interviews. As is CBI's standard practice, interviews will be approximately two to four hours in length. Targeted research will be done prior to each interview. The resulting transcripts will be edited for clarity and accuracy by the interviewees and project staff, with careful attention to maintaining the integrity of the original oral interview. Once final editing is complete, the oral histories will be added to the CBI oral history database. Additionally a project wiki-site will be created to provide further information on the interviews.

CBI oral histories are hailed by Mitchell Waldrop (2001: 483) as "a priceless resource for any historian of computing." The understanding of computing institutions, software innovations, and early networking depends on our oral history transcripts (Abbate 1999, Akera 2007, Aspray, Beyer 2009, Campbell-Kelly and Aspray 2004, Hafner and Lyon 1996, Lohr 2001, McCartney 1999, Misa 2010, Norberg and O'Neill 1996, Norberg 2005, Roland 2002, Yost 2005). Our oral histories are on a publicly available website <www.cbi.umn.edu/oh>. In the past two years, the number of downloads of CBI's 300-plus oral histories have increased dramatically. Recent figures record 30,000 downloads of CBI oral histories *per month*.

2. Knowledge Networking Wiki

Public interest in computer security has clearly outpaced the supply of well-written and carefully sourced reference materials on the topic. In popular press and media accounts, terminology is used, and sometimes misused, and is often not explained, or is explained poorly. Wikipedia is a reliable reference for some topics. However, its entries on many specialized topics—including computer security—are sparse, incomplete, and most often entirely ahistorical. There is a timely opportunity for experts in the domain to engage in knowledge networking to create and refine a

wiki resource on computer security. The IEEE Global History Network <ieeeghn.com> demonstrates the value of a wiki-based, specialized reference source that draws on the expertise of the scientific and engineering community.

Project staff will create a wiki site for knowledge networking on computer security. We will register all contributors to the wiki and monitor content to best assure quality and accuracy. Together with our advisory board of pioneering figures in computer security, we will "seed" the wiki with draft entries and promote it to the computer security community. We will also post key documents to solicit expert feedback and to gain context. Although some of the entries on key events, techniques, and individuals may overlap with Wikipedia entries (such as computer worm, trojan horse, RACF, TCSEC/Orange Book, etc.) we will produce a resource with far deeper and more historically informed content. Additionally, we will include a number of computer security terms, events, and individuals that do not have Wikipedia entries (such as computer security pioneer Willis Ware). Already we have formed a preliminary list of 75 key security concepts, projects, and products. We have successfully used wikis on other CBI research projects and believe that we can create the premier online reference source on the emergence of computer security. At the same time, we will promote a useful model for others to develop historically informed wikis on specialized topics in contemporary science and technology.

3. Collection Development

The Charles Babbage Institute is by far the world's leading repository of archival research materials on computing, software, and networking. For more than three decades it has engaged in collection development of carefully selected materials of high research value. Many influential works of scholarship make use of CBI print and archival collections (Abbate 1999; Akera 2007; Aspray and Ceruzzi 2008; Campbell-Kelly and Aspray 2004; Cortada 1993, 2004, 2006, 2008; Ensmenger 2010; Grier 2005; Lecuyer 2006; Misa 2010; Norberg and O'Neill 1996, Norberg 2005, Yost 2005). Every year, numerous scholars from around the world visit the Charles Babbage Institute to conduct research on-site—for weeks, months, or even entire academic years. Through our oral histories, extensive finding guides, digitized documents, and other material on our website, many other researchers use our materials remotely. In the 12 months ending July 2010, we made available to researchers 1,000 archival items including boxes of archival documents, rare books, specialized serials, photographs, and audio-visual materials, not including oral-history downloads. Overall, the Charles Babbage Institute has more than 200 archival collections (ranging in size from hundreds of cubic feet to a single cubic foot), focused on the digital computer era (1935-present). The institute, a partnership between the University of Minnesota's University Libraries and College of Science and Engineering, is physically located in a climate-controlled building for the preservation of paper records and audiovisual materials, and features a well-appointed reading room for researchers.

In the area of computer security, CBI already has three especially strong collections. The Donn B. Parker Papers represent the foremost archival collection on computer crime. The Willis H. Ware Papers focus on Ware's leadership with the Advisory Committee on Automated Personal Data (which led to the 1974 Privacy Act) and his co-leadership of the Privacy Protection Study Commission. The Ware Papers represent one of the most significant collections worldwide on the advent and growth of government and industry computer databases and related privacy concerns and evolving legislation during the 1970s. The David Cavanagh Collection on Computer Security 1974-1996 documents his activities as chief information security officer at Sun Life in Canada and an active member of the International Information Integrity Institute (I-4). Further, CBI's National Bureau of Standards Computer Literature collection, the Carl Hammer papers, and the Walter L. Anderson Papers supplement these core resources.

Major CBI research projects, especially those focused on conducting numerous oral histories, offer tremendous opportunities to advance archival collections in targeted areas. In addition to the production and public dissemination of extensive new data on the emergence of computer security with the oral history transcripts, this project will yield extensive additions of new collections on computer security. These materials and collections will be promptly processed and made publicly available to researchers.

4. Scholarship

The PI, Co-PI, and GSRA will collaborate on analyzing existing and collected archival material and the data from the oral histories, to publish a series of peer-reviewed articles on different aspects of computer security. CBI has successfully conducted major research projects on the history of computer networking and the history of software, publishing scholarship, advancing knowledge, and building a research infrastructure in these areas. The scholarship for the computer security project will be a response to opportunities generated by the new archival materials, oral-history interview data, and advice from our committee. We will be guided in this work by a set of **core research questions** (listed on page 5).

The project team will be particularly attentive to underrepresented groups' participation and perspectives on computer security. We will be proactive in identifying women and minority pioneers as oral history interview candidates, as well as for participation with the wiki. We will also examine underrepresented groups in our collection development and with our analysis and publications. In doing so, we will disseminate narratives of role models to inspire future computer security scientists.

Project Personnel

PI Misa is director of the Charles Babbage Institute, ERA Land Grant Chair in the History of Technology, and Professor of Electrical and Computer Engineering. He teaches in the graduate program in the History of Science, Technology, and Medicine at the University of Minnesota. He is one of the international leaders in the history of technology and a specialist in the history of

computing. Misa is author of *Leonardo to the Internet: Technology and Culture from the Renaissance to the Present* (2004, 2011 2nd edition) and editor of *Gender Codes: Why Women Are Leaving Computing* (2010). He is PI of NSF-sponsored "HCC: History of FastLane: Lessons for Cyberinfrastructure."

