Federal Funding for Cyber Security R&D

Findings and Recommendation
by the
Cyber Security Industry Alliance

July 2005

Federal Funding for Cyber Security R&D

FINDINGS AND RECOMMENDATION BY THE
CYBER SECURITY INDUSTRY ALLIANCE

JULY 2005

Federal leadership in cyber security Research & Development is lacking. The crisis in leadership in cyber security R&D will hold long term implications for the U.S. if it is not arrested soon. The President's Information Technology Advisory Committee (PITAC) report issued in February called for elevating the priority of cyber security R&D and increasing funding. Last month, the PITAC was dissolved for reasons which remain unclear. The recent lapse of the PITAC is yet another blow to the R&D community. The loss of this independent committee's expertise and advice reduces the priority level of cyber security R&D, and it will continue to dissipate without an advisory body or another leader to oversee R&D. The PITAC recommendations endure despite the Committee's lapse, and it is imperative, now more than ever, to act. We urge the new assistant secretary at the Department of Homeland Security (DHS), who is responsible for cyber and telecommunications security, to review the status of cyber security R&D efforts and prioritize requirements for action.

The Cyber Security Industry Alliance (CSIA) strongly supports the PITAC's report and the designation of top cyber security priority areas. Congressional backing via appropriations and committee hearings, combined with private-sector funding, offer for potential solutions. Leadership by the Administration will encourage proper attention to what is viewed as a much-overlooked need to secure cyberspace and maintain the global economy. Increasing cyber security R&D funding will foster a more secure, stable global information infrastructure, create a larger pool of experts in information assurance, and enable the full potential of the Internet.

This document surveys the impact of Federal R&D funding for cyber security, identifying several ways that Federal funding has improved cyber security. The report also proposes priorities for cyber security R&D over the next ten years, many of which are in the PITAC report. Finally, CSIA offers solutions and next steps, including a recommendation to develop a national "vision" for the security, reliability, and resiliency of the information infrastructure.

I. Why R&D is Important

Research and Development can each be identified by the level of the task each is trying to accomplish. "R," which tries to discover knowledge and insight about fundamental aspects of phenomena, tends to refer to "basic science," and taking it to a product idea. "D" applies those discoveries to solve specific applications, taking a product idea to prototype. Convergence can occur when creating best practices and standards. "R" is generally more long term and provides the basis for technological progress, while "D" can be short term and solutions-oriented. Both are essential for continuous improvement in technology, although current economic realities translate into industry investing more in "D" and less in "R," a trend that seems unlikely to change any time soon. Nevertheless, R&D funding is the catalyst to seed and nurture long-term explorations that can trigger vast benefits.

In the U.S.A., private industry provides about 61% of all R&D funding; Federal sources contribute about 39%. In 2005, total funding for R&D in all areas, not solely cyber security, will grow 3.6% to $312 billion. Private industry's share will be about $191 billion – up 2% but anemic for the fifth consecutive year. The Federal government will fund about $121 billion.[1]

The Federal role in science and technology R&D has been crucial for many transformative discoveries. The Internet is a famous example. It began in 1962 with the Defense Advanced Research Projects Agency's (DARPA) first head of computer research: J.C.R. Licklider. His breakthrough concept of a "Galactic Network" was similar to the Internet of today. Funding by DARPA spawned its revolutionary open infrastructure, including packet-switched networking, protocols such as TCP/IP, and network applications such as electronic mail. Other Federal investments in high speed networking such as NSFNET triggered more research innovations, which, in turn, enabled massive global scale and eventual commercialization. It was the long-term Federal role in R&D funding that enabled the Galactic Network idea.

The Internet is now a vital global infrastructure almost entirely owned and operated by the private sector. Even though these are still the "early days" of e-commerce, during 2004, total online spending in the U.S.A. by consumers grew about 26% to a record level of more than $117 billion.[2] The Internet has assumed central roles in business and education. It is important in facilitating social governance and defense. And it is rapidly changing entire industries, such as telephony, media and entertainment. The initial investments in the Internet have not only resulted in a technology revolution, but they have also produced jobs, increased productivity and provided a higher standard of living. These changes could not have happened without Federal funding for R&D of the Internet. From 1968-1973, the federal government invested $26 million in the development of ARPANET. The social and economic returns of this modest investment are incalculable.[3]

---

[1] "R&D Outlays to Rise In 2005, Driven by Military," *The Wall Street Journal*, Jan. 7, 2005; p. A2.
[2] comScore Media Metrix study, Jan. 10, 2005.
[3] Dr. Lawrence G. Roberts, *The Top Five Lessons Learned from the ARPANET Applicable to IPv6*, http://www.usipv6.com/6sense/2005/mar/02.htm (March 2005).

