Cybersecurity

Ed Lazowska
IT & Public Policy
Autumn 2004

Topics

- Status regarding "traditional" vulnerabilities
- Some "grand challenges"
- IT and counterterrorism
- Some legal and regulatory issues
- Security in open vs. closed systems
- Does it make sense to hunt for security holes?
- An economic perspective
- President's Information Technology Advisory Committee on Cybersecurity

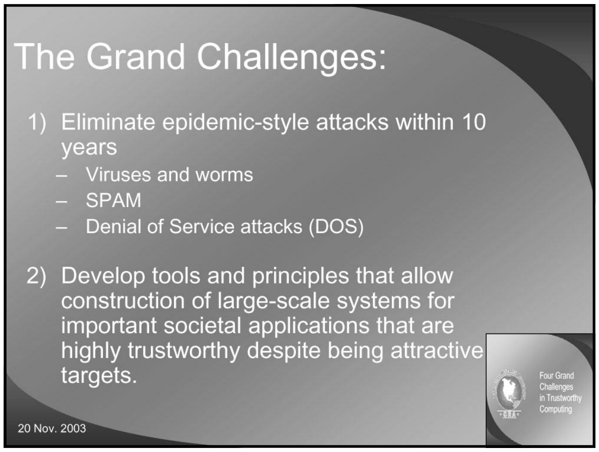
Cybersecurity Today and Tomorrow – NRC CSTB 2002

- General observations
  - Vulnerabilities are growing faster than our ability/willingness to respond
  - Achieving/maintaining security is expensive, so people "use" as little as they think they can get away with
  - Overall security is only as strong as the weakest link
  - The best is the enemy of the good
  - Constant action and reaction
  - Commercial and face-saving concerns of victims constitute a barrier to reporting

- Management
  - We are doing far worse than best practices make possible
  - We must change market incentives – for example, by becoming able to quantify security, and by shifting liability

- Operational considerations
  - To promote accountability, frequent and unannounced penetration testing ("red-teaming") is essential
  - Mis-configuration is a leading cause of vulnerabilities; configuration tools are "miserably inadequate" today
  - Organizations must have actionable fallback plans for when a cyberattack occurs

- Design and architectural considerations
  - "Human error" is usually scapegoating – the problem usually is management, or operational, or design
  - Current authentication methods are lame
  - The "defensive perimeter" approach, while not totally useless, falls way short – there must be mutual suspicion within the perimeter

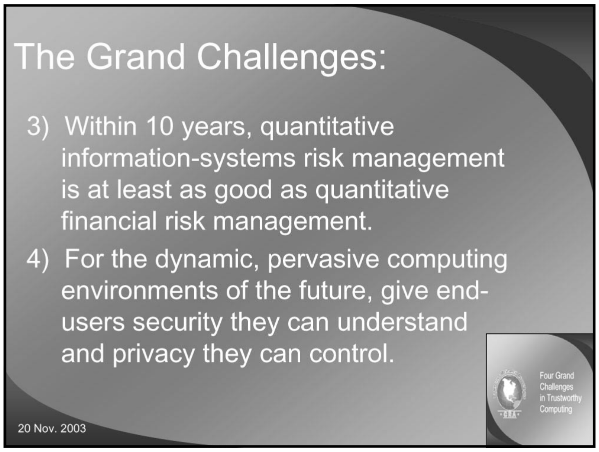


The Grand Challenges:

1) Eliminate epidemic-style attacks within 10 years
   - Viruses and worms
   - SPAM
   - Denial of Service attacks (DOS)
2) Develop tools and principles that allow construction of large-scale systems for important societal applications that are highly trustworthy despite being attractive targets.

Four Grand Challenges in Trustworthy Computing

20 Nov. 2003

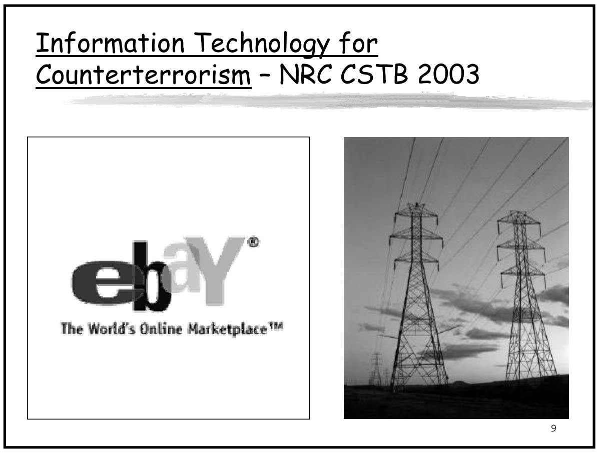


The Grand Challenges:

3) Within 10 years, quantitative information-systems risk management is at least as good as quantitative financial risk management.
4) For the dynamic, pervasive computing environments of the future, give end-users security they can understand and privacy they can control.

