The National Institute for Standards and Technology
Computer Security Division:
The Case for Adequate Funding

A Report by the Information Security and Privacy Advisory Board

June 2004

EXECUTIVE SUMMARY

This paper reflects the results of a year-long review by the Information Security and Privacy Advisory Board. The Board is a federal advisory committee established by the Computer Security Act of 1987 and reauthorized by the Federal Information Security Management Act of 2002 (FISMA) "to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget on information security and privacy issues pertaining to Federal Government information systems, including thorough review of proposed standards and guidelines developed by NIST." [See http://csrc.nist.gov/ispab/]

The principal findings of this review are that

- Security standards and guidelines are critical components of an effective cyber security program for the Federal government and must be a focus of continuous development. They must also be understood by and adopted for Federal agencies to effectively manage their cyber security risks.

- The cyber security program of the National Institute of Standards and Technology's Computer Security Division (CSD) performs a vital function in helping protect the critical information systems not only of the civilian (non-defense) side of the Federal Government but also of the nation as a whole. Legislation enacted by Congress in recent years such as the Federal Information Security Management Act (FISMA) and the Cyber Security R&D Act suggests that the Congress recognizes this function, but the programs authorized in these laws require adequate funding.

- NIST's cyber security record of accomplishment is impressive and spans a wide range of areas that continue to demonstrate far greater value than the resources allocated to CSD.

- The Federal government spends annually about $60 billion dollars to purchase and operate information technology products, about half by civilian agencies. The civilian agencies in turn spend 6 to 7 percent of their IT funding, about $2 billion annually, on computer security. NIST's cyber security work should be funded at a level commensurate with the civilian agencies' security investments – and that would be substantially greater funding than NIST now receives.

- While funding for the CSD program in real terms has grown modestly over time, it has not kept pace with the growing demand for cyber security guidelines and standards as a result of the government's and the nation's growing reliance on information technology, the growth and

diversity of the technologies on which we have come to depend, and the increased threat both from acts of negligence and neglect and from those who seek to disrupt or disable the nation's vital systems.

- Interagency transfers of funds, while an important part of CSD's budgeted revenues, are not an appropriate mechanism for ensuring the health of CSD's cyber security efforts as they are (1) inherently unpredictable; and (2) *per force* tied to an agency's specific needs rather than the good of the larger community.

The consequences of inadequate funding for NIST's CSD cyber security programs are that Federal civilian agency systems are not as well protected as they should be, and further, that resources are being wasted as each agency independently devises measures to protect itself.

I. INTRODUCTION

The State of Cyber Security

In December 2002, the U.S. Government passed the Federal Information Security Management Act (FISMA) and the Cybersecurity Research and Defense Act (CR&DA). FISMA requires the "development and maintenance of minimum controls required to protect Federal information and information systems" and "a mechanism for improved oversight of Federal agency information security programs." The law gave authority to the National Institute of Standards and Technology (NIST) to set standards for these controls. The CR&DA authorizes "funding for computer and network security research programs and research fellowship programs." Both bills authorize funding for computer security. These laws are the most recent in a series of statutes enacted over the past several decades that confer substantial responsibilities on NIST in the area of cyber security. However, funds were not appropriated by the Congress for these purposes.

By any measure, the current state of cyber security in Federal systems needs improvement[1]. And by any measure, NIST's cyber security job, primarily carried out by its Computer Security Division (CSD), is huge. The challenges include legacy systems, systems currently being deployed, and the new cyber technology which is being developed --- and deployed --- at an ever-increasing pace.

NIST has been in the computer security business since the 1960s[2]. The Internet revolution has changed the information security equation in fundamental ways. The Internet has vastly increased the importance of computers in government, with computing technology becoming the natural way for many citizens to communicate with government and for government to communicate with itself[3]. By changing the boundaries between what is "inside" and what is "outside," the Internet has made achieving true computer security a much more challenging task.

The Internet era has also been accompanied by a great increase in the virulence of cyber security attacks and their impact. The Morris Worm was launched in the fall of 1988 and affected six thousand UNIX computers. Shortly afterwards, the Defense Advanced Research Projects Agency established, as part of the Software Engineering Institute, a federally-funded research and development center at Carnegie Mellon University, the Computer Emergency Response Team, CERT [www.cert.org], which tracks such incidents[4]. A particularly troubling trend is the annual doubling of incidents: in 1998, there were 3,734 incidents reported to CERT; by contrast, in 2003 there were 137,529. This is the environment that NIST faces.

