(corrected)

March 19, 2004

The Honorable Tom Ridge
Secretary
Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Ridge:

I am writing to express my deep concern that far too little progress has been made in securing the information systems on which the nation's critical infrastructures depend. Systems and facilities essential to our economy, public safety, and national security – the Internet and other telecommunications networks, our power grid and water supply, our public health and law enforcement services, emergency response, and even national defense – all depend on the security of their interconnected computer operations. This critical cyber infrastructure is subject to a growing risk of attack from a variety of individuals and groups. Terrorists, international criminal groups, and intelligence services, as well as hackers and disgruntled insiders, are quickly developing the ability to use, and are using, cyber tools to steal data or cause damage to government and business systems.

The Administration issued a *National Strategy to Secure Cyberspace* in February 2003, laying out general strategic objectives for the Department of Homeland Security (DHS) and other agencies with responsibilities in this area, but has accomplished little since then. The 2003 year-end flurry of activity – the December 3 "National Cyber Security Summit" convened by DHS and industry, and the December 17 directive issued by the President on critical infrastructure protection – lay out plans and intentions for the future that reveal how little has actually been accomplished. The Summit was convened to form private/public sector taskforces to address cybersecurity problems, and, in your remarks, you presented to the Summit the following goal: "The President laid out a vision, but what we need now is a blueprint ... the practical steps we must take to realize that vision and our goal of greater security for our cyber networks and the physical infrastructures that support." Most striking was that more than a year after enactment of the Homeland Security Act (HSA), and 10 months after issuance of the *National Cyberspace Strategy*, all that could be announced in December was neither a plan nor a blueprint, but a plan to create a blueprint.

Events over the past year have dramatically demonstrated the vulnerability of our critical infrastructure to cyber attack and the urgent need for action. The SoBig, Blaster, Slammer, MyDoom, and other worms that disrupted and crashed Internet-connected systems and corporate networks throughout the past year have shown how the number and virulence of attacks are escalating exponentially. *Business Week* estimated that the damage from these worms in the first three quarters of 2003 alone may have amounted to over $13 billion.[1] Last August, three new highly virulent worms emerged in just 12 days, infecting millions of computers worldwide; and, in end-of-the-year reckoning, the Sobig.F virus was dubbed "worm of the year" – having spread more ferociously than any virus ever before seen, and having subjected some companies to hundreds of thousands of infected e-mails every day.[2]

In addition to the cost and disruption of these Internet-borne worms and viruses, there is a growing concern that cyber attacks could yield a crippling blow to specific, essential infrastructure sectors. Internet worms have silenced the electronic switchboards that run emergency 911 systems, and, in January 2003, shut down the monitoring system of a – thankfully, idle – nuclear power plant. The power blackout that paralyzed the Northeast U.S. and parts of Canada last summer, while apparently not caused by malicious activity this time, nevertheless exposed vulnerability of the computer systems that control the grid[3] and demonstrated the magnitude of the harm that a malicious disruption of the grid could cause.

Although the risk from our cyber vulnerability spirals upward each passing year, this is far from a new problem. As early as 1996, Congress required the President to review and report on policy for protecting the national information infrastructure against strategic attack.[4] That same year, President Clinton established the President's Commission on Critical Infrastructure Protection, which laid out an initial strategy that underpinned the President's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 (PDD-63) issued in May 1998. While the scope encompassed all critical infrastructure, the emphasis of PDD-63 was on protecting the cyber systems on which critical infrastructure depends. The directive set forth a goal of achieving the ability to protect the nation's critical infrastructure from intentional

[1] "Epidemic: Crippling Computer Viruses and Spam Attacks Threaten the Information Economy. Can they be stopped?" *Business Week* Page 28. September 8, 2003.

[2] "Security Threats Coming from all Sides" *Small Business Computing.com* (http://www.smallbusinesscomputing.com) March 18, 2004. "Sobig-F Wins 2003 War of the Worms" press release (www.sophos.com) December 3, 2003.

[3] "Hackers Did not Cause Blackout - Report" *Washington Post* (http//www.washingtonpost.com) November 19, 2003, quoting Joseph Weiss.