Co-PI Yost is associate director of the Charles Babbage Institute and on the graduate faculty of the program in the History of Science, Technology, and Medicine at the University of Minnesota. He has published three books and more than a dozen peer-reviewed articles and book chapters on computer, software, and networking history—including several on the history of computer security and privacy (Yost 2004, 2007) as well as completed oral histories with four security pioneers (Bidzos, Hellman, Parker, and Ware). He is the Editor-in-Chief of the leading publication in the history of information technology*, IEEE Annals of the History of Computing*. He successfully led the NSF-sponsored "KDI: Building a Future for Software History"—a project that substantially enhanced the infrastructure for research on software history by developing online and archival resources.

A GSRA will be trained in oral history methodology by PI Misa and Co-PI Yost, both of whom have substantial experience conducting oral histories. The GSRA will be mentored by Misa and Yost and will present papers at conferences and publish from the research of this project.

Advisory Committee

A team of experts have all formally agreed in writing to serve on our advisory committee. They bring incredible experience and connections in all the major settings for computer security research, implementation, and policymaking—academia, industry, military (US Army, US Air Force), government (NSA, NBS/NIST, Los Alamos), nonprofits (SRI), and criminal justice. All committee members have also agreed to be interviewed and to help identify and provide introductions to the most critical individuals to interview (outside the committee).

Robert Abbott (Principal Investigator of the RISOS Project [Research In Secured Operating Systems] 1971-1976. This was a pioneering ARPA-funded research project addressing computer security).

Rebecca Bace (Vice President Security Practice, In-Q-Tel, Inc.; formerly President and CEO of Infidel, Inc. She previously worked at NSA and Los Alamos National Lab and is one of the world experts on intrusion detection).

Dr. Matt Bishop (University of California-Davis. He led the project to disseminate pioneering unpublished computer security papers <csrc.nist.gov/publications/history>. Published influential textbooks *Computer Security: Art and Science* and *Introduction to Computer Security*.)

Bob Johnston (Consultant. Was U.S. Army Retired Chief Warrant Officer with more than 35 years in information security. Columnist "For the Sake of Security" in *Computer Decisions* in 1980s).

Dr. Stuart Katzke (Currently a Senior Research Scientist at NIST. In January 2000 joined NSA as Chief Scientist of the Information Assurance Solutions Group. Previously he was Chief of the Computer Security Division in the Information Technology Laboratory at NIST. He initiated and participated in the Common Criteria Project).

William Murray (Naval Postgraduate School. He did pioneering computer security work at IBM and other organizations, and is a recognized international leader on computer security).

Dr. Andrew Odlyzko (University of Minnesota. In addition to his original research on cryptosystems, he has expertise on the economics of computer security and privacy)**.**

Donn Parker (Retired, SRI—One of the foremost experts on computer crime and a founder of International Information Integrity Institute. He has published six books and led many projects on computer crime research for NSF and the U.S. Department of Justice).

Dr. Gene Spafford (Purdue University. He is a pioneer in computer security and one of the internationally recognized leaders in computer science).

Project Management

All the work for the project will be done at the Charles Babbage Institute, aside from travel to conduct oral histories and collection development, and the broader computer security community's participation with the wiki. The PI, co-PI, and GSRA will meet every two weeks to discuss overall progress on the project, the ongoing work with the wiki, collection development, and opportunities for analysis, presentations, and publications. In year one, the PI and co-PI will work closely to educate GSRA on methods and best practices in oral histories. PI Misa is an expert in oral history education, having served as an instructor for a European Science Foundation-sponsored oral history summer school in 2009. Co-PI Yost has conducted dozens of oral histories (including four with security pioneers) and is also a recognized expert in this area. The PI and co-PI will conduct roughly 80 percent of the oral histories (and even more in the first year while the GSRA gains expertise with pre-interview research, interview techniques, and post-interview processes). The GSRA will conduct about 20 percent of the oral histories under supervision by the PI/co-PI.

The advisory committee for the project will consult with project staff on the individuals to interview, and suggest key topics and themes to cover. Where appropriate, committee members will help encourage the chosen computer security pioneers to participate. Informal email exchanges have generated a preliminary list of four dozen leading figures in computer security,[2] so a project result of 30 oral histories is entirely feasible.

[2] Sadly, Paul Karger, a leading expert in high assurance systems, passed away in September 2010.

Careful analysis of various computer security conferences, and computer security papers at broader computer science and engineering meetings, will also be critical to our oral histories. The earliest papers and sessions on computer security were held at leading computer science conferences to alert the community to new security risks with the advent of time-sharing, most notably Bernard Peters and Willis Ware's landmark session on computer security at the 1967 Spring Joint Computer Conference. During the 1970s a handful of computer security conferences emerged, including the annual National Computer Security Conference and Computer Security Institute, as well as well as one-time conferences on particular computer security topics. Only some of these events have published proceedings. During the 1980s and 1990s the number of annual conferences and one-time events grew rapidly, as did the presentations at more general computer science conferences, and meetings focused on software engineering, data management, infrastructure systems, and other areas. Our research on the National Computer Security Conference, its successor, the National Information Systems Security Conference, Computer Security Applications Conference, Computer Security Institute conferences, IEEE Symposium on Security and Privacy, and others, coupled with ongoing input from our expert advisory committee, will help guide our oral histories, our collection development efforts, our work on the project wiki, and our overall analysis and publication efforts.

The Charles Babbage Institute has an excellent record of success in completing interviews with top computer and software pioneers from academia, government, and industry. The advisory committee, with deep connections and leadership within all the major computer security communities (academia, government, industry and criminal justice), will only add to this. A selection of completed CBI oral histories and full-text edited transcripts is available at <www.cbi.umn.edu/oh>.

The PI and Co-PI will work closely with the GSRA to set up of the knowledge networking wiki and strategize to optimally create, structure, and populate this resource. The GSRA will then manage the wiki throughout the remainder of the project, with careful mentorship and oversight from the PI and Co-PI and strategic advice from the advisory committee.

