CSTB Update
February 2011

Jon Eisenberg
Director, CSTB

CRA Leadership Summit
February 28, 2011

CSTB Charter

- Monitoring and promoting **the health of the CS, information technology, and telecommunications fields**, including attention as appropriate to issues of human resources and funding levels and program structures for research.
- Initiating **studies involving CS, IT, and telecommunications as critical resources and sources of national economic strength.**
- Responding to requests from the government, non-profit organizations, and private industry for **expert advice on CS, information technology, and telecommunications issues**; and to **requests from the government for expert advice on computer and telecommunications systems planning, utilization, and modernization**.
- **Fostering interaction** among CS, IT, and telecommunications researchers and practitioners, and with other disciplines.
- Providing a **base of expertise in the National Research Council** in the areas of CS, IT, and telecommunications

What CSTB Provides

- **Studies**—consensus advice based on objective analysis
  - generally 1-2 years duration, deliberative, ad hoc committees
  - produce reports with detailed analysis, findings, and recommendations

- **Workshops** and other convenings
  - neutral meeting ground
  - identify issues and competing perspectives
  - lay framework for further exploration and action; stimulate discussion and interactions
  - produce reports summarizing discussions

- Independent and objective advice
  - Consensus recommendations
  - Based on objective analysis
  - Free from COI, advocacy
  - Balanced perspectives & bias
  - Careful, thorough review
  - Independence from sponsors

- Authoritative analysis
  - Technology trends and futures
  - Interactions of IT, econ, soc, law, policy, +
  - NAS + NAE + IOM
  - Academia + industry, scholars+ practicioners

- Publicly disseminated
  - All reports available at cstb.org and National Academies Press

CSTB members

ROBERT F. SPROULL [NAE]
Oracle Corporation, Chair

PRITHVIRAJ BANERJEE
Hewlett-Packard Company

STEVEN M. BELLOVIN [NAE]
Columbia University

SEYMOUR E. GOODMAN
Georgia Institute of Technology

JOHN E. KELLY III
IBM

JON M. KLEINBERG [NAE]
Cornell University

ROBERT KRAUT
Carnegie Mellon University

SUSAN LANDAU
Radcliffe Institute for Advanced Study

PETER LEE
Microsoft Research

DAVID E. LIDDLE
US Venture Partners

WILLIAM H. PRESS [NAS]
University of Texas, Austin

PRABHAKAR RAGHAVAN [NAE]
Yahoo! Labs

DAVID E. SHAW
D.E. Shaw Research

ALFRED Z. SPECTOR [NAE]
Google, Inc.

JOHN A. SWAINSON
Silver Lake

PETER SZOLOVITS, MIT [IOM]

PETER J. WEINBERGER
Google, Inc.

ERNEST J. WILSON
University of Southern California

4

CSTB committees

COMMITTEE ON SUSTAINING GROWTH IN COMPUTING PERFORMANCE

SAMUEL H. FULLER, Analog Devices Inc.,*Chair*
LUIZ ANDRÉ BARROSO, Google, Inc.
ROBERT P. COLWELL, Independent Consultant
WILLIAM J. DALLY, NVIDIA Corporation and Stanford University
DAN DOBBERPUHL, P.A. Semi
PRADEEP DUBEY, Intel Corporation
MARK D. HILL, University of Wisconsin–Madison
MARK HOROWITZ, Stanford University
DAVID KIRK, NVIDIA Corporation
MONICA LAM, Stanford University
KATHRYN S. McKINLEY, University of Texas at Austin
CHARLES MOORE, Advanced Micro Devices
KATHERINE YELICK, University of California, Berkeley

COMMITTEE ON ASSESSING THE IMPACTS OF CHANGES IN THE INFORMATION TECHNOLOGY RESEARCH AND DEVELOPMENT ECOSYSTEM

ERIC BENHAMOU, Benhamou Global Ventures, *Co-Chair*
RANDY H. KATZ, University of California, Berkeley, *Co-Chair*
STEPHEN R. BARLEY, Stanford University
ANDREW B. HARGADON, University of California, Davis
MARTIN KENNEY, University of California, Davis
STEVEN KLEPPER, Carnegie Mellon University
EDWARD D. LAZOWSKA, University of Washington
LENNY MENDONCA, McKinsey & Company
DAVID C. NAGEL, Ascona Group
ARATI PRABHAKAR, U.S. Venture Partners
RAJ REDDY, Carnegie Mellon University
LUCINDA SANDERS, National Center for Women and Information Technology