CURRENT FEDERAL FUNDING FOR CYBER SECURITY R&D

Cyber security has been left by the wayside in terms of Federal funding for R&D. Although most cyber security "incidents" are enabled by the Internet, the first decades of Internet R&D devoted few resources to cyber security. According to Internet pioneers, "early networks were purpose-built – i.e., they were intended for, and largely restricted to, closed communities of scholars…."[4] In those days there was no perceived need to build security into the Internet. Today, hundreds of millions of strangers worldwide use the Internet, and there has been an associated geometric rise in the number of cyber security incidents exploiting vulnerabilities in the Internet, operating systems and applications. Reported cyber security incidents rose 1,295% during a recent five-year period.[5] These incidents now cost the U.S. economy billions of dollars in direct losses, downtime, stolen identities and intellectual property, and pose risks of catastrophic system failures from weakened critical infrastructure. The need for stronger cyber security led President George W. Bush to devise a national strategy in 2003, which underscored the importance of long-term basic research about cyber security.[6]

Unfortunately, priorities established for cyber security have not yet been supported by Federal appropriations for R&D funding. For example, a January 2005 update[7] on national cyber security R&D expenditures by the President's Information Technology Advisory Committee provided this analysis:

Federal Cyber Security R&D Expenditures

Preliminary PITAC Analysis
(Based on FY 2004 data)

	Military and Intelligence	*Civilian*	*Totals*
Short Term	$136+ million	$38 million	$174 million
Long Term	$27 million	$37 million	$64 million
Totals	$163 million	$75 million	$238 million

[4] "Birth of the Internet," Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, Aug. 4, 2000.
[5] CERT Coordination Center statistics: 1999 -- 9,859 incidents; 2000 – 21,756; 2001 – 52,658; 2002 – 82,094; 2003 – 137,529. According to CERT, "An incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may involve ongoing activity for long periods of time."
[6] "*The National Strategy to Secure Cyberspace*," The White House, Feb. 2003; see pp. 34-35.
[7] Update by the Subcommittee on Cyber Security to the President's Information Technology Advisory Committee, January 12, 2005. Final report due in March 2005.

More than 83% of spending by the military and intelligence agencies is short term, or production-based. About 73% of all Federal R&D expenditures are for short-term projects; 27% are for long-term projects, or basic research. A budget breakout by sample departments and agencies reveal:

- **Department of Homeland Security**. The FY 2005 science and technology budget is $1.039 billion, which is focused on weapons of mass destruction. Less than 2% ($18 million) is for cyber security, and of that only about $1.5 million is for basic research.
- **National Science Foundation**. NSF is the primary source of money for cyber security research by the private sector through its Cyber Trust program. The FY 2005 budget is $30 million. During 2004, the NSF was able to fund 8% of grant proposals, which received an average of 6% of requested amounts; about 25% were deemed worthy of funding.
- **Defense Advanced Research Projects Agency**. The FY 2005 budget for cyber security R&D is $50 to $100 million, but almost all of that is classified.
- **Advanced Research and Development Agency**. The FY 2005 budget of $17 million for cyber security R&D focuses entirely on the intelligence community.

These organizations have requested much larger budgets for cyber security R&D. During 2002, Congress established some funding priorities in the "Cyber Security Research and Development Act,"[8] but virtually all were slashed in appropriations. The January 2005 update from the President's IT Advisory Committee advised quadrupling the Federal budget for basic cyber security research by the private sector. The need for more funding is underscored by a recent report by the National Academy of Sciences, which identified a substantial decade-long decline in basic research by the Department of Defense. That report also noted a trend during the past five years for basic research funded by the Department of Defense to reduce unfettered exploratory research and increase support for meeting more specific needs. Since the private sector already focuses on "D" instead of "R," the National Academy of Sciences urged the Federal government to shift Department of Defense funding back to its historical priority of facilitating basic research.[9]