The advisory committee has already provided extensive advice (though multiple emails and a hour-long conference call) and will continue to advise on all project components throughout the three-year project. There will be quarterly conference calls between the project staff and the entire advisory committee. In year two, the committee will meet at the Charles Babbage Institute to assess and evaluate results and to make the project as valuable as possible in furthering knowledge and resources. Committee members will help shape our project deliverables to be useful to the computer security community. The in-person meeting will also assess the wiki and develop concrete plans for achieving the broadest possible participation from the computer security community with the wiki. This will include making sure we have representatives (advisory committee members and/or project staff) at major computer security events (such as the IEEE Symposium on Security and Privacy and the annual RSA Conference).

Project Year	Oral Histories	Wiki	Presentations/Publications	Collection Development
1	First 12 oral histories conducted. GSRA to be trained and begin oral history work	GSRA will set up site and work with project staff in strategic planning for seeding and publicizing the wiki	Project staff will present on the design, early work, and expectations for the project	Evaluation and assessment of potential collections
2	12 additional oral histories will be conducted	Wiki to include ~50 entries on computer security history	Project staff will present ongoing research at leading history of science and technology conferences	Student archive worker will process collections
3	Final 6 oral histories—all oral histories completed and posted	Wiki to include ~100 entries on computer security history, and oral histories	Project staff will submit multiple articles to leading peer-reviewed history journals	Processing completed and collections become publicly accessible

Deliverables

The four major project deliverables extend directly from the four components of the project: oral histories, project wiki, collection development, and analysis/scholarship.

[1] The primary deliverable will be 30 **research-grade oral histories** with computer security pioneers from academia, industry, government, and criminal justice. The resulting full-text edited transcripts will be disseminated on the Charles Babbage Institute's searchable oral history database (publicly available) and will be a fundamental research tool for computer scientists, computer engineers, historians, social scientists, students, and others seeking a clearer understanding of past developments and what contemporary lessons can be drawn from this history. CBI, with the assistance of its advisory team of experts in computer security, is in a unique position to create this valuable infrastructural resource. Given the age of some pioneers, the opportunity to create this resource will not be possible if quick action is not taken.

[2] The second deliverable will be a computer security history **wiki**. Through knowledge networking within the computer security community, the project staff will lead an effort to produce a core reference source for understanding key developments and terminology in computer security within their historic contexts. As with the oral history component, success here depends on the participation of computer security pioneers from the 1970s and 1980s. The advisory committee will help project staff gain broad participation in the effort.

[3] The third deliverable will be an archival **collection development effort**. The Charles Babbage Institute has been the leading research institute and archives for the history of

computing for more than three decades. Past research projects at CBI have led to major collection development opportunities. For instance, our NSF-funded "Building a Future for Software History" (PI-Yost) created many frequently used oral histories, produced and disseminated scholarship, and created online reference resources, as well as led to new archival collections on software history. These included the records of the leading software and computer services trade association ADAPSO, the papers of Martin Goetz (the leader of the first software products company ADR and the first to receive a software patent), the ADR Software Division Records, the Milton Wessel papers (general counsel to both ADAPSO and American Federation of Information Processing Societies), the Robert V. Head papers (a leading IT consultant and editor whose papers provide much data on software applications in airline reservations systems, banking, government services, and other fields), the John Day papers (on computer and software networking standards), and most recently, the Carl Machover papers (on computer graphics).

[4] Finally, the PI, Co-PI, and GSRA will collaborate to **publish peer-reviewed scholarly articles** on the history of computer security in leading journals such as *Isis*, *Technology and Culture*, *History and Technology*, as well as top specialized journals on computing, including *IEEE Annals of the History of Computing* and *The Information Society*. This research will be made possible by the oral histories, knowledge networking wiki, and new archival collections.

CBI will build on its existing computer security records to extend its leadership as the top repository in the world to study the emergence of computer security. Having archival records in a single publicly available archive offers particular synergies for research. It also increases the likelihood that collections receive significant and sustained use by the research community.

Collectively these deliverables—research-grade oral histories, a knowledge networking wiki reference resource, new archival collections, and scholarly publications by the project team—will build a new future for understanding the emergence of computer security. The project will produce a lasting infrastructure for computer security history as well as publications that will be valuable to contemporary computer security specialists, security scholars, policymakers, students, and the broader public. These research materials will certainly broaden and deepen the resources that are publicly available for cybersecurity education and hence, in a modest way, help achieve one of the goals of *Cyberspace Policy Review* (2009: pp. 13-15, 37).

References Cited

Akera, A. *Calculating a Natural World: Scientists, Engineers, and Computers During the Rise of U.S. Cold War Research* (MIT Press, 1997).

Anderson, J.P. "Computer Security Technology Planning Study, Volume 1-2" (ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford MA, October 1972).*

Anderson, J.P. "Computer Security Threat Monitoring and Surveillance." (James P. Anderson Co., Fort Washington PA, April 1980).*

Aspray, W., and P.E. Ceruzzi, eds. *The Internet and American Business* (MIT Press, 2008).

Babcock, J.D. "A Brief Description of the Privacy Measures in the RUSH Time-Sharing System." *Proceedings of the Spring Joint Computer Conference* (New York: ACM, April 18-20, 1967): 301-302.

Bauer, F.L. "Rotor Machines and Bombs." In K. de Leeuw and J. Bergstra, eds. *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007), 381-446.

Bell, D.E. and L. LaPadula. "Secure Computer System: Unified Exposition and Multics Interpretation." (ESD-TR-75-306, ESD/AFSC, Hanscom AFB, Bedford MA, 1975).*

Beyer, K.W. *Grace Hopper and the Invention of the Information Age* (MIT Press, 2009).

Bidzos, James. Oral history conducted by Jeffrey R. Yost in Mills Valley, California (December 11, 2004). Charles Babbage Institute, University of Minnesota.

Bingham, H.W. "Security Techniques for EDP of Multilevel Classified Information." (RADC-TR 65-415, Rome Air Development Center, Griffiss Air Force Base, New York, December 1965). National Bureau of Standards Collection, Charles Babbage Institute, University of Minnesota.*

Bishop, Matt "Early Computer Security Papers, Part I" <csrc.nist.gov/publications/history> *[Note: this includes 16 unpublished papers; papers available from this site have a "*" following the citation.]*

Black, J. "Intelligence and the Emergence of the Information Society in Eighteenth-Century Britain." In K. de Leeuw and J. Bergstra, eds. *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007), 369-380.