---

[1]For example, on December 9, 2003, Federal Computer Security Report Cards were announced. The Nuclear Regulatory Commission and the National Science Foundation did well, receiving an "A" and "A-" respectively. The Social Security Administration got a "B+" and the Department of Labor, a "B." There was a single "C+" – the Department of Education. No other government department or agency did better than a "C." The Departments of Energy, Interior, and Homeland Security all failed, receiving "F's. " In recent months, the Department of Interior has even had its web site shut down by a Federal judge because of the department's poor cyber security.

[2]This was mandated by the Brooks Act (89-306(f)). The 1987 Computer Security Act (Public Law 100-235) reiterated NIST's responsibility for developing Federal civilian computer-security standards.

[3]The General Accounting Office has noted "[V]irtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions ... without these information assets" [Dacey, p.7].

[4]CERT also provides technical advice and coordinates responses to security incidents, as well as identifying trends and analyzing attacks.

NIST's customers are not simply Federal civilian agencies, but also include U.S. industry. Computing systems have become pervasive and are integrated into every step of the research and development process and production cycles. As this is true across the world, it is no exaggeration to say that CSD's customers transcend international borders, and weak security abroad threatens U.S. cyber security. The internationalization of CSD's work thus provides direct benefits to the U.S. And because of the standardization and greater interoperability provided through CSD's cyber security efforts, U.S. computer products are made more useful to potential customers and hence more attractive.

Despite the critical importance of the NIST cyber security mission, the agency's cyber security efforts are substantially under funded, with the CSD heavily impacted. FISMA and CR&DA are only the most recent in a series of un-funded mandates. The National Information Assurance Partnership (NIAP) is a textbook example of the problems created by the lack of sufficient funding for NIST cyber security responsibilities.

NIAP is a joint effort of NIST and the Information Assurance Directorate at the National Security Agency (NSA). The international situation for evaluating the adequacy of IT security was quite confused in the early 1990s. NIAP was formed to define and implement the Common Criteria, used by the U.S., Canada and many European countries for evaluating the security of IT products. NIST and NSA worked together in the evolution and early development of the Common Criteria and also to specify the process by which Common Criteria-compliant products would be evaluated.

Initially NIST's CSD was a full participant in NIAP and very heavily engaged in all aspects of the definition of the Common Criteria. However, because of recent funding limitations, NIST's role has been reduced to operating the Common Criteria Evaluation Laboratory certification process (under NIST's National Voluntary Laboratory Accreditation Program) and to participating in some standards efforts focused on Protection Profiles (or "PP's," defined under the Common Criteria as sets of security requirements for categories of IT products to meet specific customer needs) independent of NIAP. NSA has assumed the burden for the entire NIAP program, which is inappropriate given NSA's need to focus on national security matters. Given the potential importance of NIAP for civilian agencies, NIST should be provided appropriated funds to co-manage the NIAP program.

The impact of this situation is clear. NIST's input into NIAP, which reflects civilian agency needs and the requirements and practices of the non-defense sector, has been significantly reduced. An April 2004 combined government-industry task force concluded:

> The stated objectives of NIAP are to meet the needs of government and industry for cost-effective evaluation of Information Technology (IT) products and to improve the availability of evaluated IT products. Currently NIAP has failed to accomplish these objectives. NIAP has been focusing on meeting the needs of the government intelligence community. It needs to re-focus its efforts on the security needs of other government agencies and the needs of the private sector. Getting the National Institute of Standards and Technology re-engaged fully will be critical to the future success of the NIAP by representing the security interests of the private sector and the rest of the government (NCSP, p. E-2). Today, due to budget limitations, there is essentially no NIST representation in NIAP. The NSA-only driven NIAP lacks the balanced view of security to cover all interests, not just the U.S. intelligence community [NCSP, p. E-7).

It is admirable that NSA stepped into the NIAP funding breach. But as the National Cyber Task Force observed:

> NIST should receive new appropriations to be used for the greater adoption of Common Criteria through supporting the development of "market appropriate" PP's. The majority of customers do not need the higher assurance or specific technical security features that the so-called "higher-assurance" evaluations for classified systems entail" [NCSP, p. E-7]

NIST/CSD's Broader Cyber Security Role

Although NIST's legislated responsibilities are for Federal computer security, its computer security work has had wide impact in other sectors. For example, with the passage of the Privacy Act of 1974, and the sharing of protected personal information with state and local governments, agencies needed to protect citizens' personal information as data moved among these jurisdictions. Many states had very strong privacy laws and resisted putting data at risk. NIST's Data Encryption Standard (DES) enabled secure information exchange among federal agencies and with the states, greatly improving program efficiency government-wide and decreasing opportunities for fraud, misuse and abuse of government programs. It also decreased the chance of unintended disclosure of private information. With the availability of DES, critical state information needed to accurately administer these programs could be shared using more advanced transmission methods. The result was better service to the public and more effective state operations.

