Computer & Communications Industry Association
666 Eleventh Street, N.W., Sixth Floor
Washington, D.C. 20001
202.783.0070 Fax 202.783.0534

November 18, 2002

Mr. Richard Clarke
Chairman
President's Critical Infrastructure Protection Board
1800 G Street, NW - 10th Floor
Washington, DC 20502

Dear Mr. Clarke:

On behalf of the Computer & Communications Industry Association (CCIA), I would like to submit our formal comments to the recently issued "Draft National Strategy to Secure Cyberspace" (Draft Report). While we are generally pleased, and advocate many of the proposals detailed, there are several ways in which it could be improved.

CCIA is an association of computer, communications, Internet and technology companies that range from small entrepreneurial firms to some of the largest members of the industry. CCIA was founded over 30 years ago and our members include equipment manufacturers, software developers, providers of electronic commerce, networking, telecommunications and online services, resellers, systems integrators, and third-party vendors. Our member companies employ nearly one million people and generate annual revenues exceeding $300 billion.

The task you and your colleagues have undertaken is one of immense importance. Each day, more people log on to computers and other devices that are more powerful and more connected than ever before. And each day, every user becomes more vulnerable to attacks on computers and telecommunications networks whose importance have never been greater. We offer our comments in the hopes of ensuring security for all of society.

The President's Critical Information Protection Board has done an admirable job of concentrating on goals, rather than becoming enmeshed in the way in which they must be achieved. Nonetheless, we believe there also may be much to be gained through concentrating on enforcement of existing rules and regulations within government. We, therefore, applaud your intent to do better what should have been done before. We want to urge you, in the strongest possible terms, to bring accountability to a process that has far too little.

As the report's authors point out on p. 34, the Department of Defense is moving forward to implement a procurement policy that requires that commercial software products purchased for national security systems successfully complete an independent security evaluation. Evaluations can take place under the international

Common Criteria (ISO-15408), or the US Federal Information Processing Standard (FIPS)-140.

Those requirements notwithstanding, Defense Department acquisitions have routinely continued without any independent guarantees of information assurance. We therefore support language attached to the U.S. House of Representatives' version of the Defense Authorization bill that would direct the Secretary of Defense to assure compliance with this guideline, which became mandatory earlier this year.

Problems with computer security are found throughout government. Indeed, as General Accounting Office (GAO) officials have privately confided, many Federal agencies have undergone several audits over the past ten years, and each time have shown the same deficiencies in their handling of computer-security problems. The GAO has issued literally dozens of such reports in recent years.

These problems can most clearly be seen in the GAO's recent audit of reports required under the Government Information Security Reform Act (GISRA).

Among other things, the law requires Federal Government agencies to ensure that their systems are secure. Failing that, the Office of Management and Budget (OMB) has the authority to earmark an amount of the agencies' budgets for security improvements.

The GAO, in fact, gave a clean bill of health to only one agency of more than 20 in a recent survey. A recent OMB study reached much the same conclusion. Yet, for all the glaring problems, we are aware of no federal official who has lost his job, been demoted or even reprimanded as a result of the ongoing information-security crisis in government.

We encourage you, then, to act swiftly in fulfilling your pledge to bring greater accountability for security within the Federal government. Likewise, we applaud efforts by Congress to make permanent the GISRA. While proponents may differ on OMB's role in the process, we believe that proposals to make GISRA permanent, including the latest version of Department of Homeland Security legislation, are an excellent first step to real computer security.

Write Good standards, Enforce Better Ones

Despite more than a decade of effort, we know today that the Federal government often sets a high hurdle for security, only to waive its own security requirements when the time comes to award contracts to the private sector.

OMB and other government agencies must limit the practice of granting waivers to security requirements simply because contractors claim that security is too difficult or cumbersome to implement. In some cases, the government should consider delaying some contracts or paying a premium for goods and services when such delays will ensure that the government will be able to purchase technology that can secure

networks broadly.

At the same time, we believe the government must examine closely the state of computer-security benchmarks currently in use. We especially urge reexamination of Validated Protection Profiles, which are part of the internationally recognized Common Criteria for computer security.[1] Because many protection profiles have little to do with real-world security problems, they are less effective than they should be in offering protection against real-world security challenges. That lack of practicality, moreover, mans contracting specialists can justify use of clearly insecure products by asserting that certified ones are equally flawed for the task at hand.