[4] Section 1053, National Defense Authorization Act for FY 1996, Public Law No. 104-106.

destructive acts within five years, emphasized the importance of a public-private partnership, and set up a governmental structure to address the country's potential vulnerability. Among other things, federal and private-sector representatives were given responsibility for developing protection plans for each infrastructure, and those recommendations were ultimately to be used to build a National Infrastructure Assurance Plan. An initial version of such plan, entitled *Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0: An Invitation to a Dialogue* (the "*National Plan*"), was released in January 2000.

After the events of September 11, 2001, of course, the need to protect the nation's critical infrastructure took on even greater urgency; and the physical threat, including the risk of a simultaneous physical and cyber attack, was made even more apparent. The Governmental Affairs Committee held a series of hearings in the fall and winter of 2001-2002 on homeland security, including a number that addressed critical infrastructure protection. Following up on those hearings, I sent you a letter on March 19, 2002, in your capacity then as Assistant to the President for Homeland Security, requesting, among other things, an update on the federal government's planning to protect key critical infrastructures. In your response, dated April 10, 2002, you assured me that the Office of Homeland Security and the President's Critical Infrastructure Protection Board were "currently engaged in National-level efforts to review critical infrastructures by sector, identify problems associated with their protection across both the cyber and physical dimensions, and propose solutions across a wide range of possible candidate actions . . . ."

On January 23, 2003, sixty days after enactment of the HSA, the DHS was established and assumed overall responsibility for securing our cyber infrastructure. Then on March 1, 2003, several offices established by PDD-63 for identifying and responding to cyber incidents and for coordinating the national effort to reduce infrastructure vulnerabilities were consolidated into the Department pursuant to the Act.

After these many years of planning and effort, and one year since the Department of Homeland Security was established, I am deeply troubled at how little has been accomplished to reduce the very real threat to our computer-based infrastructure. The *National Strategy to Secure Cyberspace*, issued with much fanfare in February 2003, explained how the government's cybersecurity responsibilities were being reassigned after creation of the Department. The *Strategy* laid out strategic objectives, updating and expanding upon those in PDD-63 and the 2000 *National Plan*, and assigned to DHS overall responsibility for cybersecurity, by, for example, developing a comprehensive national plan for securing cyber-dependent and other critical infrastructure, providing crisis management for cyber attacks, coordinating with others to provide specific warning information and advice about protective measures, and funding research and development. But the *Strategy* expressed these and other responsibilities in vague generalities, without clear assignment of responsibilities and without time frames or deadlines or benchmarks for measuring performance.[5] Moreover, under pressure from business interests, the Administration substantially weakened the *Strategy* while readying it for the President's signature, stripping any hint that the federal government might require or even exert pressure on non-federal entities to make the parts of cyber infrastructure for which they are responsible more secure. Instead, the document relies on hopeful words about how DHS will "encourage" the private sector and state and local governments to reach consensus and to take necessary actions, and on glowing promises of what the Department will accomplish sometime in the future.

Having issued this vague and weak plan, the Administration did little in the area of cybersecurity for over half a year. Richard Clarke, President Bush's special advisor for cybersecurity, resigned two weeks before the *Strategy* was issued, and his successor, Howard Schmidt, resigned two months later after unsuccessfully attempting to persuade the Department to create a high-ranking cybersecurity position.[6] It was not until mid-September that a cybersecurity chief was brought into the Administration, when Amit Yoran was appointed to head the Department's new National Cyber Security Division. While he brings valuable computer-security experience to the job, the Administration's lassitude and lack of leadership have left him the unenviable job of playing a difficult game of catch-up.

In early December of 2003, the "National Cyber Security Summit" put the Administration's lack of leadership on full display. In an apparent effort to jump-start the Administration's stalled cybersecurity program, the Department and several industry groups jointly convened the Summit in Santa Clara, California. The days leading up to the Summit saw a flurry of finger-pointing in the press, as high-tech industry leaders publicly expressed their frustration with the lack of progress and said that they hoped to use the Summit to refocus the administration's attention on cybersecurity.[7] At the Summit, the Department pointed the finger back to industry, as when Robert Liscouski, Assistant Secretary for Infrastructure Protection at DHS, said, "The private sector has to step up to its responsibility." He continued, "There are a lot of people who are willing to legislate . . . . If that's what you want, I can promise you that's what you're going to get."[8]

[5] See the assessment of the *National Strategy to Secure Cyberspace* by the General Accounting Office, *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues* (GAO-03-1165T) September 17, 2003 Page 24.