The Computer Security Division in the National Institute of Standards and Technology (NIST) has long played a key role in the development of standards and guidelines for cyber security, but it too is lacking in adequate funds to ensure it carries out its objectives. In 2002, the Federal Information Security Management Act and the Cyber Security Research and Development Act were passed, adding new responsibilities to NIST. Some of NIST's new responsibilities for cyber security include developing minimum security requirements for all government systems and finding improved ways to meet the security product testing needs of federal agencies, consumers and producers of information technology, and running unfunded security research grants and fellowships programs. In CSIA's *Agenda for the Next Administration*, we urged the Administration and Congress to ensure that NIST's Computer Security Division receives funding commensurate with their important responsibilities, and we reiterate that request here.

---

[8] Public Law 107-305, Nov. 2002.
[9] *Assessment of Department of Defense Basic Research*, National Academy of Sciences, Dec. 2004.

Simply increasing funding for cyber security R&D will not alone stimulate better results. The lack of a clear implementation plan for the national strategy means there is very little coordination across these Federal funding streams. The strong emphasis on classified research eliminates opportunities for many research organizations. And in a self-fulfilling prophecy, the lack of available funding and long-term careers in cyber security has led to a general lack of interest by researchers in the topic.

The Cyber Security Industry Alliance believes there is a strong need to prioritize funding efforts in a new national agenda for cyber security R&D. The nation must elevate cyber security from being a bolt-on afterthought to a built-in solution.

FEDERAL FUNDING HAS IMPROVED CYBER SECURITY

Despite the comparatively low level of Federal funding for cyber security R&D, money from DARPA and other agencies has triggered significant innovation and improvement during decades of Federal-supported research. Examples include:

Firewalls A firewall repels unauthorized intruders from a network; they are a key element of cyber security systems. DARPA funded research during the late 1980s and early 1990s that led to the first firewall. Analysts predict total revenues for the firewall and related virtual private network market will be just under $6 billion by 2007 (Source: Datamonitor).[10]

Intrusion Detection Systems IDS alerts security administrators to cyber attacks. IDS are critical for accelerating responses to security incidents. Funding from the National Security Agency in the late 1980s and early 1990s, and from DARPA during the middle 1990s, led to the first intrusion detection systems. The combined market of IDS and the newer intrusion prevention systems is projected to be $520 million by 2007 (Source: Yankee Group).[11]

Fault Tolerant Networks A fault tolerant network guarantees continuous communications for critical infrastructure, even if a cyber attack takes out part of the network. DARPA has funded research during the past decade under its Fault Tolerant Networks, which led to failsafe networking technology used by all major hardware and software suppliers.

Operating Systems Poor software code can inadvertently cause cyber vulnerabilities. A recent program at DARPA has helped significantly improve security of operating systems in the open source community, including Linux, OpenBSD and FreeBSD.

Cryptography and Advanced Authentication Individuals can communicate with one or more known parties securely through advanced cryptography and authentication. The

[10] Cited at www.fiberlink.com/release/en-US/Home/KnowledgeBase/Resources/Stats/.
[11] Cited at www.csoonline.com/analyst/report1265.html.

National Science Foundation and the Office of Naval Research provided funding for private sector R&D of public-key cryptography.

Investment in R&D pays off. In a recent memo from i2010, information and communication technology research efforts are measured against productivity and growth.[12] The chart below illustrates that countries with a large Information and Telecommunications (ITC)-producing sector have the highest growth rates of productivity. [13]

	GDP share of ITC-producing sector 1995-2000	*Labour productivity growth 1995-2000*
Ireland	12.3 %	5.3 %
Finland	10.6 %	2.5 %
US	**7.3 %**	**2.5 %**
Sweden	7.3 %	2.1 %
UK	7.1 %	1.8 %
EU	5.9 %	1.4 %
Netherlands	5.8 %	0.9 %
Germany	5.6 %	1.3 %
France	5.5 %	1.2 %
Italy	4.7 %	0.8 %
Denmark	4.7 %	1.9 %

[12] "i2010 – A European Information Society for Growth and Employment," i2019 Information Space Innovation & Investment in R&D Inclusion, June 1, 2005.
[13] "ICT and Economic Growth: Evidence from OECD Countries, Industries and Firms", OECD, 2003.