NIST/CSD's Value to the Federal Government

FISMA requirements make department and agency Chief Information Officers (CIOs) heavily dependent on NIST. Civilian agencies are required to implement "adequate" security commensurate with their operational risks. However, it is often difficult to decide what constitutes adequate security. Agencies may invest too many resources to protect low-risk systems in order to err on the "safe" side. As a result, resources may be diverted from protecting the more important systems. In recent years NIST has published a series of guidelines aimed at helping agencies use a risk-based approach to implementing computer security. These guidelines are critical in ensuring cost-effective investment of limited resources. Additionally, they provide a comfort level to senior management who must accredit systems for operational use.

If CSD is insufficiently staffed and is unable to provide needed security guidance, agency CIOs will look elsewhere for necessary guidance, and may attempt to replicate functionality similar to that being offered by (or which could be offered by) CSD. From a cost and efficiency viewpoint, as well as from the concern about providing high quality cyber security, such duplicative efforts would not be in the government's interest. Money invested in the CSD is money saved at the agency level. It is money that solves the problem once, and allows the solution to be deployed widely, providing both important efficiencies and improved security across the government.

NIST/CSD's Value to Industry

NIST has played a vital role in developing standards that are critical to the nation. The banking industry, for example, embraced DES for electronic banking and EFT applications. Particularly important to banking was the fact that risk and liability were substantially reduced because they were able to obtain high quality cryptographic functionality certified by the government. Thus DES served as an enabler for

the banking industry. Recent further CSD successes include the development and adoption of the Advanced Encryption Standard, a new symmetric-key algorithm for bulk encryption[5].

Even more striking has been the impact of NIST's work on the pharmaceutical industry. This sector has a vital need for high-quality security to support strong authentication for access to sensitive company and patient information, digital signatures to certify the authenticity and integrity of medical data, and encryption to ensure confidentiality of company and patient information. Many of these needs are prescribed by statutes or regulations (e.g., Health Insurance Portability and Accountability Act; 21 CFR Part 11 Electronic Records/Signatures regulations of the U.S. Food and Drug Administration). To meet the needs, pharmaceutical companies employ several products that implement security standards developed by NIST. For example, several companies require that cryptographic devices used to make digital signatures and encrypt/decrypt information comply with FIPS 140 series and that the digital signatures meet FIPS 186 requirements. NIST certification of critical technologies provides the industry with simplified purchase and use criteria, which yield significant cost savings and higher quality product alternatives.

The level of standardization NIST provides around these core technologies enables the industry to create new value. The pharmaceutical industry's use of FIPS-validated cryptography is growing as enormous savings in cost and time can be realized by using secure electronic processes in the conduct of clinical trials. Such trials may take years to perform. Using high-quality cryptographic mechanisms allows the clinical trial process to be dramatically accelerated, leading to increased revenues for the affected companies and quicker availability of drugs and devices to patients. It has been estimated that for so-called "blockbuster" drugs, an acceleration of clinical trials by even one month translates into many tens of millions of dollars of savings. The use of NIST-certified cryptography substantially reduces the potential for later concern over the authenticity, integrity and validity of data used to get FDA approval.

NIST/CSD's computer security work provides a "public good" for government **and** industry. NIST/CSD's success in computer security efforts results from both the quality of their work and their unique role in government. As the Department of Commerce's Deputy Under Secretary for Technology Administration, Ben Wu, observed, "NIST's success relies on its status as an objective, neutral, third party, allowing it to leverage its unique competencies to develop consensus solutions among private sector vendors, standards development organizations, and consortia."[Wu, p.1]

Budget Challenges

During the last decade, as the spectacular changes engendered by the Internet took place, the Computer Security Division's[6] budget has not kept pace with increased demands. While the dollars appropriated to NIST/CSD for cyber security have grown steadily since 1987 (the earliest year for with the Board was able to obtain data), there remains a substantial, unmet demand for NIST/CSD programs and services. See table 1, which shows NIST/CSD funding and staffing since 1987.