Government should encourage a greater and more useful variety of protection profiles. Today, there are a large number of protection profiles that have been submitted as evaluation standards to the Federal government by the private sector. Most of them languish unused while the ones that have been approved are too often flawed, or of limited real-world usefulness. We urge you to direct the National Information Assurance Partnership (NIAP) to clear its backlog of protection profile proposals, providing industry and government with standards in which they can have confidence. Better profiles will lead to greater trust in the NIAP and greater assurance in security overall.

Finally, we note that today there are open source programs that have earned certification under the Common Criteria. Given the nature of open source development, it is not surprising that an organization or group has expended the effort and resources necessary to achieve such certification. At the same time, DARPA is sponsoring an important open source security program known as the Composable High Assurance Trusted Systems program, or CHATS.[2] If DARPA completes this work, it seems axiomatic that it should also fund its certification.

Use the Government's Market Power

It is imperative for the Federal government to leverage its enormous purchasing power as a commercial IT consumer to foster a stronger "culture of security" within the technology industry. Producers of technology products will never create sufficiently secure technology until their customers insist on secure products and services. Leadership by the world's *largest* IT customer – the Federal government – is indispensable to this effort.

Indeed, the Draft Strategy seems to recognize this fact, but at the same time seems dismissive of the notion that government procurement policies will likely produce change. As we see it, claims that such efforts have "failed" in the past[3] ignore decades in which the government had little interest in promoting security in private networks and computer systems. They also seem unaware of the plethora of specialized computing devices still made for the National Security Agency, which employs more

[1] http://niap.nist.gov/cc-scheme/PPRegistry.html
[2] http://www.darpa.mil/ato/programs/chats.htm
[3] Draft Report, 34

computer-security experts than any other organization on Earth, and utilizes the most advanced security (and hacking) technologies available.

Homogeneous Networks, Dangerous Networks

Home users are frequently victims of network insecurity, and home users who fail to use firewalls, anti-virus software and the latest software patches are the most vulnerable. The tens of millions of home users are also particularly useful as unwitting accessories for hackers who want to launch distributed denial-of-service attacks.

Despite this situation, we see little hope in asking the average computer user to upgrade his system, as proposed by the Draft Strategy. Given the complexities of even rudimentary security, there will always be thousands, if not millions, of PCs ready to be exploited as network "zombies." And as long as those machines exist, hackers will scan the network for them, and then exploit them. To be sure, individuals will be safer when they utilize the security tools available to them, but hackers don't need to attack protected computers. They will always go after the "low-hanging fruit," of which there will undoubtedly be enough to cause significant harm.

For all the emphasis on good behavior and best practices, the Draft is inexplicably silent on the dangers of computing homogeneity – a fundamental principle of information security that says when all systems are the same, all will fail the same. Under the proper circumstances, such common vulnerabilities lead to a snowball effect that can crash major nodes of the network, and greatly increase the power of even unsophisticated attacks launched by those who would harm our computing infrastructure.

Unfortunately, actual examples of this problem abound. In recent years Outlook and Outlook Express -- Microsoft's dominant e-mail client -- have spread billions of copies of Windows worms around the globe due to poorly vetted coding and fundamental weaknesses in security design. Damages resulting from these attacks have climbed into the multiple billions because, unlike other e-mail programs, Outlook is part of the Microsoft Office suite of PC software, which relies on Windows scripting technologies. Windows scripts, among other things, can execute almost any random code on a Windows computer, including commands that can send copies of an attacking virus to 50 or more recipients found in a typical Outlook address book. And like virtually every virus, worm and similar malware, such scripts will run on Windows, but not Macintosh, Linux, Unix or any other operating system unless the user himself decides to install Microsoft products.[4]

Paul Strassman, a lecturer at the National Defense University and Special Assistant to NASA's Administrator for Information Management warned of this syndrome as it applied to the Windows monopoly back in November 1998.

---

[4]High-profile worms that have exploited this single flaw in Outlook include the Klez and Klez.g worms, the I LOVE YOU and Melissa worms, ExploreZip, BugBear, Nimda, SirCam and others too numerous to mention.