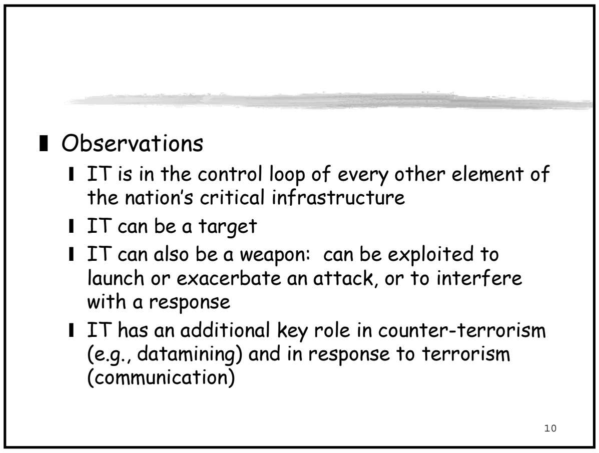
Four Grand Challenges in Trustworthy Computing

20 Nov. 2003



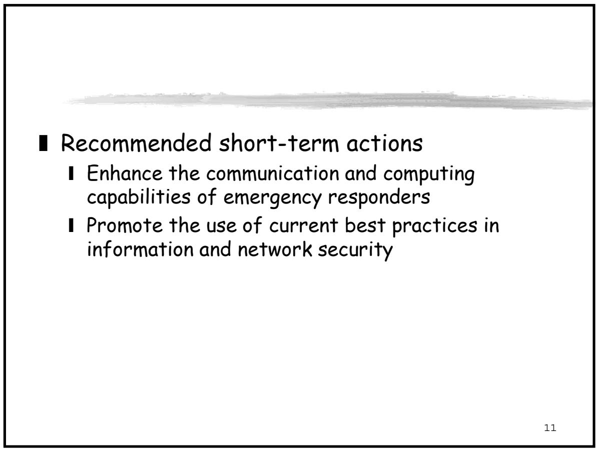
Information Technology for Counterterrorism – NRC CSTB 2003

9



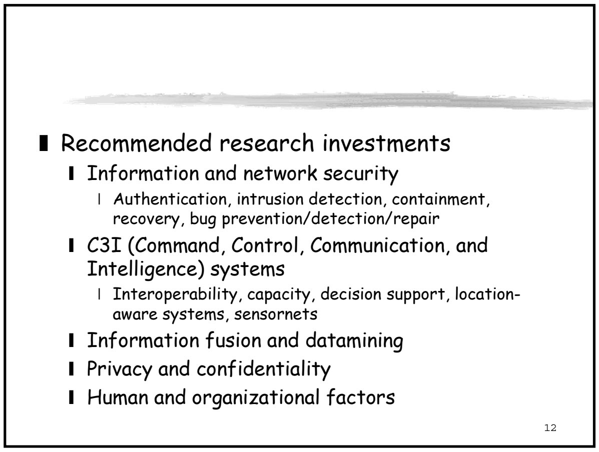
- Observations
  - IT is in the control loop of every other element of the nation's critical infrastructure
  - IT can be a target
  - IT can also be a weapon: can be exploited to launch or exacerbate an attack, or to interfere with a response
  - IT has an additional key role in counter-terrorism (e.g., datamining) and in response to terrorism (communication)

10



- Recommended short-term actions
  - Enhance the communication and computing capabilities of emergency responders
  - Promote the use of current best practices in information and network security

11



- Recommended research investments
  - Information and network security
    - Authentication, intrusion detection, containment, recovery, bug prevention/detection/repair
  - C3I (Command, Control, Communication, and Intelligence) systems
    - Interoperability, capacity, decision support, location-aware systems, sensornets
  - Information fusion and datamining
  - Privacy and confidentiality
  - Human and organizational factors

12

Critical Information Infrastructure Protection and the Law – NRC CSTB 2003

- Information sharing
  - Freedom of Information Act – companies reluctant to disclose CIIP-related information with the government
  - Antitrust law – companies reluctant to share CIIP-related information with competitors

- Liability
  - May need civil as well as criminal liability, to allow victims to recover losses from parties guilty of negligence or misconduct
  - May need tort law as well as contract law – is there a legal duty on the part of a company to secure its CII?
  - Standards, best practices, and audits: improve security, and provide a defense
  - Current patchwork of regulations must be regularized