[6] "Government Creates New Cybersecurity Office" *WashingtonPost.com* (http//www.washingtonpost.com) June 6, 2003.

[7] "Computer Security in Focus" *San Jose Mercury News* December 3, 2003 Page 1. "Cybersecurity Talk is Cheap" *WashingtonPost.com* (http//www.washingtonpost.com) December 3, 2003.

[8] "U.S. Pressing Industry on Technology Security" *New York Times* December 4, 2003.

What emerged from the Summit was the formation of several taskforces, under mostly industry leadership, to develop plans to address five key aspects of cybersecurity: security education and awareness for home and small-business computer-users, a national early warning capability for cyber attacks, best practices and standards for corporate governance, technical standards and common criteria, and achieving secure software through security across the software development cycle.

In your prepared remarks at the Summit, you explained that the main purpose of the event was "to further strengthen the partnerships between Homeland Security and the private sector," and you stated: "The President laid out a vision, but what we need now is a blueprint ... the practical steps we must take to realize that vision and our goal of greater security for our cyber networks and the physical infrastructures that support" – thus acknowledging that, 10 months after the *National Cyberspace Strategy* was issued, all we have is a "vision" and we are still waiting for the blueprint.

The working groups agreed at the Summit to release whitepapers by March 1, 2004, outlining their recommendations for action, and said they would meet again in September 2004, by which time each group will deliver at least some results. Now acting through a business coalition called the National Cyber Security Partnership, two of the task forces released tentative recommendations on March 18. Among other things, the task force on early warning recommended the creation of an Early Warning Alert Network by year-end to enable prompt and reliable distribution of information and facilitation of crisis communications among business and government entities, and the establishment of a National Crisis Coordination Center by 2006 to share threat and vulnerability data within and among different industries. The task force on cybersecurity awareness developed educational materials for small businesses and home users and proposed plans for direct mail and regional forums to target top executives of the largest companies. The other working groups plan to issue their initial reports in the next several weeks.

According to news reports, the private-sector executives who announced the plans on March 18 struck a cautious note, describing the recommendations as a "good starting point," but as a strictly "voluntary effort" and definitely "not a one-stop solution" for cybersecurity or an advisory effort for DHS.[9] One security expert has been quoted in the press as saying that these task forces are attempting to shift the responsibility for security from the vendors to the end users; Alan Paller, director of research at the Bethesda, Md.-based SANS Institute, said, "In essence, the vendors are promoting a 'blame-the-user' strategy because they cannot or will not

[9] "Security Groups Call for Education, Alert Systems" *CNET News.Com* (http://msnbc.msn.com) March 18, 2004. "IT Industry Releases Security Action Plans for DHS" *Computerworld* (http://www.computerworld.com) March 18, 2004.

build comprehensive security solutions that protect their clients."[10] Committee staff are reviewing these just-released task force reports.

Indeed, those who buy and use technology – the operators of the critical infrastructures themselves, such as power companies and the telecommunications industry – were largely absent from the Summit – but DHS officials said that they would be meeting with those organizations early in 2004.[11] Richard Clarke, President Bush's former chief adviser for cybersecurity, stated that, by allowing a small group of IT vendor associations to sponsor this first Summit, the DHS seems "to have outsourced the effort to the IT industry." He said: "It was not a Department of Homeland Security meeting. . . . The department should have taken the leadership, and all of the key infrastructure sectors should have been represented."[12]

Moreover, this Summit did not even begin to address the broader question of how to secure individual computer-dependent sectors, such as the power grid or water facilities. There has been little indication of any progress by the Administration on this front, and on December 17, in the Homeland Security Presidential Directive/HSPD-7, the President granted the Homeland Security Department yet another year – nearly 2 years after the Department was established – just to develop a "plan" to identify, prioritize, and protect key cyber systems and other critical infrastructures. Comprehensive planning is essential to establish priorities and to coordinate the activities of the multitude of public and private organizations whose efforts must be marshaled cost-effectively and strategically to reduce the threat of cyber-related attack to our infrastructure and national security. It appears the Administration has been running in place, leaving us little closer to having meaningful protections for the vital computer-dependent systems on which the country depends on each day.