[5] Some implementations that have been reviewed and approved by the National Security Agency may be used for transmitting up to Top Secret information [NSA].

[6] Although computer security work in NIST occurs mainly in the Computer Security Division, (CSD), there is related work in other components of the Information Technology Laboratory (ITL) on matters like biometrics. Because it is not possible to break out the cyber security component of other work in ITL, our analysis was based on budget numbers are for the Computer Security Division only.

Computer Security Division
Funding and staffing 1987-2004

($ in thousands)

Fiscal Year	FTE's	Total Budget		Reimbursements		%	Direct $		%	Net change in base funding	ATP $	ATP%	GDP Deflator/non defense**
		Nominal	Real**	Nominal	Real**		Nominal	Real**					
2004	53.44	$15,130	$14,024	$ 5,372	$4,979	36%	$ 9,758	$ 9,044	64%	-14%			1.0789
2003	52.80	$16,508	$15,600	$ 5,367	$5,072	33%	$ 11,141	$ 10,528	67%	6%			1.0582
2002	53.52	$12,550	$12,088	$ 2,199	$2,118	18%	$ 10,351	$ 9,970	82%	-42%			1.0382
2001	47.66	$20,190	$19,742	$ 2,105	$2,058	10%	$ 17,615	$ 17,224	87%	159%	$ 470	3%	1.0227
2000	48.48	$ 8,526	$ 8,526	$ 1,545	$1,545	18%	$ 6,648	$ 6,648	78%	11%	$ 333	4%	1.0000
1999	51.38	$ 8,675	$ 8,889	$ 2,618	$2,683	30%	$ 5,856	$ 6,001	68%	-8%	$ 201	2%	0.9759
1998	49.04	$ 9,986	$10,377	$ 3,677	$3,821	37%	$ 6,309	$ 6,556	63%	-8%			0.9623
1997	39.15	$11,552	$12,117	$ 4,758	$4,991	41%	$ 6,794	$ 7,126	59%	17%			0.9534
1996	36.64	$ 9,980	$10,667	$ 4,219	$4,509	42%	$ 5,691	$ 6,083	57%	2%	$70	1%	0.9356
1995	39.57	$ 7,513	$ 8,192	$ 1,865	$2,034	25%	$ 5,449	$ 5,942	73%	41%	$ 199	2%	0.9171
1994	39.30	$ 5,609	$ 6,270	$ 1,828	$2,043	33%	$ 3,781	$ 4,226	67%	34%			0.8946
1993		$ 4,995	$ 5,696	$ 2,237	$2,551	45%	$ 2,758	$ 3,145	55%	1%			0.8770
1992		$ 5,011	$ 5,874	$ 2,349	$2,753	47%	$ 2,662	$ 3,120	53%	-6%			0.8531
1991		$ 4,292	$ 5,211	$ 1,569	$1,905	37%	$ 2,723	$ 3,306	63%	10%			0.8236
1990		$ 3,790	$ 4,796	$ 1,420	$1,797	37%	$ 2,370	$ 2,999	63%	-3%			0.7902
1989		$ 3,158	$ 4,134	$ 798	$1,045	25%	$ 2,360	$ 3,089	75%	145%			0.7640
1988		$ 1,909	$ 2,598	$ 984	$1,339	52%	$ 925	$ 1,259	48%	-8%			0.7349
1987		$ 1,420	$ 2,003	$ 445	$628	31%	$ 975	$ 1,375	69%				0.7090

Table 1

** Real dollars based on OMB published GDP deflators

ATP = funding received from the NIST Advanced Technology Program in 2004

In 2001, added: $5M for a CIP grants program, ~$3M for CIP research and ~3M for CSEAT

In 2002, lost the $5M for grants program and $3M for CSEATA

In 2003, gained back $1M for CSEAT

In 2004, took share of budget cuts

CSD also receives funds transferred from other agencies. Those funds are typically used to meet a specific need of a particular agency and do not contribute materially to financing the Division's core program. As the data show, they also vary widely from year to year so that it is especially risky to build a program based on interagency reimbursements. Some level of interagency transfers is healthy, however, as it gives NIST/CSD staff the opportunity to work on practical applications.

Lack of adequate budget has meant that serious security issues, such as those surrounding the use of wireless communications, are not addressed in a timely fashion. Other proactive work, such as security requirements for operating systems, firewalls, biometrics, and process control systems, or guidelines for retrofitting cryptographic security modules for Supervisory Control and Data Acquisition (SCADA) systems used by critical infrastructure industries such as utilities, are delayed. Programs such as NIAP do not get the full benefit of NIST's knowledge of industry needs and directions, and both the public and private sector suffer as a result. And emerging, large-scale issues requiring NIST's attention, such as critical infrastructure protection, cannot be addressed.