- The big picture
  - Collective risks => collective actions
  - "The crisis management mentality in the aftermath of 9/11 has pushed aside issues of privacy and civil liberties"
  - Confused and confusing messages from government are a real problem – "a clear and consistent message from the government to the private sector will go a long way toward building the trust that is necessary to protect the nation's CII"

Security in Open vs. Closed Systems – Ross Anderson, 2002

- It cuts both ways!
  - When a researcher publishes a new abstract vulnerability, an attacker can devise a concrete attack much more easily if source is available
  - However, time-to-market for a defense may be shorter for OSS
  - But OSS makes it possible to identify new code, which is where the bug density will be highest
  - But each individual tester has preferences, so there is something to "many eyeballs" at least in terms of variation in focus

Is finding security holes a good idea? – Eric Rescorla, 2004

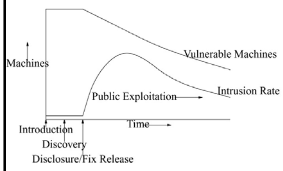


Figure 1 White Hat Discovery process when disclosure and fix release occur together

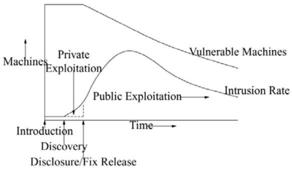
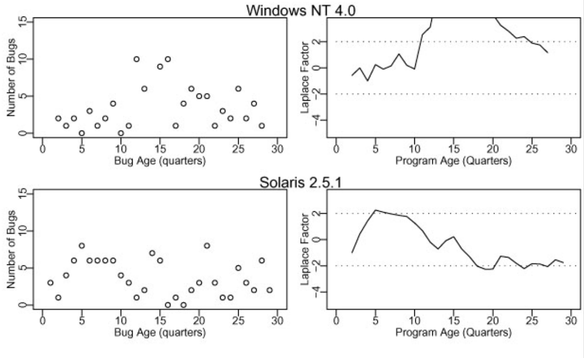


Figure 2 Black Hat Discovery Process



Eric Rescorla, "Is finding security holes a good idea?," Workshop on Economics and Information Security, May 2004

Why Information Security is Hard: An Economic Perspective – Ross Anderson, 2001

- Asymmetry of security
  - Suppose Windows has 1M bugs, each with MBTF of 1B hrs
  - Suppose Paddy works for the IRA, trying to hack the British Army's Windows systems
  - Suppose Brian is the British Army assurance guy in charge of blocking Paddy
  - Paddy has a day job – so he can only test 1000 hrs/yr
  - Brian has full Windows source code, dozens of Ph.D.s at his disposal, etc. – 10M hrs/yr of testing

- After a year, Paddy finds 1 bug, Brian patches 100K
- But the chance Brian has patched Paddy's bug is only 10%

- Assignment of liability is crucial
  - Survey of fraud against automatic teller machines
    - US: if a customer disputes a transaction, the bank must prove the customer was mistaken
    - Britain, Norway, the Netherlands: burden of proof lies with the customer
  - Clear differences in bank behavior in these two situations!

- Alignment of financial incentives also is crucial
  - Hal Varian: A consumer might pay $100 for anti-virus software to keep her system clean, but is unlikely to pay even $1 to prevent her system from being used to attack Amazon.com!

President's Information Technology Advisory Committee

Subcommittee on Cyber Security

Presentation of Draft Findings and Recommendations

F. Thomson Leighton, Chair

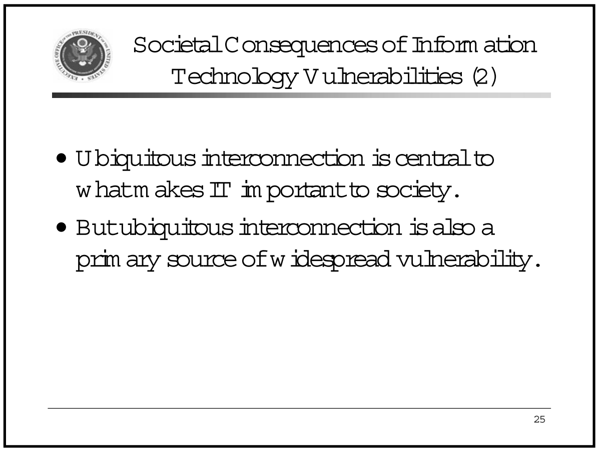
November 19, 2004

Grand Hyatt Washington at Washington Center

Washington, D.C.