I am therefore requesting that you provide a full account of the Administration's efforts to protect our nation's critical computer-dependent infrastructure and to evaluate its vulnerabilities. In doing so, please include answers to the following specific questions:

[10] "IT Industry Releases Security Action Plans for DHS" *Computerworld* (http://www.computerworld.com) March 18, 2004.

[11] "Reporter's Notebook: At the DHS National Cyber Security Summit" *Computerworld* (http//www.computerworld.com) December 4, 2003.

[12] "Cybersecurity Debate Heats up" *Computerworld* (http//www.computerworld.com) December 12, 2003.

QUESTIONS

A. **Reduction of Cyber Vulnerabilities.** Hostile actors could inflict harm by attacking our information infrastructure in a variety of ways. Some are straightforward cyber attacks, such as using the Internet to spread viruses, to gain access to confidential data, or to disrupt the power grid. Other troubling scenarios involve a combination of cyber and physical attack. For example, while recent virus attacks demonstrate the vulnerability of the Internet to temporary disruption, some experts speculate that terrorists could combine viruses with well-placed bombs to bring down the Internet for months.[13] Others see cyber terrorism as a "force multiplier," by for example taking down emergency response 911 networks after a physical terrorist attack.[14] However, we cannot afford to squander precious time and resources by addressing every worst-case scenario. Accordingly, an essential part of defending our information infrastructure is to prepare a comprehensive plan – to identify and thoroughly assess critical system assets, interdependencies, and vulnerabilities and to develop realistic programs for remedying the vulnerabilities, while continuously updating the assessment and remediation efforts.

The federal government recognized and assumed responsibility in this area in PDD-63 and the 2000 *National Plan for Information Systems Protection.* In the July 2002 *National Strategy for Homeland Security*, the Administration made bold promises about such planning, asserting that "baseline" cyber and physical infrastructure protection plans would be released by the end of Fiscal Year 2002, and then the proposed Homeland Security Department would build on these plans to develop and coordinate implementation of a comprehensive national plan, which would include standards and benchmarks for measuring performance, and would inform the Department's annual process for planning, programming, and budgeting, including research and development. (Page 33.) The Homeland Security Act codified the Department's obligation to "develop a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including . . . information technology, . . . [several cyber-reliant sectors such as electric power, telecommunications, and electronic financial systems,] and the physical and technological assets that support such systems." (Section 201(d)(5)).

The *National Strategy to Secure Cyberspace* (the *Cyberspace Strategy*, or the *Strategy*) issued in February 2003, almost a half year later than promised, singled out three particular

[13] "Bringing Down the Internet: What if hackers were motivated not by loneliness or greed, but by malice? Some experts now think a global cybercrisis is inevitable." *Newsweek International* (http//msnbc.msn.com/id/3339638) October 28, 2003.

[14] "Experts: Little Chance of 'Digital Pearl Harbor'" (http//www.newsday.com) February 12, 2003.

aspects of our information infrastructure – the mechanisms of the Internet, the digital systems that control and monitor industrial equipment, and the quality of software generally – and tasked DHS with responsibility for encouraging or effecting increased security in these areas. Even in these specific areas where the *Strategy* directed the Department's attention, the *Strategy* only made vague promises without specifying clear responsibilities, interim steps, timetables, or benchmarks.[15] And beyond these three areas singled out for attention, the *Strategy* essentially punted, directing DHS to fill in the specifics by further vulnerability assessment and planning – again with no timetables or benchmarks, thus deferring the hard work of establishing priorities and establishing standards for measuring success. Then on December 17, 2003, the President issued HSPD-7, acknowledging the need for such planning and granting the Secretary of Homeland Security yet another year to accomplish it.