Brassard, G. "Brief History of Quantum Cryptography: A Personal Perspective*." 2005 IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security* (2005): 19-23.

Campbell-Kelly, M. *From Airline Reservations to Sonic the Hedgehog: A History of the Software Industry* (MIT Press, 2003).

Campbell-Kelly, M. and W. Apray. *Computer: A History of the Information Machine* (Westview, 2004; 2nd edition).

Ceruzzi, P.E. *A History of Modern Computing* (MIT Press, 1998).

Ceruzzi, P.E. *Internet Alley: High Technology in Tysons Corner, 1945-2005* (MIT Press, 2008).

Cohen, E. S., et al. "HYDRA: The Kernel of a Multiprocessor Operating System." *Communications of the ACM* 17:6 (1974): 337-345.

Copeland, B. J. ed. *Alan Turing's Automatic Computing Engine: The Master Codebreaker's Struggle to Build the Modern Computer* (Oxford University Press, 2005).

Copeland, B. J. ed. *Colossus: The Secrets of Bletchley Park's Code Breaking Computers* (Oxford University Press, 2006).

Cortada, J.W. *Before the Computer: IBM, NCR, Burroughs, and Remington Rand and the Industry They Created, 1865-1956* (Princeton University Press, 1993).

_____. *The Digital Hand: How Computers Changed the Work of American Manufacturing, Transportation, and Retail Industries* (Oxford University Press, 2004).

_____. *The Digital Hand, Volume 2: How Computers Changed the Work of American Financial, Telecommunications, Media, and Entertainment Industries* (Oxford University Press, 2006).

_____. *The Digital Hand, Volume 3: How Computers Changed the Work of American Public Sector Industries.* (Oxford University Press, 2008).

De Leeuw, K. and J. Bergstra. eds., *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007).

_____. "Cryptology in the Dutch Republic: A Case-Study." In K. de Leeuw and J. Bergstra, eds. *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007), 327-368.

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure (2009). [published on White House Website. Accessed July 20, 2010] <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>

Denardis, L. *Protocol Politics: The Globalization of Internet Governance* (MIT Press, 2009).

Dent. A.W. “A Brief History of Security Models for Confidentiality.” *Provable Security: Proceedings Third International Conference ProvSec* (2009).

Department of Defense. “Trusted Computer System Evaluation Criteria.” [Orange Book] (DOD 5200.28-STD, Department of Defense, 1983, 1985).*

Diffie, W. “The First Ten Years of Public-Key Cryptography.” *Proceedings of the IEEE* 76:5 (May 1988): 560-577.

Diffie, W. and M. E. Hellman. “New Directions in Cryptography.” *IEEE Transactions on Information Theory* IT-22 (1976): 644-654.

Diffie, W. and S. Landau. *Privacy on the Line* (MIT Press, 1998; 2010; 2nd edition).

Doyle, R. “The US Navy’s First Online Crypto System.” *IEEE Annals of the History of Computing* 23 (2001): 17-21.

Ensmenger, N.L. *The Computer Boys Take Over: Computers, Programmers, and the Politics of Technical Expertise* (MIT Press, 2010).

Gligor, V.D. “20 Years of Operating Systems Security.” *Proceedings of the 1999 IEEE Symposium on Security and Privacy* (1999): 108-110.

Grier, D.A. *When Computers Were Human* (Princeton University Press, 2005).

Hafner, K. and M. Lyon. *Where Wizards Stay Up Late: The Origins Of The Internet* (Simon and Schuster, 1996).

Hellman, Martin. Oral history conducted by Jeffrey R. Yost in Stanford, California (November 22, 2004). Charles Babbage Institute, University of Minnesota.

Highland, H.J. “A History of Computer Viruses: Three Special Viruses.” *Computers & Security* 16:5 (1997): 430-438.

Hinsley, H. and A. Stripp. *Code Breakers: The Inside Story of Bletchley Park* (Oxford University Press, 1993).

Hodges, A. *Alan Turing: The Enigma* (Walker & Company, 2000).

Hoffman, L.J. “The Formulary Model for Flexible Privacy and Access Controls.” *Proceedings of the Fall Joint Computer Conference* (New York: ACM, November 16-18, 1971): 587-601.

Hofmeyr, S. "Why Today's Security Technologies Are So Inadequate: History, Implications, and New Approaches." *Information Systems Security* 12:1 (March-April 2003): 17-21.

Kahn, D. *The Codebreakers: The Story of Secret Writing* (Macmillan, 1967).

Karger, P.A. and R.R. Schell. "MULTICS Security Evaluation: Vulnerability Analysis." (ESD-TR-74-193 Vols. 2 ESD/AFSC, Hanscom AFB, Bedford, MA, June 1974).*

Karger, Paul A. and Roger Schell. "Thirty Years Later: Lessons from the Multics Security Evaluation." *Proceedings of the 18th Annual Computer Security Applications Conference* (2002): 119-126.

Landwehr. C.E. "How Far Can You Trust a Computer?" *SAFECOMP 1993. 12th International Conference on Computer Safety, Reliability and Security* (1993): 313-325.

Lecuyer, C. *Making Silicon Valley: Innovation and the Growth of High Tech, 1930-1970* (Cambridge: MIT Press, 2006).

Levy, S. *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age* (Viking, 2001).

Linden, T.A. "Operating System Structures to Support Security and Reliability Software." (NBS Technical Note 919, Institute for Computer Sciences and Technology, National Bureau of Standards, Department of Commerce, Washington, D.C., August 1976).*

Lohr, S. *Go To: The Story of the Math Majors, Bridge Players, Engineers, Chess Wizards, Maverick Scientists and Iconoclasts—The Programmers Who Created the Software Revolution* (Basic Books, 2001).

MacKenzie, D. "The Automation of Proof: A Historical and Sociological Exploration." *IEEE Annals of the History of Computing* 17:3 (July 1995): 7-29.