Societal Consequences of Information Technology Vulnerabilities (1)

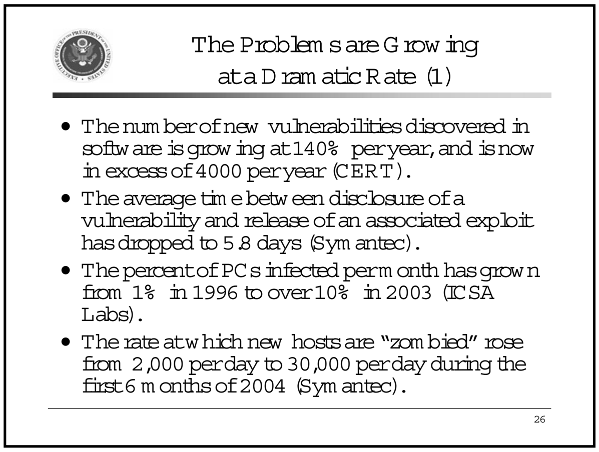
- IT is at the heart of society; IT runs critical infrastructures: electric power grid, financial systems, air traffic control, food distribution, defense networks, etc.
- The use of IT (and the faith in it) has had enormous positive impact on productivity, with tremendous remaining potential (e.g., see PITAC Health Care report).



Societal Consequences of Information Technology Vulnerabilities (2)

- Ubiquitous interconnection is central to what makes IT important to society.
- But ubiquitous interconnection is also a primary source of widespread vulnerability.

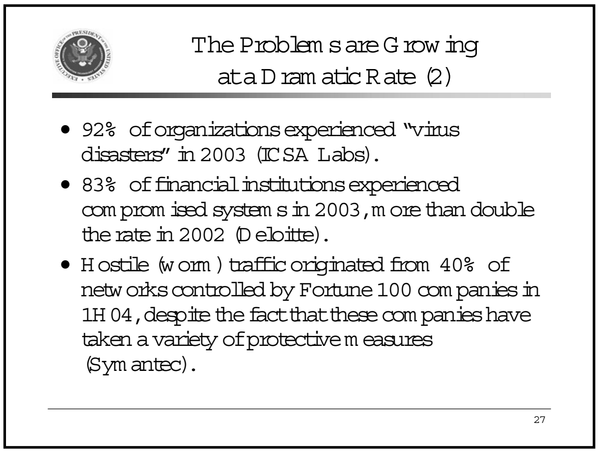
25



The Problems are Growing at a Dramatic Rate (1)

- The number of new vulnerabilities discovered in software is growing at 140% per year, and is now in excess of 4000 per year (CERT).
- The average time between disclosure of a vulnerability and release of an associated exploit has dropped to 5.8 days (Symantec).
- The percent of PCs infected per month has grown from 1% in 1996 to over 10% in 2003 (ICSA Labs).
- The rate at which new hosts are "zombied" rose from 2,000 per day to 30,000 per day during the first 6 months of 2004 (Symantec).

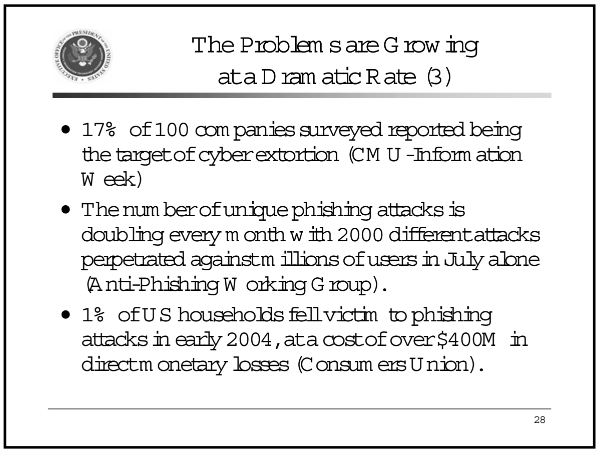
26



The Problems are Growing at a Dramatic Rate (2)

- 92% of organizations experienced "virus disasters" in 2003 (ICSA Labs).
- 83% of financial institutions experienced compromised systems in 2003, more than double the rate in 2002 (Deloitte).
- Hostile (worm) traffic originated from 40% of networks controlled by Fortune 100 companies in 1H04, despite the fact that these companies have taken a variety of protective measures (Symantec).