Areas Specifically Identified in the *National Strategy*

1. Securing the Mechanisms of the Internet. The *Cyberspace Strategy* includes: *(1)* DHS, in coordination with the Commerce Department, will coordinate public-private partnerships to encourage: *(a)* the adoption of improved security protocols in the Internet, *(b)* the development of more secure router technology, and *(c)* the adoption by Internet Service Providers of a "code of good conduct," including cybersecurity practices; and *(2)* DHS will support these efforts as required for their success, subject to other budget considerations. No interim steps, deadlines, and benchmarks for success in securing the mechanisms of the Internet are included in the *Strategy*. (Pages 30-32.)

    a. What steps has DHS taken, and what steps has the Commerce Department taken, to establish and coordinate effective partnerships with the private companies that own and operate the mechanisms of the Internet?

    b. Are the taskforces established at the National Cyber Security Summit addressing the security of the mechanisms of the Internet? If so, how is the work of those

[15] The General Accounting Office evaluated the *Cyberspace Strategy*, as well as the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, which, like the *Cyberspace Strategy* was released in February 2003, and determined: "Neither strategy (1) clearly indicates how the physical and cyber efforts will be coordinated; (2) defines the roles, responsibilities, and relationships among the key CIP [critical infrastructure protection] organizations, including state and local governments and the private sector; (3) indicates time frames or milestones for their overall implementation or for accomplishing specific actions or initiatives; nor (4) establishes performance measures for which entities can be held responsible." *Homeland Security: Information Sharing Responsibilities, Challenges, and Key Management Issues* (GAO-03-1165T) September 17, 2003. Page 24.

taskforces being coordinated with the efforts of the partnerships established with the owners and operators of the mechanisms of the Internet?

c. What steps to secure the mechanisms of the Internet has DHS already completed?

d. Please provide a timetable, including final deadlines, for taking steps to secure the mechanisms of the Internet, including each of the relevant tasks as set forth in the *Cyberspace Strategy*. Please include a description of processes by which DHS will identify, and will establish timetables for addressing, emerging threats to, and vulnerabilities of, the Internet.

e. What benchmarks has DHS established for measuring its success in securing the mechanisms of the Internet? If DHS has not established such benchmarks, please provide a timetable, including final deadlines, for doing so.

The report on hardening the Internet, made at the January 2004 session of the National Infrastructure Advisory Council (NIAC) (a partnership of industry executives and government officials), was full of hope but little progress. The responsible working group was "just getting started" and had not even met yet, according to its chairman, but said he expected to produce a full report by the summer of this year.[16]

f. To what extent does NIAC's lack of progress on hardening the Internet reflect DHS's own lack of progress on this subject, and to what extent has DHS made greater progress that the private-sector members of NIAC are not aware of or privy to?

g. How is NIAC's working group on hardening the Internet being coordinated with any similar work being undertaken by task forces convened at the National Cyber Security Summit in December 2003?

2. Fostering Secure Digital Control and Monitoring Systems. Many industries increasingly rely on digital control and monitoring systems, called DCS/SCADA systems, to control large processes, such as power plants, refineries, and chemical plants, and dispersed assets such as electrical lines, water systems, railroads, and gas pipelines. (Digital Control Systems (DCS) are used for single facilities, and Supervisory Control and Data Acquisition (SCADA) Systems are used for dispersed assets.) In October 1997, the President's Commission on Critical Infrastructure Protection stated that "the widespread and increasing use of SCADA systems for control of energy systems provides increasing

[16] "Cyber Security: Council Officials Discuss Progress On Information Sharing" *National Journal's Technology Daily* (http//nationaljournal.com) January 16, 2004.

ability to cause serious damage and disruption by cyber means." Control systems have already been subject to a number of cyber attacks, including attacks on a sewage treatment system in Australia in 2000 and, more recently, on a nuclear power plant in Ohio.[17] GAO has stated that attacks on control systems "could have devastating consequences, such as endangering public health and safety; damaging the environment; or causing a loss of production, generation, or distribution of public utilities."[18]