COMMITTEE ON TECHNICAL AND PRIVACY DIMENSIONS OF INFORMATION FOR TERRORISM PREVENTION AND OTHER NATIONAL GOALS

WILLIAM J. PERRY, Stanford University, *Co-chair*
CHARLES M. VEST, National Academy of Engineering, *Co-chair*
W. EARL BOEBERT, Sandia National Laboratories
MICHAEL L. BRODIE, Verizon Communications
DUNCAN A. BROWN, Johns Hopkins University
FRED H. CATE, Indiana University
RUTH A. DAVID, Analytic Services, Inc.
RUTH M. DAVIS, Pymatuning Group, Inc.
WILLIAM H. DuMOUCHEL, Lincoln Technologies, Inc.
CYNTHIA DWORK, Microsoft Research
STEPHEN E. FIENBERG, Carnegie Mellon University
ROBERT J. HERMANN, Global Technology Partners, LLC
R. GIL KERLIKOWSKE, Seattle Police Department
ORIN S. KERR, George Washington University Law School
ROBERT W. LEVENSON, University of California, Berkeley
TOM M. MITCHELL, Carnegie Mellon University
TARA O'TOOLE, University of Pittsburgh Medical Center
DARYL PREGIBON, Google, Inc.
LOUISE RICHARDSON, Harvard University
BEN A. SHNEIDERMAN, University of Maryland
DANIEL J. WEITZNER, Massachusetts Institute of Technology

CSTB Portfolio Themes

- CS/IT research impacts and future directions
- Research agenda/directions in subfields of CS/IT
- Effective development and use and management of IT by government agencies
- IT and broad public policy issues
- IT and homeland/national security
- Cybersecurity and information system trustworthiness
- Internet, networking, & telecommunications

Recent CSTB Impacts

- **Explaining how information technology evolves, the role of R&D, and the role of different contributors--public and private--to that process**
  - Ecosystems
  - Tiretracks + update
- **Guiding the evolution of computer science research programs and stimulating work in emerging/key areas**
  - Computing Performance
  - Defense Software
  - Biometrics
  - Wireless
  - Health IT
  - …
- **Providing public, unclassified analysis of offensive side of cybersecurity, fostering public discussion and debate**
- **Enhancing development, use, and strategic planning for information technology in the federal government**
  - SSA, IRS, NARA, FBI, …, CMS, …
- **Providing an evaluation framework for assessing information-based government programs**
  - **Efficacy as well as privacy**

Recent Reports

- **Wireless Technology Prospects and Policy Options** describes key technology trends, their implications, and options for facilitating the introduction of enhanced and new services.

- **Public Response to Alerts and Warnings on Mobile Devices: Summary of a Workshop on Current Knowledge and Research Gaps** reviews the extensive body of knowledge about the public response to alerts and warnings and the challenges and open research questions associated with their delivery using cell phones and other new technologies.

- **Critical Code: Software Producibility for Defense** assesses the growing importance of software for national security and examines how the DOD can most effectively meet its future software needs.

- **Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options** examines governmental, economical, technical, legal, and psychological challenges involved in deterring cyber attacks.

- **Biometric Recognition: Challenges and Opportunities** presents a broad and comprehensive assessment of biometric recognition systems, articulating design and operational considerations as well as outlining a research agenda to bolster the scientific and engineering underpinnings of these systems.

- **Toward Better Usability, Security, and Privacy of Information Technology** identifies research opportunities and ways to embed usability considerations in design and development related to security and privacy, and vice versa.

- **Achieving Effective Acquisition of Information Technology in the Department of Defense** calls for the DOD to acquire information technology systems using a fundamentally different acquisition process based on iterative, incremental development practices

The Future of Computing Performance: Game Over or Next Level?
A Symposium

DRAFT AGENDA

March 22, 2011
Venable LLP Conference Center, 575 7th Street NW, Washington, DC 20004

Overview: This symposium will begin with a briefing and discussion of the recently-released National Research Council report, *The Future of Computing Performance: Game Over or Next Level?* Subsequent panel sessions will explore issues raised by the report and consider opportunities and challenges for sustaining growth in computing performance. Panels will focus on software (parallelism, programming models, and so on), hardware and power (chip multiprocessors, computer architectures, energy constraints), computer science and engineering education, and federal and industrial research efforts.