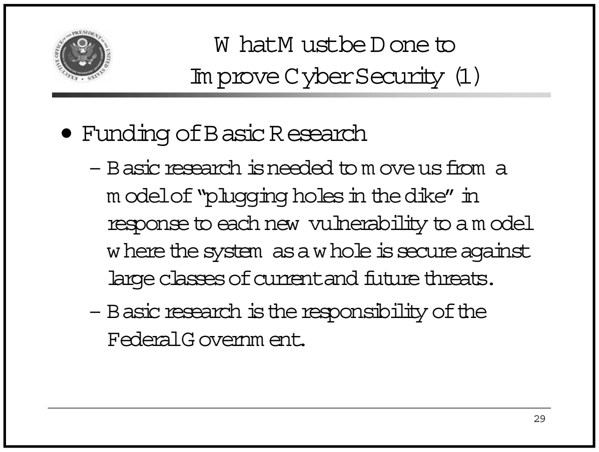
27



The Problems are Growing at a Dramatic Rate (3)

- 17% of 100 companies surveyed reported being the target of cyber extortion (CMU-Information Week)
- The number of unique phishing attacks is doubling every month with 2000 different attacks perpetrated against millions of users in July alone (Anti-Phishing Working Group).
- 1% of US households fell victim to phishing attacks in early 2004, at a cost of over $400M in direct monetary losses (Consumers Union).

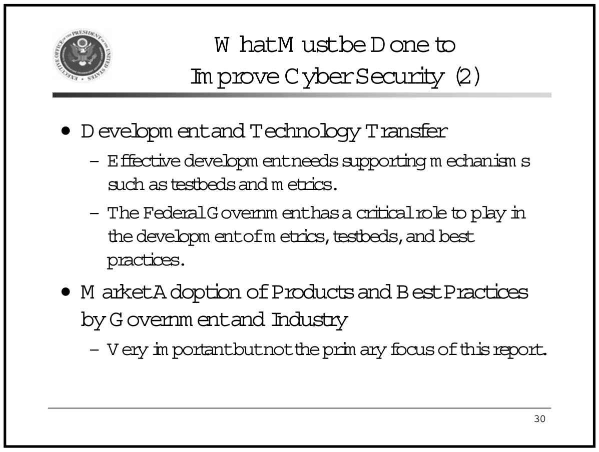
28



What Must be Done to Improve Cyber Security (1)

- Funding of Basic Research
  - Basic research is needed to move us from a model of "plugging holes in the dike" in response to each new vulnerability to a model where the system as a whole is secure against large classes of current and future threats.
  - Basic research is the responsibility of the Federal Government.

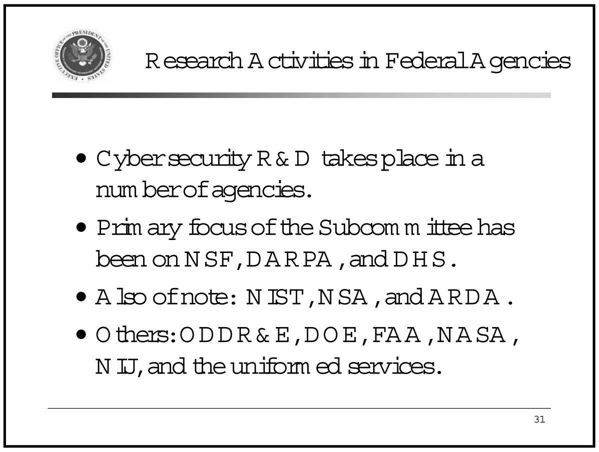
29



What Must be Done to Improve Cyber Security (2)

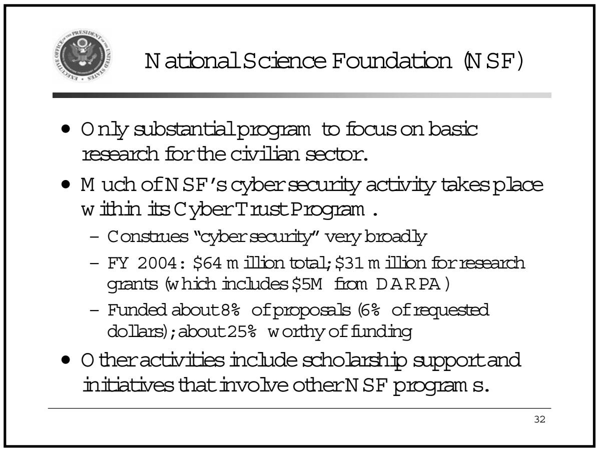
- Development and Technology Transfer
  - Effective development needs supporting mechanisms such as testbeds and metrics.
  - The Federal Government has a critical role to play in the development of metrics, testbeds, and best practices.
- Market Adoption of Products and Best Practices by Government and Industry
  - Very important but not the primary focus of this report.