_____. *Knowing Machines: Essays on Technical Change* (MIT Press, 1996).

_____. "Slaying the Kraken: The Sociohistory of a Mathematical Proof." *Social Studies of Science* 29 (1999): 7-60.

_____. *Mechanizing Proof: Computing, Risk, and Trust* (MIT Press, 2001).

MacKenzie, D. and G. Pottinger. "Mathematics, Technology, and Trust: Formal Verification, Computer Security, and the U.S. Military." *IEEE Annals of the History of Computing* 19: 3 (1997): 41-59.

McCartney, S. *ENIAC: The Triumphs and Tragedies of the World's First Computer* (Walker, 1999).

McLean, J. "Twenty Years of Formal Methods." *Proceedings of the 1999 IEEE Symposium on Security and Privacy* (1999): 115-116.

Michael, B., J. Voas, and P. Laplante. "Cyberpandemics: History, Inevitability, Response." *IEEE Security & Privacy* 7:1 (January-February 2009): 63-67.

Misa, T. J. *Leonardo to the Internet: Technology and Culture from the Renaissance to the Present* (Johns Hopkins University Press, 2004; 2011, 2nd. edition).

Misa, T. J. ed. *Gender Codes: Why Women Are Leaving Computing* (IEEE Computer Society Press/Wiley, 2010).

Morris, R. and K. Thompson. "Password Security: A Case History." *Communications of the ACM* 22:11 (1979): 594-597.

Myers, P. "Subversion: The Neglected Aspect of Computer Security." (MA Thesis, Naval Postgraduate School, Monterey CA, 1980).

Neumann, P.G., L. Robinson, K.N. Levitt, R.S. Boyer, and A.R. Saxena. "A Provably Secure Operating System." (M79-225, Stanford Research Institute, Menlo Park CA, June 1975).*

Nibaldi, G.H. "Proposed Technical Evaluation Criteria for Trusted Computer Systems." (M79-225, MITRE Corporation, Bedford MA, October 1979).*

Norberg, A. *Computers and Commerce: A Study of Technology and Management at Eckert-Mauchly Computer Company, Engineering Research Associates, and Remington Rand, 1946-1957* (MIT Press, 2005).

Panza, M. "Francois Viete: Between Analysis and Cryptanalysis." *Studies in the History and Philosophy of Science* 37 (2006): 269-289.

Parker, D.B. *Fighting Computer Crime* (Charles Scribner & Sons, 1983).

Parker, Donn. Oral history conducted by Jeffrey R. Yost in Palo Alto, California (May 14, 2003). Charles Babbage Institute, University of Minnesota.

Parker, D.B. "The Dark Side of Computing: SRI International and the Study of Computer Crime." *IEEE Annals of the History of Computing* 29:1 (2007): 3-15.

Rivest, R., A. Shamir, and L. Adleman. "A Method for Obtaining Digital Signatures and Public Key Cryptosystems." MIT Laboratory for Computer Science Technical Memo 82 (MIT LCS TM 82).*

Roberts, D.W. “Evaluation Criteria for IT Security.” *Computer Security and Industrial Cryptography. State of the Art and Evolution. ESAT Course* (1993): 151-161.

Roland, A. *Strategic Computing: DARPA and the Quest for Machine Intelligence, 1983-1993* (MIT Press, 2002).

Ruthberg, Z.G., and H.F. Tipton. *Handbook of Information Security Management* (Auerbach, 1993).

Schell, R.R., P.J. Downey, and Gerald J. Popek. “Preliminary Notes on the Design of Secure Military Computer Systems.” (MCI-73-1, ESD/AFSC, Hanscom AFB, Bedford MA, January 1973).*

Schiller, W.L. “The Design and Specification of a Security Kernel for the PDP-11/45.” (MTR-2934, MITRE Corporation, Bedford MA, 1975).*

Schneier, B. *Secrets and Lies: Digital Security in a Networked World* (Wiley, 2000).

Singh, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography* (Anchor Books, 1999).

Singh, S. *The Code Book: How to Make It, Break It, Hack It, and Crack It.* (Delacorte Press, 2003).

Snyder, S.S. “Computer Advances Pioneered by Cryptologic Organizations.” *Annals of the History of Computing* 2 (1980): 60-70.

Solomon, A. “A Brief History of PC Viruses.” *Proceedings of COMPSEC International* (1993): 181-194.

Spafford, E.H. “Making Unix Secure.” *Proceedings of the First International Virus Bulletin Conference* (1991): 125-131.

_____. “Privacy and Security: Answering the Wrong Questions Is No Answer.” *Communications of the ACM* 52:6 (June 2009): 22-24.

Strasser, G.F. “The Rise of Cryptography in the European Renaissance.” In K. de Leeuw and J. Bergstra, eds. *The History of Information Security: A Comprehensive Handbook* (Amsterdam: Elsevier, 2007), 277-326.

Waldrop, M. *The Dream Machine: J.C.R. Licklider and the Revolution that Made Computing Personal* (Viking Penguin, 2001).

Ware, W.H. “Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security” (RAND Report R609-1, RAND Corporation, Santa Monica CA, February 1970).*

Ware. W.H. “Perspectives on Trusted Computer Systems.” *Computer Security in the Age of Information. Proceedings of the Fifth IFIP International Conference* (1989).

Ware. W.H. “New Vistas on Info-System Security.” *Information Security in Research and Business Proceedings of the IFIP TC11 13th International Conference on Information Security SEC* (1997): 177-196.

Ware, Willis. Oral history conducted by Jeffrey R. Yost in Santa Monica, California (August 11, 2003). Charles Babbage Institute, University of Minnesota.

Weisschuh, T. “IT Security: An Historical Perspective.” *Computer Fraud & Security* (September 2000): 9-11.

West, Nigel. *VENONA: The Greatest Secret of the Cold War* (HarperCollins, 1999).

Wrixon, F.B. *Codes and Ciphers* (Prentice Hall, 1992).

Yost, J. R. *A Bibliographic Guide to Resources in Scientific Computing, 1945-1975* (Greenwood Press, 2002).

_____. “Reprogramming the Hippocratic Oath: A Historical Examination of Early Medical Informatics and Privacy.” In Boyd Rayward and Mary Ellen Bowden, eds. *The History and Heritage of Scientific and Technological Information Systems* (Medford, MA: ASIS&T and CHF, 2004), 46-55.

_____. *The Computer Industry* (Greenwood Press, 2005).

_____. “Computers and the Internet: Braiding Irony, Paradox, and Possibility.” In Carroll Pursell. ed. *A Companion to American Technology* (Blackwell, 2005), 340-360.