9:00 AM	-	10:15 AM	**Welcome**
			Samuel H. Fuller, Analog Devices, Inc.
			    Chair, Committee on Sustaining Growth in Computing Performance
			
			The Future of Computing Performance: Game Over or Next Level?
			Report Briefing and Discussion
			Samuel H. Fuller, Analog Devices, Inc.
			    Chair, Committee on Sustaining Growth in Computing Performance

10:15 AM	-	10:25 AM	**Break**
10:25 AM	-	11:25 AM	**Session 1 – Parallelism and Innovative Programming Models, Algorithms, and Languages** Panel moderator: *Kathryn McKinley, University of Texas, Austin*

Current and prospective activities

Current

- Ethical and societal implications of advances in militarily significant technologies that are rapidly changing and increasingly globally accessible
- Future information architectures, processes, and strategies for the Centers for Medicare and Medicaid services
- Electronic vehicle controls and unintended acceleration (with TRB)
- Electronic health records and patient safety (with IOM)
- Computing research for environmental and societal sustainability
- Computational thinking for everyone: a workshop series
- Depicting innovation in information technology

Prospective

- Public response to alerts and warnings: social media & privacy implications of using social media
- Building and sustaining the nation's cybersecurity workforce
- Broadband R&D roadmap

What else should CSTB be working on?