30



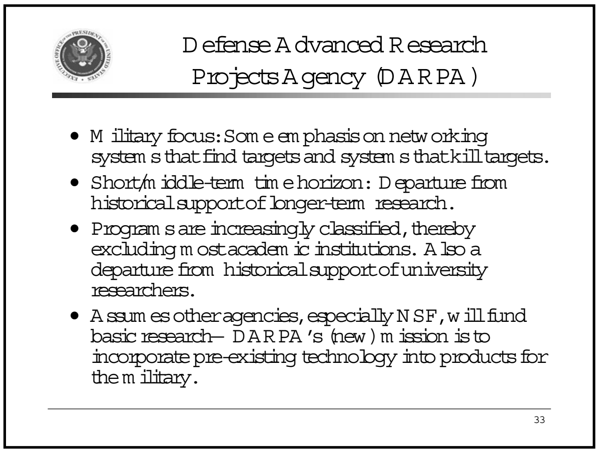
Research Activities in Federal Agencies

- Cyber security R&D takes place in a number of agencies.
- Primary focus of the Subcommittee has been on NSF, DARPA, and DHS.
- Also of note: NIST, NSA, and ARDA.
- Others: ODDR&E, DOE, FAA, NASA, NIJ, and the uniformed services.



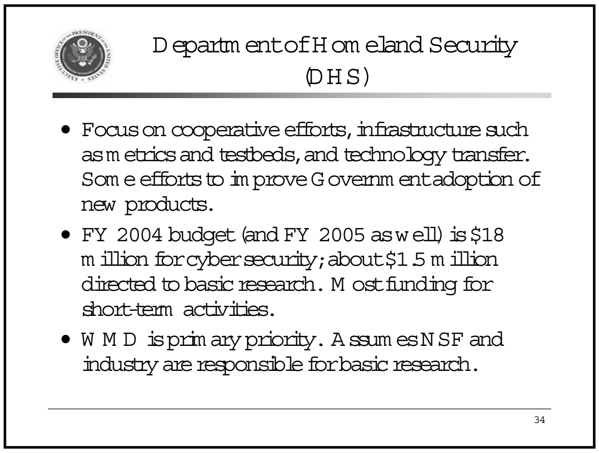
National Science Foundation (NSF)

- Only substantial program to focus on basic research for the civilian sector.
- Much of NSF's cyber security activity takes place within its Cyber Trust Program.
  - Construes "cyber security" very broadly
  - FY 2004: $64 million total; $31 million for research grants (which includes $5M from DARPA)
  - Funded about 8% of proposals (6% of requested dollars); about 25% worthy of funding
- Other activities include scholarship support and initiatives that involve other NSF programs.



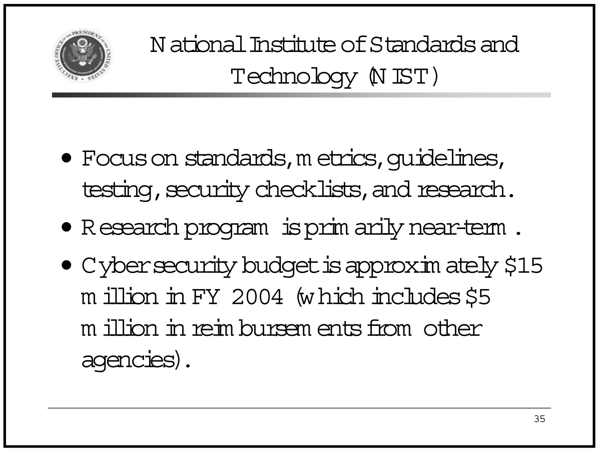
Defense Advanced Research Projects Agency (DARPA)

- Military focus: Some emphasis on networking systems that find targets and systems that kill targets.
- Short/middle-term time horizon: Departure from historical support of longer-term research.
- Programs are increasingly classified, thereby excluding most academic institutions. Also a departure from historical support of university researchers.
- Assumes other agencies, especially NSF, will fund basic research– DARPA's (new) mission is to incorporate pre-existing technology into products for the military.