> "It's only a question of time before the ubiquitous presence of Microsoft operating systems -- supported by a software-updating network -- reaches a state of interconnectivity that makes a universal systems crash feasible," Strassman wrote. "All that will be required is inducement of a widespread information infrastructure collapse through a deliberately executed and preplanned act of information warfare ... What's at stake for society is not Microsoft profit but the enormous risk to the economic viability of all computer-dependent enterprises." [5]

MITRE echoed Strassman's thoughts in an Oct. 28 monograph "Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense."

MITRE prepared the report for the Defense Information Systems Agency, in part in order to catalogue the influence of open source software on the Defense Department. Among other things, open source opponents have argued that "free" software poses security risks, but MITRE came to the opposite conclusion. Diversity in computing, the research group found, is something to be pursued: "Acquisition diversity reduces the cost and security risks of being fully dependent on a single software product, while architectural diversity lowers the risk of catastrophic cyber attacks based on automated exploitation of specific features or flaws of very widely deployed products."[6]

Indeed, MITRE found open source software itself is indispensable to DoD security:

> One unexpected result was the degree to which Security depends on [Free and Open-Source Software (FOSS)]. Banning FOSS would remove certain types of infrastructure components (e.g., OpenBSD) that currently help support network security. It would also limit DoD access to—and overall expertise in—the use of powerful FOSS analysis and detection applications that hostile groups could use to help stage cyberattacks. Finally, it would remove the demonstrated ability of FOSS applications to be updated rapidly in response to new types of cyberattack. Taken together, these factors imply that banning FOSS would have immediate, broad, and strongly negative impacts on the ability of many sensitive and security-focused DoD groups to defend against cyberattacks.[7]

Open source software typically allows anyone to examine, modify and copy programs as they desire. Yet, Hewlett -Packard, Sun Microsystems, Silicon Graphics, Oracle, IBM, America Online, Red Hat and a host of others have shown significant profits from giving this software away, integrating it into their commercial products, and providing related products and services.

Given all we know about diversity in software and the software community's dependence on open source software for good security, we believe you should take a closer look encouraging use of a wide range of products and services within the government. Rather than focusing on a specific configuration, we think the government needs to focus on the power of open standards and good security

---

[5] http://www.strassmann.com/pubs/cw/ms-security.shtml

[6] USE OF FREE AND OPEN-SOURCE SOFTWARE (FOSS) IN THE DEPARTMENT OF DEFENSE: VERSION: 1.2, Prepared by the MITRE Corporation for the Defense Information Systems Agency (October 28, 2002), at 2. www.egovos.org/pdf/dodfoss.pdf

[7] Id. at 2. (emphasis in original).

practices.

Perversely, the plan takes precisely the opposite approach. Rather than recognizing that networks are most secure when they are heterogeneous and based on open, transparent standards, "OMB is exploring ways to promote greater uniformity of systems throughout the Federal enterprise."[8] (p. 34) Again, such thinking is entirely counter to good security practices. The fact that the government has effectively chosen Windows as its standard personal computing platform makes this policy all the more alarming.

Get It Right From the Start

The report properly focuses on the need for more and better research and development in security. We agree enthusiastically that more R&D is needed and urge you to press hard for the resources needed for such projects.

But as the government explores new avenues for R&D, we hope you will think deeply, and act boldly, in addressing problems we face. Once developers have rewritten much of the flawed work that exists today, they must concentrate on building security in from the ground up. We as an industry still struggle to write truly secure software or design truly secure hardware. Government and industry can and should collaborate on finding new ways to develop software that go far beyond being more careful with the techniques we have today.

Reform the Digital Millennium Copyright Act

CCIA recently wrote to you, commending your call for reforms to the Digital Millennium Copyright Act (DMCA) to allow for better security research and vulnerability disclosure. We again reiterate our offer to work with you and Congress in the upcoming term to help ensure this happens. We have long believed that the DMCA would have many unintended consequences, and during Congressional consideration worked hard to alleviate some of these concerns. We are gratified to see that the Administration, and you in particular, recognize these same concerns.