BACKUPS
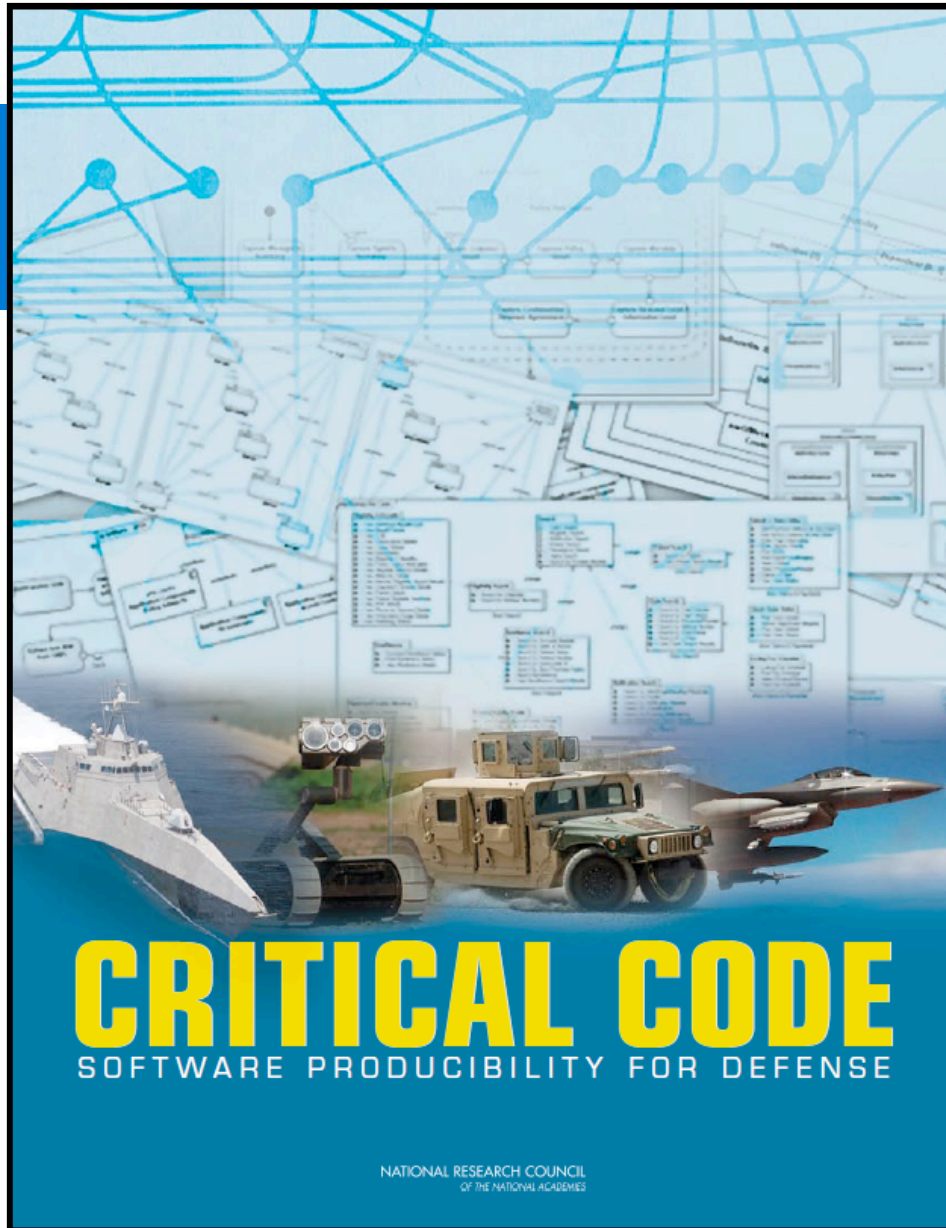
Critical Code

Software Producibility for Defense

Summary points from the final report of the
**Committee on Advancing
Software-Intensive Systems
Producibility**   (ASISP)

William Scherlis, *Chair*

Enita Williams, Study Director
Jon Eisenberg, CSTB Director

December 2010

v03

Summary of issues addressed

- Improve critical areas of current **practice**
  - Enable incremental iterative development at arm's length
    - **Process and measurement**
  - Enable architecture leadership, interlinking, flexibility
    - **Architecture**
  - Enable mission assurance at scale, with rich supply chains
    - **Assurance and security**
- Undertake **research** to support the critical areas of practice
  1. **Architecture modeling and architectural analysis**
  2. **Validation, verification, and analysis of design and code**
  3. **Process support and economic models for assurance**
  4. **Requirements**
  5. **Language, modeling, code, and tools**
  6. **Cyber-physical systems**
  7. **Human-system interaction**

One slide summary:
areas of focus

Critical Code – Software Practice and Research

1. **Software has become critical in its role and strategic significance for DoD**
   - Software enables capability, integration, and agility in defense systems
   - DoD needs to actively and directly address its software producibility needs
   - NITRD data reveal the extent of the S&T disengagement that must be reversed
2. **Innovative software-intensive engineering can be managed more effectively**
   - Apply advanced practice and supporting tools for iterative incremental development
   - Update earned value models and practices to support management process
3. **DoD needs to be a smarter software customer**
   - There is insufficient DoD-aligned software expertise within and around DoD
4. **Assert DoD architectural leadership**
   - In highly complex systems with emphasis on quality attributes, architecture decisions may need to dominate functional capability choices
5. **Adopt a strategic approach to software-intensive mission assurance**
   - Integrate preventive practices into development to support ongoing creation of evidence in support of assurance
6. **Reinvigorate and focus DoD software engineering research**
   - Apply appropriate criteria in identifying goals for research programs
   - Focus research effort on identified goals in seven technical areas

One slide summary:
recommendations

Biometric Recognition Challenges and Opportunities

- Sponsors: DHS, CIA, DARPA, NSF
- Key results:
  - Human recognition systems are inherently probabilistic, and hence inherently fallible.
  - The scientific basis of biometrics—from understanding the distributions of biometric traits within given populations to how humans interact with biometric systems—needs strengthening, especially at very large scale
  - Analyses of biometric systems' performance, effectiveness, trustworthiness, and suitability should take a broad systems perspective.
  - The field of biometrics would benefit from more rigorous and comprehensive approaches to systems development, evaluation, and interpretation

A Well-Designed Biometric System

- Takes into account that recognition is based on similarity and probabilistic not absolute matching; presumptions and burdens of proof are correspondingly conservative
- Anticipates a lifecycle corresponding to changes in presentation distributions, stability of traits, and technology
- Assesses the reliability of information associated with a recognition independently of the confidence in correct recognition
- Handles error conditions gracefully and without violating dignity, privacy or due process rights
- Publicly states explicit security, privacy and legal goals
- Recognizes that biometric traits are inherently not secret and will minimize risks to privacy and of misrecognition arising from this fact
- Provides alterative modes that are as robust as the primary biometrics process

The Difference Engine: Dubious security

Oct 1st 2010, 8:22 by N.V. | LOS ANGELES

THANKS to gangster movies, cop shows and spy thrillers, people have come to think of fingerprints and other biometric means of identifying evildoers as being completely foolproof. In reality, they are not and never have been, and few engineers who design such screening tools have ever claimed them to be so. Yet the myth has persisted among the public at large and officialdom in particular. In the process, it has led—especially since the terrorist attacks of September 11th 2001—to a great deal of public money being squandered and, worse, to the fostering of a sense of security that is largely misplaced.