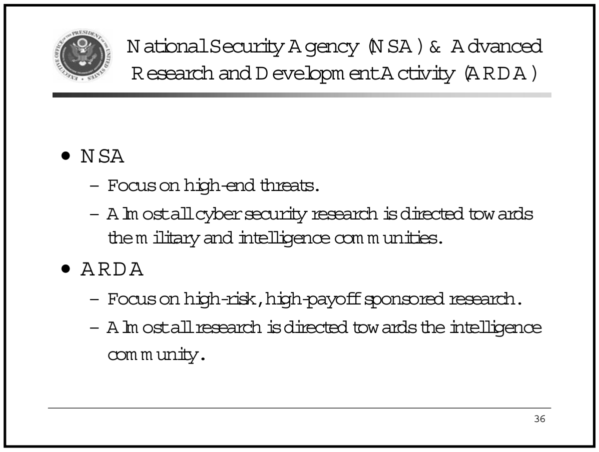
Department of Homeland Security (DHS)

- Focus on cooperative efforts, infrastructure such as metrics and testbeds, and technology transfer. Some efforts to improve Government adoption of new products.
- FY 2004 budget (and FY 2005 as well) is $18 million for cyber security; about $1.5 million directed to basic research. Most funding for short-term activities.
- WMD is primary priority. Assumes NSF and industry are responsible for basic research.



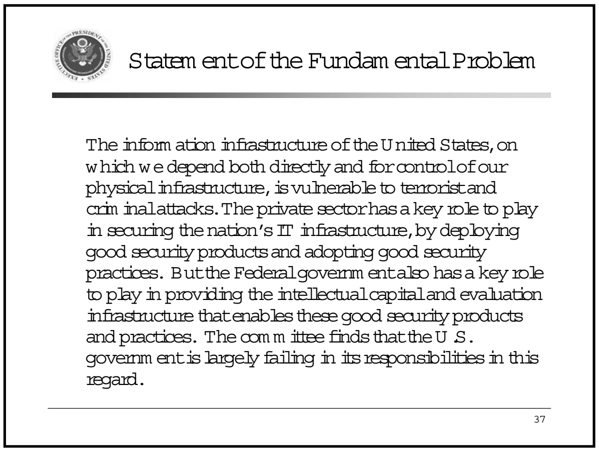
National Institute of Standards and Technology (NIST)

- Focus on standards, metrics, guidelines, testing, security checklists, and research.
- Research program is primarily near-term.
- Cyber security budget is approximately $15 million in FY 2004 (which includes $5 million in reimbursements from other agencies).



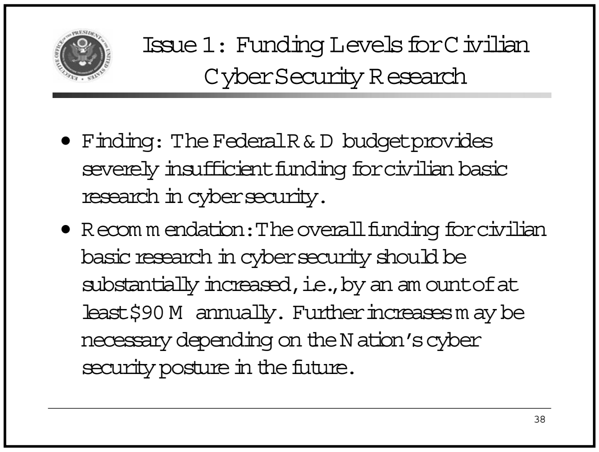
National Security Agency (NSA) & Advanced Research and Development Activity (ARDA)

- NSA
  - Focus on high-end threats.
  - Almost all cyber security research is directed towards the military and intelligence communities.
- ARDA
  - Focus on high-risk, high-payoff sponsored research.
  - Almost all research is directed towards the intelligence community.



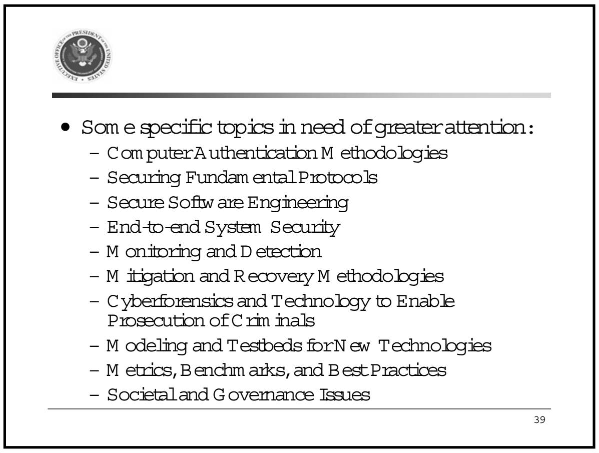
Statement of the Fundamental Problem

The information infrastructure of the United States, on which we depend both directly and for control of our physical infrastructure, is vulnerable to terrorist and criminal attacks. The private sector has a key role to play in securing the nation's IT infrastructure, by deploying good security products and adopting good security practices. But the Federal government also has a key role to play in providing the intellectual capital and evaluation infrastructure that enables these good security products and practices. The committee finds that the U.S. government is largely failing in its responsibilities in this regard.