In the next two sections we will discuss CSD's role in securing cyberspace and potential sources of funding.

II. THE COMPUTER SECURITY DIVISION'S MISSION

Under FISMA, e-government initiatives, and Department of Homeland Security responsibilities, NIST is the cyber security advisor for the civilian side of the Federal government. NIST is broadly responsible for establishing minimum information security requirements (technical, operational, and management controls) for federal information systems, for developing highly-technical cryptographic standards, and for providing management guidelines for information security.

During hearings on the creation of the Department of Homeland Security, industry strongly urged that the CSD be maintained within NIST because of CSD's strong partnerships with industry and the importance of these ties to creating good cyber security. In addition, CSD had significant synergy with other parts of NIST's Information Technology Laboratory. It was deemed inappropriate to recreate CSD in the Department of Homeland Security. Rather, CSD is the scientific/technology partner for information protection at DHS, and it should be used to develop underlying security standards. DHS should solicit from NIST and CSD relevant standards, and then focus on the implementation of these standards in its critical infrastructure protection initiatives.

CSD's efforts are in four areas: (i) emerging technologies, (ii) cryptography standards and applications, (iii) security testing and metrics, and (iv) security management and assistance.

Emerging Technologies

Computing technology changes at a rapid pace: an Internet year appears to be measured in months, if not weeks. Wireless security standards are high on CSD's priority list in emerging technologies. CSD already provides security expertise within standards bodies, and is issuing guidance on wireless security design, implementation, and best practices, all of which are crucial for ensuring security.

There are other emerging technologies for which CSD ought to be developing similar design and implementation guidance. Some, such as RFID (radio frequency ID) are rapidly being adopted for inventory control purposes and have important security and privacy implications. Others, such as Voice over IP, are likely to be rapidly deployed across both Federal and private sectors because of the value they add. Early efforts at "getting it right" can stave off serious security, interoperability, and trade issues later (see related story on China (in box)).

Cryptography Standards and Applications

CSD's unique working relationships with industry, academia, and the Federal government[7] have been crucial in bringing consensus, standards, and interoperability to emerging technologies. The importance of interoperable standards to both industrial development and security cannot be overemphasized. CSD develops fundamental security standards including cryptography that underlies the Internet and other computing technologies. CSD's experience has led to some recent quite stunning successes, including the Advanced Encryption Algorithm (AES) and the Elliptic Curve Cryptosystems (ECC) standards.

CSD has also had major success with Public Key Infrastructure (PKI) technology. PKI is an important tool combining cryptographic algorithms, policies, and process controls permitting strong electronic credentials that can be employed for user authentication, electronic signatures, and data integrity and encryption. PKI is a technology where the devil is in the details, and thus standards and policies have a heightened role in PKI's adoption. NIST's ability to work effectively with civilian and Defense Department agencies and the private sector (including international partners) has enabled the agency to play an important role in advancing PKI policies and standards and in implementing demonstration test beds. Further, NIST has been at the forefront of developing "bridge" technology which permits different PKI's to interoperate, bringing the promise of electronic identity credentials working across multiple agencies, with the private sector, and with foreign governments.

The China Story

CSD is focusing on smart card infrastructure, wireless and mobile device security, access control and authorization management, IPSec, and quantum computing. CSD's goals include developing prototypes and reference implementations, as well as tests, tools, and methods for evaluation and testing. These are the right technologies and the right processes for CSD to be working on.

Wireless provides a critical example of what happens when emerging technologies are deployed without adequate security. Wireless computing incorporated security technology where the underlying cryptography was good, but where the initial protocol implementations were not. There was a series of public breaks and private patches, and a delay in adoption of the technology. This resulted in a more serious problem.

Instead of using the international standard 802.11, China proposed requiring a proprietary cryptographic standard for all WLAN products sold in China that would only be available to Chinese manufacturers of wireless equipment. Such a requirement would have put U.S. manufacturers at a strong disadvantage. A proprietary Chinese cryptographic standard would also have created serious interoperability problems for telephony, which needs to operate internationally. The Chinese government's requirement was to have taken effect in June 2004.