To secure DCS/SCADA systems, the *Cyberspace Strategy* provides that: DHS, in coordination with the Energy Department and other concerned agencies, and in partnership with industry, will *(a)* develop best practices and new technology to increase security of control systems, *(b)* determine the most critical DCS/SCADA-related sites, and *(c)* develop a prioritized plan for short-term cybersecurity improvements in those sites. No interim steps, deadlines, and benchmarks for success in securing DCS/SCADA systems are included in the *Strategy*. (Page 32.)

a. What steps has DHS taken to coordinate with the Energy Department and other concerned agencies to establish partnership with the private companies and municipalities that operate DCS/SCADA systems?

b. Are the taskforces established at the National Cyber Security Summit addressing the security of DCS/SCADA systems? If so, how is the work of those taskforces being coordinated with the efforts of the partnerships established with the operators of DCS/SCADA systems?

c. What steps to secure DSC/SCADA systems have been completed?

d. Please provide a timetable, including final deadlines, for securing DCS/SCADA systems, including a timetable for completing each of the relevant tasks as set forth in the *Cyberspace Strategy*. Please include a description of processes by which DHS will identify, and will establish timetables for addressing, emerging threats to, and vulnerabilities of, DCS/SCADA systems.

e. What benchmarks has DHS established for measuring its success in securing DCS/SCADA systems? If DHS has not established such benchmarks, please provide a timetable, including final deadlines, for doing so.

[17] *Critical Infrastructure Protection: Challenges in Securing Control Systems* (GAO-04-140T) October 1, 2003 Page 2.

[18] *Id.*

3. Reducing and Remediating Software Vulnerabilities. The *Cyberspace Strategy* includes: *(1)* DHS will work with the National Infrastructure Advisory Council and private sector organizations to develop an optimal means by which software vulnerabilities may be disclosed; and *(2) (a)* GSA will work with DHS on an improved method for testing an implementing a clearinghouse for testing patches for use by the federal government, and *(b)* DHS will share lessons learned and encourage development of a voluntary national effort to develop a similar clearinghouse for other sectors. The *Strategy* also provides that the software industry "is encouraged to consider" promoting more secure installation and implementation of their products. No interim steps, deadlines, and benchmarks for success in reducing and remediating software vulnerabilities are included in the *Strategy*.

   a. What steps has DHS taken to work with NIAC and other organizations to develop optimal means for the disclosure of vulnerabilities?

   b. What steps has DHS taken, working with GSA, on establishing a patch clearinghouse, and what steps has DHS taken in sharing lessons learned and encouraging similar methods in other sectors?

   c. Please provide a timetable, including a final deadline, for completing these tasks.

   d. What benchmarks has DHS established for measuring its success?

   The *Strategy* also provides that the software industry "is encouraged to consider" promoting more secure installation and implementation of their products. In fact, one of the taskforces established at the Summit has an even broader mandate, being responsible for considering how to improve patching and configuration of software and how to build more secure software.

   e. What guidance is DHS providing to the task force to enable the task force to fulfill national security priorities?

   The December 2003 National Cyber Security Summit, sponsored by IT vendor associations, reportedly did not invite companies that develop Linux software, so that Linux companies were not included in the working groups, at least initially. (Linux, a non-proprietary operating system whose source-code is freely available to anyone, is emerging as a substantial alternative to the proprietary Microsoft and Unix operating systems.)

   f. Were Linux developer companies included in the Summit, and, if not, why? What plans does DHS have to include Linux developer companies in the public-private partnership the Department is relying on to develop cybersecurity plans and recommendations?

g. In the highly competitive technology industry, what generally is DHS's strategy to assure that its information-sharing and other partnership arrangements with certain companies and trade-associations does not unfairly disadvantage other companies or industry sectors that are not included or represented in these arrangements?