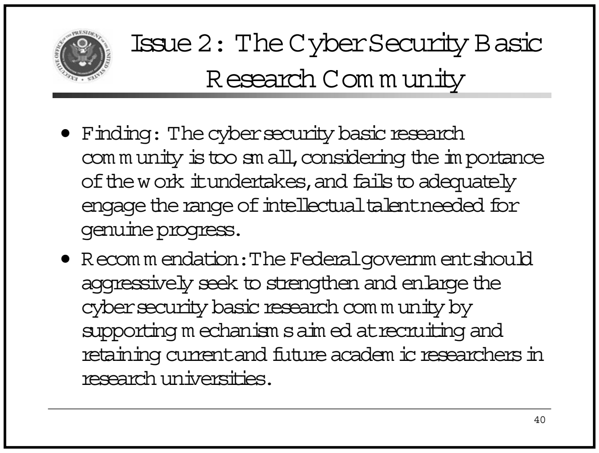


Issue 1: Funding Levels for Civilian Cyber Security Research

- Finding: The Federal R&D budget provides severely insufficient funding for civilian basic research in cyber security.
- Recommendation: The overall funding for civilian basic research in cyber security should be substantially increased, i.e., by an amount of at least $90M annually. Further increases may be necessary depending on the Nation's cyber security posture in the future.

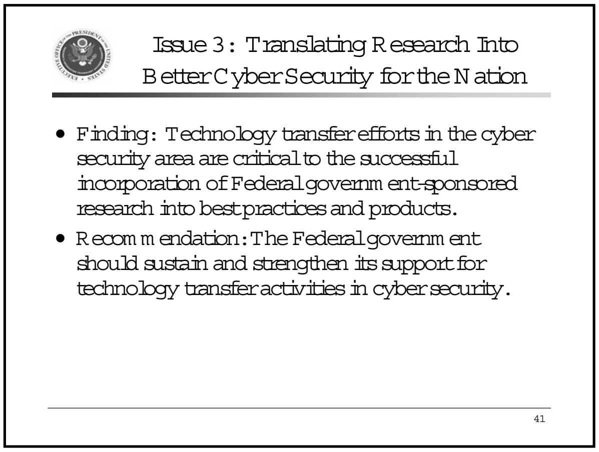


- Some specific topics in need of greater attention:
  - Computer Authentication Methodologies
  - Securing Fundamental Protocols
  - Secure Software Engineering
  - End-to-end System Security
  - Monitoring and Detection
  - Mitigation and Recovery Methodologies
  - Cyberforensics and Technology to Enable Prosecution of Criminals
  - Modeling and Testbeds for New Technologies
  - Metrics, Benchmarks, and Best Practices
  - Societal and Governance Issues



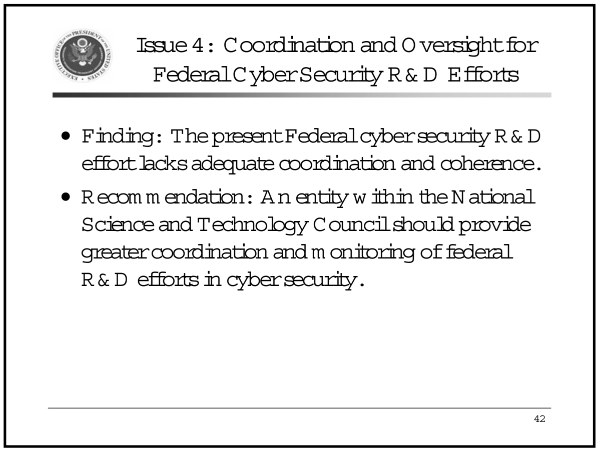
Issue 2: The Cyber Security Basic Research Community

- Finding: The cyber security basic research community is too small, considering the importance of the work it undertakes, and fails to adequately engage the range of intellectual talent needed for genuine progress.
- Recommendation: The Federal government should aggressively seek to strengthen and enlarge the cyber security basic research community by supporting mechanisms aimed at recruiting and retaining current and future academic researchers in research universities.



Issue 3: Translating Research Into Better Cyber Security for the Nation

- Finding: Technology transfer efforts in the cyber security area are critical to the successful incorporation of Federal government-sponsored research into best practices and products.
- Recommendation: The Federal government should sustain and strengthen its support for technology transfer activities in cyber security.



Issue 4: Coordination and Oversight for Federal Cyber Security R&D Efforts

- Finding: The present Federal cyber security R&D effort lacks adequate coordination and coherence.
- Recommendation: An entity within the National Science and Technology Council should provide greater coordination and monitoring of federal R&D efforts in cyber security.