CSD provided the technical justification for senior U. S. officials to argue with China that their approach would impede interoperability and potentially stifle free trade. Through their intervention – which included Secretary of Commerce Donald Evans, Secretary of State Colin Powell, and U.S. Trade Representative Robert Zoellick, as well as various members of Congress - China announced that it would indefinitely delay this requirement. Thus CSD's work in cyber security has a second, unseen benefit: preventing and preempting such incidents as these.

[7]These include IBM, Microsoft, Sun, Boeing, Intel, Computer Associates, Lucent, Symantec, Oracle, Mitre, Purdue, University of Maryland and University of Maryland Baltimore County, Washington State University, and the University of Idaho, University of San Diego, University of Pittsburgh, the National Security Agency, the Department of Defense, the Naval Research Labs, the Defense Advanced Research Projects Administration, and the Department of Justice.

Security Testing and Metrics

CSD's role as an impartial evaluator makes the division invaluable as an IT security and testing organization. At a time when the government is committed to purchasing commercial off-the-shelf (COTS) equipment, CSD evaluations provide very important benefits to securing Federal infrastructure. One example suffices to show this: during the testing of cryptographic modules, fully 48.8% had security flaws while fully 96.3% had documentation flaws (many of which would likely have led to security problems).

The Cryptographic Module Validation Program (CMVP) tests all types of cryptographic modules including radios and phones, link and frame encryptors, fax machines, postal machines, PDAs, kernels, routers and VPNs, cryptographic accelerators and co-processors, and smart cards and tokens. In addition, the CMVP has accredited test laboratories in England and Canada (as well as in the U.S.). This international cooperation in security testing is extremely useful. International efforts are, of course, crucial to security in a time of the global Internet.

Security Management and Assistance

Within NIST, CSD provides additional value not usually found in a scientific organization. Not only does CSD undertake scientific and technological projects, it produces management guidelines. In computer security, science and management must be integrated, and CSD has done an excellent job of integration. The Computer Security Division is *the* Federal organization that provides security guidelines. Funds spent on CSD are repaid many times over to the Federal government through incidents avoided, computer systems and networks not breached, and information secured. Through its guidelines work, CSD touches every Federal civilian agency. Private industry also relies heavily on the NIST guidelines. For more on NIST's work, see Appendix A.

III. Need for Adequate Funding

We note that aspects of civilian computer security appear in several places in the Federal government. NIST has the responsibility for computer security standards for the civilian agencies of the Federal government. Because the Internet is both a supporting structure for critical infrastructure and is also itself an element of critical infrastructure, DHS has a role to play in cyber security. This creates a potential conflict, but the distinction is that DHS focuses on applications of cyber security to critical infrastructure, while CSD focuses on fundamental security standards, implementations, and guidelines.

DHS has already funded some research at CSD and it should continue to do so. Within the Federal government, only NIST can support the type of work that CSD does, which combines scientific quality with a keen understanding of industry's needs. Paul Kurtz, executive director of the Cyber Security Industry Alliance, has said, "If NIST is not strong enough [in terms of guidelines and efficient, open processes and certification], then I think we will see a proliferation of standards that will complicate the security situation." In a time of tight budgets, money invested in CSD activities is money wisely spent. As this report discusses in detail above, CSD's guidelines are used across many Federal departments and agencies as well as large swaths of the private sectors, so a single CSD investment is leveraged many times.

Critical Work that CSD Must be Funded to Carry Out

Properly funding NIAP efforts at NIST is a priority. This includes NIST's current participation as well as various pro-active projects that would build on and simplify evaluation processes. It should also include

developing Protection Profiles (PPs) for routers, PDAs, and virtual private networks, and updating the firewall PP --- *even if NSA has developed PPs for these products.* NSA's PPs apply to the national-security sector; NIST's are for the civilian sector, where the needs are substantially different. (It is not unreasonable to expect that, where both NIST and NSA develop PPs for a single class of products, the NSA PPs will be extensions of NIST's PPs.)

In the area of cryptography and cryptographic protocols, an extremely important CSD project is the development of comprehensive standards for random and pseudo-random number generation. As new technology comes along, there will be new cryptographic problems that need solution; one of these is wireless key management for secure communications.

CSD's to-do list, awaiting increased funding, includes guidelines for effective implementation of COTS products, an important initiative in today's commercial products environment. In line with recommendations from the National Cyber Security Strategy, CSD seeks to provide minimum recommended security requirements for the home and small-business user. This is the type of outreach for which CSD is noted and which it does very effectively.

Another crucial CSD project is a guideline for retrofitting cryptographic security modules for SCADA, as mentioned above. SCADA systems typically do not use encryption and thus are particularly vulnerable to sniffing and attack.