II. 2005 PITAC REPORT: TEN PRIORITIES FOR CYBER SECURITY RESEARCH

Priority II of President Bush's *National Strategy to Secure Cyberspace* directed establishment of a national cyberspace security threat and vulnerability reduction program. Part of that effort was a directive to prioritize the Federal R&D agenda.[14] The biggest obstacle to prioritization is that there is no long-term, clear agenda. There are many agendas, and too many of those are short-term and development-oriented. In April, the 2004 "National Plan for Research and Development In Support of Critical Infrastructure Protection" was released by the Office of Science and Technology Policy and the Department of Homeland Security (DHS). The plan calls for "the articulation of a vision for the future that takes into account future needs and identifies research gaps based on known threats."[15] It states that agency capabilities and near-term plans were mapped to R&D focus areas to guide future activities, but long-term *goals* of federal R&D associated with CIP are the highlight of this first plan.[16]

Federal funding for cyber security must focus on "R" – including work on security ideas for systems that do not yet exist. The Cyber Security Industry Alliance believes the nation should begin looking at cyber security in a holistic manner, lengthen its perspective and take the long view for improving cyber security, not only in the government, but also in the commercial sector. Like other national security policy areas, co-investment will lead to a better set of solutions that can strengthen the US infrastructure against malicious attacks on our financial stability, harden the Internet economy to create a "safer place" to conduct business, and accelerate security technologies that may not otherwise be funded in an industry-only setting. Government essentially can be more forward-looking than many private sector firms.

PITAC's 2005 Report to the President supports the priorities outlined in the National Research Council of the National Academies' document, and is a good example of research priorities directed at long-term goals and support that align with both commercial and government requirements.[17]

CSIA urges adoption of the ten PITAC priorities listed below for cyber security R&D.[18] CSIA urges Federal coordination of these priorities with others such as the National Academies,[19] the Computing Research Association[20] and the Infosec Research Council.[21]

---

[14] "*National Strategy to Secure Cyberspace*," pp. 34-35.
[15] *The National Plan for Research and Development In Support of Critical Infrastructure Protection*, The Executive Office of the President, Office of Science and Technology Policy and The Department of Homeland Security, Science and Technology Directorate (2004); see p. x.
[16] Ibid, p. x.
[17] Adopted from *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*, Committee on Science and Technology for Countering Terrorism, National Research Council of the National Academies (2002); see pp. 146-176.
[18] Adopted from *Cyber Security: A Crisis of Prioritization*, President's Information Technology Advisory Committee (2005); see pp. 37-46.
[19] *Improving Cybersecurity Research in the United States*, National Research Council, Computer Science and Telecommunications Board; final report expected in 2006.

CSIA recommends the Federal coordinator use these recommendations for creation of a 10-Year Plan for Federal Funding of Cyber Security R&D. This step is more critical than ever, given the dissolution of the PITAC.

PITAC's Recommended R&D Priority Areas for Cyber Security

Priority	Description	Subtopics
Authentication Technologies	Identification, authorization, and integrity checking for hardware/ software, data and users.	Public key distribution; certificate and revocation management; integration of third factor such as tokens or biometrics; separate from identification to maintain privacy
Secure Fundamental Protocols	Hardening of current, un-secure protocols.	Secure protocols for VoIP, wireless, Web and VPN; tradeoffs between security and performance
Secure Software Engineering and Software Assurance	Development practices based on integrated scientific principles and rigorous controls.	Programming languages with integrated security; re-useable, modular secure code
Holistic System Security	The integration of systems and security to addressing inherent complexity.	Mixed environments of (un)secure and legacy/new systems; insider threats; emerging failures in complex system environments
Monitoring and Detection	Track and respond to next generation attacks.	Real-time monitoring; global intrusion detection
Mitigation and Recovery Methodologies	Routines and procedures for rapid response to new threats.	Self-healing and fault tolerance
Cyber Forensics	Online law enforcement to deter criminal activity and apprehend suspects.	Traceback; massive data store searching

[20] "Grand Research Challenges in Information Security and Assurance," Computing Research Association, Nov. 2003.
[21] "National Scale INFOSEC Research Hard Problems List," Infosec Research Council, draft Sept. 21, 1999; revision in process.