_____. “A History of Computer Security Standards.” In K. de Leeuw and J. Bergstra, eds. *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007), 595-621.

Thomas J. Misa

Professional Preparation

Massachusetts Institute of Technology. S.B. in Applied Biology, 1981; minor in Science, Technology and Society.

University of Pennsylvania. Ph.D. in History and Sociology of Science, 1987.

Appointments

University of Minnesota (2006--). ERA Land Grant Chair in the History of Technology. Director, Charles Babbage Institute for the History of Information Technology; teaching in Program in the History of Science, Technology & Medicine; faculty appointment in Department of Electrical and Computer Engineering.

University of Twente. Guest Professor Spring 1997.

Illinois Institute of Technology (1987-2005). Assistant Professor of History, 1987-94; Associate Professor of History, 1994-2005.

Publications

5 most relevant:

Gender Codes: Why Women Are Leaving Computing. IEEE Computer Society Press/Wiley, 2010. [editor and author]

Leonardo to the Internet: Technology and Culture from the Renaissance to the Present. Baltimore: Johns Hopkins University, 2004; second edition 2011.

Modernity and Technology. Cambridge: MIT Press, 2003. [co-edited with Philip Brey and Andrew Feenberg].

IEEE Annals of the History of Computing -- guest editor of special issue on "The Future and the Past: New Thoughts on the History of Computing" 29 #4 (Oct.-Dec. 2007). Misa's contributions: editor's introduction 6-7; "Arthur Norberg, the Charles Babbage Institute, and the History of Computing" 8-15; and "Understanding 'How Computing Has Changed the World'" 52-63.

"Organizing the History of Computing: Lessons Learned at the Charles Babbage Institute," in John Impagliazzo, Timo Järvi, and Petri Paju, eds., *History of Nordic Computing 2.* Second IFIP WG 9.7 Conference, HiNC2, Turku, Finland, August 21-23, 2007. (Boston: Springer, 2009), 1-12.

5 others:

Urban Machinery: Inside Modern European Cities. MIT Press, 2008 [co-edited with Mikael Hård]

Tensions of Europe: Technology and the Making of Europe - a special issue of *History and Technology* 21 no. 1 (2005): 1-139. [coedited with Johan Schot and Ruth Oldenziel]

"Inventing Europe: Technology and the Hidden Integration of Europe." *History and Technology* 21 no. 1 (2005): 1-19. [coauthored with Johan Schot]

"Beyond Linear Models: Science, Technology, and Processes of Change." In Karl Grandin, et al. eds., *The Science–Industry Nexus: History, Policy, Implications* (Science History/Watson Publishing, 2004), pp. 257-76.

Synergistic Activities

Association for Computing Machinery. History Committee. 2008--.

IEEE History Committee. 2010--.

Society for the History of Technology. Program Committee Chair 1989. Nominating Committee Chair 1991. Long-Range Planning Committee 1994-95. Executive Council 1995-97. Dexter Prize Committee Chair 2001. T&C Editor-in-Chief Search Committee Chair 2009. Editorial Committee 2010--. Presenter, session chair and/or commentator for annual meetings 1997-2010.

"Tensions of Europe: Technology in the Making of 20th Century Europe." Executive committee; co-leader research theme on "Narratives on European Cities." 2000-5. Helped organize 220-person network of historians from 22 countries; planning, workshops, conferences, recruitment, project development, fund-raising. Publications; Schot, Misa, Oldenziel (2005); Hård & Misa (2008).

"Inventing Europe." European Science Foundation funded EUROCORE research network 2007-10. Management committee.

Collaborators and Co-Editors

Philip Brey (Twente University, the Netherlands)

Andrew Feenberg (Simon Fraser University, Canada)

Mikael Hård (Technical University - Darmstadt, Germany)

Ruth Oldenziel (Technical University - Eindhoven, Netherlands)

Johan Schot (Technical University - Eindhoven, Netherlands)

Dick van Lente (Erasmus University Rotterdam, Netherlands)

Graduate and Postdoctoral Advisors

Thomas Hughes, Judith McGaw, Robert Kohler (all University of Pennsylvania)

Thesis Advisor and Postgraduate-Scholar Sponsor

Osamu Uda (Nihon University, Japan)

Mai Sugimoto (Kyoto University, Japan)

Jeffrey R. Yost

Professional Preparation

Macalester College	History	BA	1990
Case Western Reserve University	History of Technology and Science	MA	1993
University of Minnesota, Carlson	Business Administration	MBA	2007
Case Western Reserve University	History of Technology and Science	Ph.D	1998

Appointments

Associate Director, Charles Babbage Institute for the History of Information Technology, University of Minnesota, Minneapolis, Minnesota, 1998 to present

Consulting Historian, Winthrop Group, Inc., Cambridge, Massachusetts, 1994-1997

Curatorial Researcher, Dittrick Museum of Medical Technology, Cleveland, Ohio, 1992-1995

Publications

5 most relevant:

"Internet Challenges for Non-Media Industries, Firms, and Workers: Travel Agencies, Realtors, Mortgage Brokers, Personal Computer Manufacturers, and IT Services Professionals." In William Aspray and Paul Ceruzzi, eds. *The Internet and American Business* (Cambridge: MIT Press, 2008).

"History of Computer Security Standards" In Karl de Leuuw and Jan Bergstra, eds., *History of Information Technology and Security: A Comprehensive Handbook* (Amsterdam: Elsevier, 2007), pp. 595-621.

The Computer Industry (Westport, CT: Greenwood Press, 2005).

"Computers and the Internet: Braiding Irony, Paradox, and Possibility," in Carroll Pursell, ed. *American Technology: Readings in Social and Cultural History*. (Oxford: Blackwell Publishers, 2005), pp. 340-360.

Bibliographic Guide to Resources in the History of Scientific Computing, 1945-1975 (Westport, CT: Greenwood Press, 2002).

5 others:

"Programming Enterprise: Women Entrepreneurs in Software and Computer Services." In Gender Codes: Why Women Are Leaving Computing (IEEE Computer Society Press, 2010), 229-250.

"Maximization and Marginalization: A Brief Examination of the History and Historiography of the U.S. Computer Services Industry" *Entreprises et Histoire* 40 (November 2005): 87-101.