Critical Infrastructure Protection and Homeland Security

More broadly, there is a body of information security work related to critical infrastructure protection and homeland security, which, of all government divisions and agencies, CSD is in the best position to tackle. Protecting America's critical infrastructure requires a public-private partnership and CSD excels in such efforts.

The public-private partnership requires extensive information sharing between private-sector companies and government (particularly in DHS). This has been reinforced in Homeland Security Presidential Directive-7, which identifies cyber-security roles for government and the private sector and establishes broad imperatives for improving both physical and cyber preparedness. Many information-security issues are being identified that can be effectively addressed through the expertise and industry focus that CSD can provide[8].

As DHS begins implementing its Homeland Security Information Network (HSIN), the CSD can contribute by developing standards and recommendations for securing this and other public-private

[8]For example, the Council of Information Sharing and Analysis Centers (ISAC Council) has written a set of eight white papers (see www.isaccouncil.org) addressing necessary steps to enable trusted information sharing between the private sector and government for homeland security. One paper, "A Policy Framework for the ISAC Community," identifies security and privacy issues critical to establishing trusted homeland security information sharing systems. It calls for the development of "basic guidelines and procedures ... for the management of shared information, including analysis. .Basic guidelines should, at a minimum, include ... information categorization criteria for sensitivity and confidence levels ... transmission levels for specific sensitivity and confidence levels ...e.g., using encrypted or private links, and information ... [distribution] to sponsored individuals in vetted organizations."
These are fundamental security concerns and they must be addressed from both a government and private-sector perspective. This work would be a natural extension of FIPS 199*, Standards for Security Categorization of Federal Information and Information Systems*, as well as related publications. The CSD can be quite useful in workings with the ISACs and other industry organizations in bringing these issues to closure.

networks that support homeland security.[9] According to a DHS press release of February 24, 2004, HSIN "will deliver real-time interactive connectivity among state and local partners and with the DHS Operations Center (HSOC) through the Joint Regional Information Exchange System (JRIES). Other DHS agencies participate through seats at the HSOC and their own operations centers, and the system will be further expanded within DHS operations ... Examples of other points of participation include state National Guard offices, Emergency Operations Centers, and first responder and Public Safety Departments... Future program expansion will include the county level, communication at the SECRET level, and the involvement of the private sector." All of these efforts illustrate just how profound an effect CSD can have on securing the national infrastructure.

The implementation of such a new, critical network spanning federal, state, and local law enforcement, and private-sector communities, and carrying sensitive but unclassified data will require application of a number of key security standards directly related to those already initiated within the CSD.

In conclusion, NIST's CSD is the logical organization to perform this groundbreaking security work as part of its core mission. It should be provided necessary funding to carry out this and the other critical functions which we have discussed in this paper.

[9]NIST has been engaged in very constructive dialogue with DHS regarding how NIST could support DHS cyber security initiatives including enhancing its current ICAT (this is not an acronym, just a name) vulnerability database and search engine; developing appropriate security specifications for procurement and use of routers, virtual private networks, and firewalls; and developing guidelines on risk assessments, media destruction and sanitation, and mal-ware. This complements existing NIST efforts to aid DHS in the areas of checklist development, e-authentication, and PDA forensics.

References

[GAO] United States General Accounting Office, *Information Security: Continued Efforts Needed to Sustain Progress in Implementing Statutory Requirements,* testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, 16 March 2004.

[NCSP] National Cyber Security Partnership, Technical Standards and Common Criteria Taskforce, *Recommendations Report,* April 2004.

[NSA] National Security Agency, Committee on National Security Systems, *National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information,* CNSS Policy No. 15, Fact Sheet 1, June 2003.

[OMB] Office of Management and Budget, *FY 2003 Report to Congress on Federal Government Information Security and Management*, March 2004.

[Wu] Wu, Ben, *Information Security in the Federal Government: One Year into the Federal Information Security Management Act,* Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, U.S. House of Representatives, 16 March 2004.

APPENDIX A

This Appendix includes further information on the Computer Security Division's efforts.

Cryptography is the mathematical underpinning for secure communication and secure storage; it provides functionality for authentication (proving the communication is from whom it says it is), integrity (ensuing the data has not been tampered with), and confidentiality. Cryptography depends on strong algorithms, good key management (how the cryptographic keys are transmitted), and ``trust'' in the system development (which is partially a social phenomenon). Given how fundamental cryptography is to security, it should be no surprise that the Computer Security Division has a three-decades-long involvement in cryptographic standards work.