Modeling and Testbeds for New Technologies	Realistic models and pilot projects to increase the pipeline of security products.	Confidentiality prototyping; extended network validation
Metrics, Benchmarks, and Best Practices	Universally adopted measurements to evaluate new technologies.	Metrics and benchmarks; automated compliance and risk analysis
Non-Technology Issues	Leverage psychological, economic and social factors not addressed by technical means.	Continued guideline development; privacy valuation; awareness for the economic case of security

III. PROPOSED SOLUTIONS TO BRIDGE THE FUNDING GAP

Cyber security R&D is demonstrably a national priority in need of greater attention. Increased R&D funding will allow researchers to delve into the deep-rooted security issues that plague our networks, produce improved technologies that will offer better protection against cyber attacks, investigate the reliability of monitoring tools that hunt for irregular system activities, and find the way to a secure end-on-end architecture. However, to achieve these goals, extensive and immediate action is necessary in order to return cyber security R&D to the national priority level the President assigned it in 2003.

CSIA offers the following recommendations:

- **Create a Designated Entity to Coordinate Cyber Security R&D Efforts**

One central entity is needed to coordinate with government and private sector R&D efforts aimed at improving cyber security. This could be driven by the recently created Assistant Secretary for Cyber Security and Telecommunications at the DHS. Numerous committees and groups exist with this same intention; however, without a reasonable budget and the teeth to enforce a directive, the missions of these committees become diluted. The PITAC report recommends that within the Networking and Information Technology Research and Development (NITRD) Program, the Interagency Working Group on Critical Information Infrastructure Protection should become the focal point for coordinating Federal cyber security R&D efforts. The level of authority at which this organization operates is not adequate; and although over a dozen agencies participate in the NITRD program, DHS is a participating agency, but not a formal member. The new Assistant Secretary responsible for cyber security at DHS is a logical choice to drive the prioritization of requirements for research and development. There must be a clear plan of attack, a realistic budget that will provide funding to coordinate and carry out efforts, and the ability to aptly guide government and the private sector.

- **Establish a National Vision and Long-Term Plan**

The designated entity overseeing the coordination of cyber security R&D efforts must prepare a long-term plan that delineates R&D efforts, from "basic science" to a product idea to prototype. Key to the plan is establishing a national "vision" for the security, reliability, and resiliency of the information infrastructure within ten years. Such a vision can help drive investment, innovation, growth, and productivity. A deliberate and methodical approach to balancing long-term research funding and short term product development needs is crucial. The PITAC report, linked with the National CIP R&D plan, should establish a national vision and map to key milestones.

This entity needs a plan devoted to recruitment and retention of cyber security researchers. With increased funding for R&D efforts, more opportunities will be made available for students and researchers to enter this field. A recruitment and retention plan to draw in

highly trained individuals in R&D will certainly help with the development and execution of a viable long-term plan.

- **Heighten Congressional Involvement**

Congressional hearings should be held to review the state of Federal funding for R&D, identifying both public and private sector funding sources. These hearings should include testimonies from relevant industries, academic institutions, government research agencies, civilian agencies, and military and intelligence agencies. Congress should follow by appropriating adequate funding, particularly long term research projects.

- **Allow Commingling of DHS Funds**

Legislation for the Department of Homeland Security (DHS) allows the commingling of private and governmental funding sources for R&D activities, which not only creates more R&D opportunities, but is a tremendous benefit to the private sector. Specifically, by working with the government on a product resulting from thorough basic science research, the private sector will share in a joint effort with the government where a known customer awaits, and even anticipates the product; private industry is not simply throwing money into an activity that is, by best efforts, a guess at the "next big thing" for consumers. DHS should exercise the option to turn to all available funding sources and form partnerships with the private sector.

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp.; Check Point Software Technologies Ltd.; Citadel Security Software Inc.; Citrix Systems, Inc., Computer Associates International, Inc.; Entrust, Inc.; Internet Security Systems Inc., iPass, Inc., Juniper Networks, Inc., McAfee, Inc., PGP Corporation; Qualys, Inc.; RSA Security Inc.; Secure Computing Corporation, Surety, Symantec Corporation, and TechGuard Security.

Cyber Security Industry Alliance
2020 14th Street
Suite 750
Arlington, VA 22201
(703) 894-CSIA
www.csialliance.org