"Reprogramming the Hippocratic Oath: A Historical Examination of Early Medical Informatics and Privacy," in W. Boyd Rayward and Mary Ellen Bowden, eds., *The History and Heritage of Scientific and Technological*

Information Systems (Chemical Heritage Foundation and ASIS&T, 2004), 46-55.

"International Business Machines." *Encyclopedia of Business History* (New York: Facts on File, 2004).

"Overcoming the Discipline Divide: Knowledge Networking and the Advancement of the History of Software," *Journal of the American Association for History and Computing* 4:1 (April 2001).

Synergistic Activities

Was PI on "Building a Future for Software History" (NSF KDI 9979981) [1999-2002] working with historians, archivists, pioneering computer scientists, and software industry leaders to create infrastructure for the scholarly study of software history. Built a number of online tools to disseminate and share knowledge, including a software history dictionary, a peer-reviewed electronic journal (*Iterations: An interdisciplinary journal of software history*), oral histories, and bibliography.

IEEE Annals of the History of Computing. Editorial Board, 2005-present. Editor in Chief, 2008-11.

Collaborators and Co-Editors

Arthur L. Norberg, University of Minnesota (emeritus)

Graduate and Postdoctoral Advisors

Carroll W. Pursell (Primary dissertation advisor), Case Western Reserve University (emeritus), Macquarie University (adjunct)

Virginia Dawson, Case Western Reserve University (adjunct)

James Edmonson, Case Western Reserve University

Susan Helper, Case Western Reserve University

Alan Rocke, Case Western Reserve University

Thesis Advisor and Postgraduate-Scholar Sponsor

Philip L. Frana, Central Arkansas University.

SUMMARY PROPOSAL BUDGET

YEAR 1

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

ORGANIZATION
University of Minnesota-Twin Cities

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Thomas J Misa

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-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Thomas J Misa - Prof. , PI**	0.00	0.00	0.00	$ **0**	$
2. **Jeffrey R Yost - Co-PI**	0.00	0.00	3.60	**24,978**	
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**2**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	3.60	**24,978**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**1**) GRADUATE STUDENTS				**22,173**	
4. (**1**) UNDERGRADUATE STUDENTS				**2,990**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**50,141**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**24,692**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**74,833**	
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)				**16,000**	
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				**1,500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**1,000**	
3. CONSULTANT SERVICES				**4,000**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**6,500**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**97,333**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 51.0000, Base: 82510)**					
TOTAL INDIRECT COSTS (F&A)				**42,080**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**139,413**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **139,413**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Thomas J Misa

ORG. REP. NAME*
Kevin mckoskey

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
University of Minnesota-Twin Cities

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Thomas J Misa

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-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Thomas J Misa - Prof. , PI**	0.00	0.00	0.00	$ **0**	$
2. **Jeffrey R Yost - Co-PI**	0.00	0.00	3.60	**25,727**	
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**2**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	3.60	**25,727**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**1**) GRADUATE STUDENTS				**22,838**	
4. (**1**) UNDERGRADUATE STUDENTS				**3,080**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**51,645**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**25,072**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**76,717**	
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)				**28,000**	
2. FOREIGN				**2,000**	
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				**1,500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**1,000**	
3. CONSULTANT SERVICES				**4,000**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**6,500**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**113,217**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 51.0000, Base: 98310)**					
TOTAL INDIRECT COSTS (F&A)				**50,138**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**163,355**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **163,355**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Thomas J Misa

ORG. REP. NAME*
Kevin mckoskey

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
University of Minnesota-Twin Cities

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR
Thomas J Misa

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-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Thomas J Misa - Prof. , PI**	0.00	0.00	0.00	$ **0**	$
2. **Jeffrey R Yost - Co-PI**	0.00	0.00	3.60	**26,499**	
3.					
4.					
5.					
6. (**0**) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**2**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	3.60	**26,499**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**1**) GRADUATE STUDENTS				**23,523**	
4. (**1**) UNDERGRADUATE STUDENTS				**3,172**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**53,194**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**25,464**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**78,658**	
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)				**7,000**	
2. FOREIGN				**2,000**	
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				**1,500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**1,000**	
3. CONSULTANT SERVICES				**4,000**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**6,500**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**94,158**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE) **MTDC (Rate: 51.0000, Base: 79164)**					
TOTAL INDIRECT COSTS (F&A)				**40,374**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**134,532**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **134,532**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME
Thomas J Misa

ORG. REP. NAME*
Kevin mckoskey

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: **University of Minnesota-Twin Cities**

PRINCIPAL INVESTIGATOR / PROJECT DIRECTOR: **Thomas J Misa**

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-months CAL	ACAD	SUMR	Funds Requested By proposer	Funds granted by NSF (if different)
1. **Thomas J Misa - Prof. , PI**	0.00	0.00	0.00	$ **0**	$
2. **Jeffrey R Yost - Co-PI**	0.00	0.00	10.80	**77,204**	
3.					
4.					
5.					
6. ( ) OTHERS (LIST INDIVIDUALLY ON BUDGET JUSTIFICATION PAGE)	0.00	0.00	0.00	**0**	
7. (**2**) TOTAL SENIOR PERSONNEL (1 - 6)	0.00	0.00	10.80	**77,204**	
B. OTHER PERSONNEL (SHOW NUMBERS IN BRACKETS)					
1. (**0**) POST DOCTORAL SCHOLARS	0.00	0.00	0.00	**0**	
2. (**0**) OTHER PROFESSIONALS (TECHNICIAN, PROGRAMMER, ETC.)	0.00	0.00	0.00	**0**	
3. (**3**) GRADUATE STUDENTS				**68,534**	
4. (**3**) UNDERGRADUATE STUDENTS				**9,242**	
5. (**0**) SECRETARIAL - CLERICAL (IF CHARGED DIRECTLY)				**0**	
6. (**0**) OTHER				**0**	
TOTAL SALARIES AND WAGES (A + B)				**154,980**	
C. FRINGE BENEFITS (IF CHARGED AS DIRECT COSTS)				**75,228**	
TOTAL SALARIES, WAGES AND FRINGE BENEFITS (A + B + C)				**230,208**	
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)				**51,000**	
2. FOREIGN				**4,000**	
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				**4,500**	
2. PUBLICATION COSTS/DOCUMENTATION/DISSEMINATION				**3,000**	
3. CONSULTANT SERVICES				**12,000**	
4. COMPUTER SERVICES				**0**	
5. SUBAWARDS				**0**	
6. OTHER				**0**	
TOTAL OTHER DIRECT COSTS				**19,500**	
H. TOTAL DIRECT COSTS (A THROUGH G)				**304,708**	
I. INDIRECT COSTS (F&A)(SPECIFY RATE AND BASE)					
TOTAL INDIRECT COSTS (F&A)				**132,592**	
J. TOTAL DIRECT AND INDIRECT COSTS (H + I)				**437,300**	
K. RESIDUAL FUNDS				**0**	
L. AMOUNT OF THIS REQUEST (J) OR (J MINUS K)				$ **437,300**	$