The recent Advanced Encryption Standard (AES) effort demonstrated CSD's unique ability to work with all the players, particularly important in cryptography where trust is so critical to an algorithm's acceptance. A brief reprise is illuminating. CSD opened the AES competition by posting a proposed set of criteria for the new symmetric-key algorithm. When the division received suggestions that the algorithm chosen would probably be more successful if it were internationally royalty-free, CSD changed the criteria in its call for submissions. CSD held AES meetings in the U.S. and in Europe, making clear that the competition was genuinely international (the algorithm ultimately selected was Belgian). The open process was a terrific success. The chosen algorithm was internationally vetted and there is great confidence in AES's security.

The Computer Security Division has been valuable in the effort to enable Elliptic Curve Cryptosystems (ECC), a public-key method which, because it uses shorter key length to provide security equivalent with the widely-used RSA method, is already the public-key algorithm of choice by the U.S. Department of Defense. (Public-key algorithms enable two parties to communicate confidentially over an insecure channel; they are used for key exchanged in the important SSL protocol.) NIST has defined a standardized set of ``curves'' for ECC. A Canadian company, Certicom, has also defined a set of curves, but many companies have avoided implementing the Certicom curves for fear of infringing on Certicom's implementation patents. NIST's defining of the curves is a great industry enabler in productizing ECC. Again, this is exactly the sort of activity that the Computer Security Division excels at, an effort that requires a combination of scientific know-how with an understanding of what the industry implementation issues are.

NIST has played, and continues to play, a central role in the establishment and use of the Federal Bridge Certification Authority, a mechanism that ties together the Public Key Infrastructures in federal agencies, the private sector, and even with foreign governments (initially Canada). This enables electronic-credential interoperability across Federal agencies and government business partners. This saves agencies and business partners' money and effort and avoids the complications of having multiple electronic credentials.

The CSD FIPS 140-2 is the de facto international standard for cryptographic module security requirements. However, the undersized team at NIST cannot process certifications as quickly as industry desires. This often leaves consumers of FIPS solutions in the unenviable position of selecting from older, certified technology instead of opting for newer, uncertified, technology. While the rate of change of technology means there will always be a gap between certified and uncertified security solutions, it is important to keep this gap as narrow as possible so that there is broad industry adoption of certified products. Speed in the certification process has the added advantage of encouraging vendors to develop certified security solutions.

CSD's security metrics and testing group is in an excellent position to build on the successes of NIAP. Some of the NIAP evaluation efforts could be reused if the appropriate testing models existed. For example, if CSD could provide NIAP guidance to product developers on how to compose evaluation results from prior evaluations, and how to maintain Common Criteria certificates for product maintenance changes without the need for product reevaluation, this would speed up the process of NIAP (re)evaluation. One promising project is building an Assurance Maintenance module so that only the changes to a previously evaluated product would need to be evaluated; NIST, with its strong industry connections, understands how to do this in a way that would be most valuable to industry.

It would also be worth developing better guidelines for the evaluation process. It would be extremely useful to develop Common Criteria (CC) interpretations that clarify and simplify how parts of the CC are to be evaluated. CSD could extend NIAP accreditation to those labs that want to specialize in a particular technology area. Again, NIST's understanding of and connection with industry will prove invaluable.

There is a need for research to develop new, less expensive ways of conducting security testing. It is also important to broaden the testing program. NIAP works at the product level. It is important to develop security validation models for system and enterprise architecture models. There is a wealth of opportunity here.

Within the NIST guidelines efforts, one particularly useful form of outreach is the monthly Information Technology Laboratory (ITL) Computer Security Bulletins. These cover a wide variety of topics, from "Selecting Information Technology Security Products" (April 2004) to "Network Security Testing" (November 2003) and "Testing Intrusion Detection Systems" (July 2003) to "Security of Electronic Mail" (January 2003). The ITL Bulletins are quite popular and are widely read. They are an extremely cost-effective way for CSD to share important cyber security information. (See http://csrc.nist.gov/publications/nistbul.)

Several years ago, OMB had noted inconsistent application of security controls as information was shared across the civilian side of the Federal government. CSD produced guidelines: one for standardizing information categorization, one for mapping types of information and information systems to security categories, and one which defines security control minimum standards based of the impact of the information system. This gives Federal CIO's a language and methodology to do the necessary security classifications. CSD has also recently produced a computer security incident handling guide.