While our prior proposals have focused more on methods the government can enact to ensure that their systems are less vulnerable and more secure, reforms to the DMCA will have a positive impact for all computer systems and benefit the public at large. Currently, there are many in security research who have been bullied into silence from threats of legal repercussions based on the DMCA. One such example of this is Princeton University Professor Edward Felton's choice not to disclose publicly his research on security vulnerabilities to a commercially used watermark protection scheme.[9]

---

[8] Draft Report, 34.

[9] For Dr. Felton's reasons for not presenting, and a more detailed history of this example, see http://cryptome.org/sdmi-attack-02.htm.

While copyright owners, software developers and hardware makers may gain short-term commercial advantages in keeping vulnerabilities hidden, the long term harm is great. Silencing researchers does not help the cause of secure systems.

In Whom Do We Trust?

CCIA notes several references in the Draft Report to Trusted Computing. On its face, there's no clear reason to oppose efforts to coordinate hardware and software security. Indeed, the benefits promised by its proponents would answer many of the chronic problems that urgently need to be addressed. Nonetheless, trusted computing is an area that must be approached with real caution.

Although details of how Trusted Computing initiatives could work are scarce, all rely on the concept of a "trusted party" to decide what hardware and software may run on a given user's computer.

In theory, only hardware and software deliberately installed by the owner will run on a trusted platform. Thus, viruses sent without the owners' knowledge should not operate on such PCs. Hackers, likewise, will find it much harder to penetrate such systems. But "security" may mean one thing to a PC owner, another to a content producer, and yet another to a firm seeking to eliminate competition in information technology markets.

For example, a "trusted platform" could be put to anticompetitive and deeply anti-consumer uses. Depending on how it is designed, an operating system could "lock down" a PC so that only those devices approved by the OS manufacturer will run with it. The potential harm to competition under such a scenario is obvious. Conversely, a hardware manufacturer could ban the use of "unapproved" operating systems. Again, implications for competition are apparent and fraught with difficulty.

As you are doubtless aware, the best-known proposal for trusted computing is "*Trustworthy* Computing," a Microsoft marketing term that appears repeatedly in the Draft Report, rather than the far more common, vendor-independent term "*Trusted* Computing."[10]

Unfortunately, not all proponents of Trusted Computing have designated the user as the trusted party. Many would prefer that another party have control over the PC owner's machine. Indeed, when used as a technique to prevent copying or moving copyrighted material from one PC to another – so-called digital rights management as found in Windows Media Player and Adobe e-books -- someone other than the computer's owner must be the trusted party.

Such control over copying in many ways describes Sen. Ernest Hollings' (D-SC), Consumer Broadband and Digital Television Promotion Act. CCIA has expressed its objections to Sen. Hollings' bill in part for its government mandates, but also for its

[10] http://www.microsoft.com/presspass/exec/craig/10-02trustworthywp.asp.

overly restrictive nature, which would erode First Amendment rights to use, copy, and extract from others' works for many personal and non-commercial uses. While CCIA does not intend to use this forum to discuss our views on intellectual property and Fair Use, we find it disconcerting that any third party, let alone an adjudicated monopolist, could have control over any or all data residing on one's personal computer.

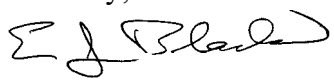
If the government is to proceed with any initiatives regarding trusted computing, such work must be done with a constant eye towards encouraging competition and protecting consumer rights. Doing otherwise will harm the very way of life this project is sworn to uphold.

Conclusion

The Draft National Strategy to Secure Cyberspace appropriately focuses on practical actions private and public sector alike can take. At the same time, the government is uniquely positioned to affect the security marketplace. For while the U.S. Government has neither legal authority nor the practical means to secure all networks, it certainly has purchasing power and maintains technology leadership sufficient to influence security products available on the market. The government, moreover, remains the largest single custodian of sensitive information, regardless of who owns the fiber and copper over which it may travel. Thus, even if the private sector owns 90 percent or more of the nation's networks, the government remains the most important player in keeping our nation safe from criminal or terrorist attacks on our technology infrastructure.

Mr. Clarke, CCIA and its members companies remain committed to helping the nation secure its critical infrastructure now and in the future. We look forward to working with you to achieve this goal.

Sincerely,



Ed Black
President and CEO