M. COST SHARING PROPOSED LEVEL $ **0** AGREED LEVEL IF DIFFERENT $

PI/PD NAME: **Thomas J Misa**

ORG. REP. NAME*: **Kevin mckoskey**

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

A budget of $437,300 over a period of 3 years is requested. A three percent increase to the salaries is added in years two and three. A breakdown of each budget category is given below.

Yost, Jeffrey, co-Principal Investigator

- The co-PI, Prof. J. Yost, will contribute 30% time annually to the proposal. Current FY11 fringe benefits are 33.30% of salary.

Co-PI Salary: $77,204 (total project)
Co-PI Fringe Benefits: $25,709 (total project)

To Be Named, Graduate Research Assistant

- Graduate Student: It is expected that 1 graduate student will be involved with this project for three years. This graduate research assistant will be appointed for 12 mos. at 50%. Current annual base salary for GRA for FY11 is $20.75/hr. Health benefits are for 12 mos. (12 mos. @ 50% appt = 780 academic at 16.86% of salary and 24.20% of 260 summer hrs). Tuition reimbursement in the academic year for FY11 is $15.40 per hour worked. Indirect Cost is 51% on salary portion plus the summer fringe benefits only. The graduate student will be involved with all aspects of the project.

Graduate RA Salary: $68,534 (total project)
Fringe Benefits + Tuition: $48,841

To Be Named, Undergraduate Research Assistant

- Funds are requested to support one Undergraduate Research Assistant in each year of this project. This student will be working a total of 260 hours throughout each year. Fringe for undergrad RA is paid only in the summer and is 7.34% of salary.

TRAVEL COSTS JUSTIFICATION(S)

Travel

- Substantial travel is necessary for project's field work to conduct oral history interviews. Travel (RT air + ground transport), hotel, and meals necessary for project's 30 oral histories and collection development, typically 3-4 days: estimated 30 trips each at average $1300 ($39,000) plus requested foreign travel in years 2-3 ($4,000). Additional travel requested in year 2 for nine-member Advisory Committee to meet with project staff at CBI: RT airfare plus ground, hotel, meals for eight out-of-town members at $1000 each ($8,000). Travel for project staff to attend conferences in years 2 and 3 (total $4,000). Grand totals: foreign travel ($4,000) and domestic travel ($51,000).

SUPPLIES JUSTIFICATION(S)

Supplies

- Modest funds have been requested supplies: consumable copier and printer supplies (paper, toner cartridges). Funds are also requested for 2 portable digital recorders (e.g. Sony ICD-PX820), including microphones and consumable batteries, needed for recording oral history interviews ($250).

OTHER EXPENSES JUSTIFICATION(S)

Consultant Services

- Support for transcribing of oral histories and interviews are budgeted under this project. Based on previous experience, we calculated the sum at $17/hour (temp. agency) at 4.5 hours of work per hour of tape time.

Facilities and Administrative Costs (INDIRECT COSTS):

The current F&A rate at the University of Minnesota is 51% of Modified Total Direct Costs (MTDC). This is a predetermined rate that was approved by the DHHS on March 23, 2010. MTDC here is calculated as following: Total Direct Costs (TDC) less equipment and academic year fringe benefits of graduate student salaries.

Current and Pending Support

(See GPG Section II.C.2.h 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: Thomas Misa	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: HCC: Small: Designing and Using FastLane: Distilling Lessons for Cyberinfrastructures

Source of Support: NSF

Total Award Amount: $ 444,509 Total Award Period Covered: 09/01/08 - 08/31/11

Location of Project: University of Minnesota

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: TC:Small:Building an Infrastructure for Computer Security History: Phase One -- Mainframes to the Advent of the World Wide Web, 1965-early 1990s [THIS PROPOSAL]

Source of Support: NSF

Total Award Amount: $ 437,300 Total Award Period Covered: 06/01/11 - 05/31/14

Location of Project: University of Minnesota

Person-Months Per Year Committed to the Project. Cal: 1.20 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: 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.C.2.h 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: Jeffrey Yost	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: TC:Small:Building an Infrastructure for Computer Security History: Phase One -- Mainframes to the Advent of the World Wide Web, 1965-early 1990s [THIS PROPOSAL]

Source of Support: NSF

Total Award Amount: $ 437,300 Total Award Period Covered: 06/01/11 - 05/31/14

Location of Project: University of Minnesota

Person-Months Per Year Committed to the Project. Cal: 3.60 Acad: 0.00 Sumr: 0.00

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

Project/Proposal Title: HCC: Small: Designing and Using FastLane: Distilling Lessons for Cyberinfrastructure

Source of Support: NSF

Total Award Amount: $ 444,509 Total Award Period Covered: 09/01/08 - 08/31/11

Location of Project: University of Minnesota

Person-Months Per Year Committed to the Project. Cal: 3.00 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: 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: All offices and work areas in the CBI office suite have fully up-to-date networked PCs, connected to laser printers and remote servers.

Office: CBI has a suite of offices in Andersen Library, which houses the archives and special collections of the university. We have ample office space for the entire team to work together, with offices for the PI, co-PI, and defined workspace for the GSRA.

Other: The basement of Andersen Library houses the climate-controlled archives where CBI?s own archival collections in the history of computing, as well as those of the University and other special collections are kept.

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.

The project PI, Prof. T. Misa, will contribute 10% time annually working on this project. This effort will be contributed as unpaid effort.

FACILITIES, EQUIPMENT & OTHER RESOURCES

Continuation Page:

OFFICE FACILITIES (continued):