Comprehensive Assessment and Reduction of Vulnerabilities

The *Cyberspace Strategy* recognizes that securing the Internet and DCS/SCADA systems and generally upgrading software security, while valuable, are far from sufficient to secure various computer-dependent sectors against attacks on information infrastructure, and that comprehensive planning and action are necessary. The *Strategy* calls on DHS to: *(a)* in coordination with appropriate agencies and the private sector, to lead in the development and conduct of a national threat assessment to identify the impact of possible attacks on a variety of targets, *(b)* establish and lead a public-private partnership to identify cross-sectoral interdependencies, both cyber and physical, and to develop plans to reduce related vulnerabilities, and *(c)* support these efforts by having the National Infrastructure Simulation and Analysis Center develop models to identify the impact of cyber and physical interdependencies. No interim steps, deadlines, and benchmarks for success in performing this planning are included in the *Strategy*. (Pages 29, 34.)

Moreover, the Department has an even more comprehensive responsibility to assess and reduce cybersecurity vulnerabilities as part of its obligation to develop a comprehensive critical infrastructure protection plan, as originally envisioned in PDD-63, assigned to the Department, in the Homeland Security Act, and recently recast in HSPD-7. All infrastructure sectors are increasingly dependent on the Internet and other telecommunications networks and associated computing assets, as well as on internal information infrastructures.[19] Accordingly, the protection of information resources against cyber and physical attack must be fully integrated into all aspects of the critical infrastructure protection plan. It was stated at the National Infrastructure Advisory Council (NIAC) meeting on January 13, 2004, that the Department expected to have available by February 2004 a "matrix" of current programs underway or completed for assessing the vulnerabilities and protective measures of critical infrastructures to cyber attacks. In other words, it has taken year since issuance of the *Cybersecurity Strategy* for the Department to merely compile a list of what work is underway.

[19] See National Academy of Engineering / National Research Council, *Critical Information Infrastructure Protection and the Law: an Overview of Key Issues* 2003 Page 8.

1. What progress has the Department made toward conducting a comprehensive national threat assessment to identify the impact of possible cyber attacks on a variety of targets, as required in the *Cyberspace Strategy*? Has the matrix referred to at the January 2004 NIAC meeting been completed? What steps have been completed, what steps remain to be completed, and what is the timetable for their completion?

2. What progress has the Department made toward identifying cross-sectoral interdependencies, both cyber and physical, and developing plans to reduce related vulnerabilities, as required in the *Cyberspace Strategy*? What steps have been completed, what steps remain to be completed, and what is the timetable for their completion?

3. What progress has the Department made toward developing comprehensive goals, objectives, milestones, and key initiatives for protection of information infrastructure as an integral part of the National Plan for Critical Infrastructure and Key Resources Protection mandated by December 17, 2004, under HSPD-7? What steps have been completed, what steps remain to be completed, and what is the timetable for their completion?

NIAC includes a working group on ranking the vulnerabilities in cyberspace, which seems to be making uncertain progress. According to the working group's report at NIAC's January 2004 meeting, the group has "had trouble coming to a consensus" and has actually given up on the effort to build a model to rank vulnerabilities, determining instead to only create hypothetical scenarios.[20]

4. To what extent does NIAC's lack of progress on ranking and prioritizing cybersecurity vulnerabilities reflect DHS's own lack of progress on this subject, and to what extent has DHS made greater progress which NIAC is not aware of or privy to?

B. **<u>Cybersecurity Incident Analysis, Warning, and Response.</u>** Under PDD-63, the federal government established a program to establish a national warning and information sharing system to facilitate the rapid sharing of information among all information infrastructure sectors about actual and possible intrusions and viruses, indicators of impending cyber attacks, and the means of defending against them. Moreover, since 1988, the Defense Department has funded the establishment at Carnegie Mellon University of the CERT Coordination Center (CERT/CC) to coordinate communications during security emergencies and to help administer programs to develop and widely distribute security practices and evaluation methods that together enable organizations to protect their systems against current

[20] "Cyber Security: Council Officials Discuss Progress On Information Sharing" *National Journal's Technology Daily* (http//nationaljournal.com) January 16, 2004.

and emerging threats. HSA consolidated into the new Department several key federal cybersecurity operations centers, to create a focal point enabling the Department to monitor and respond to cybersecurity incidents within its own systems and, to the extent coordination is established with private sector organizations, incidents in non-federal infrastructure sectors; and in September 2003, the Department entered into partnership with Carnegie Melon's CERT/CC to create a new centralized computer emergency response team called US-CERT. The stated goals of US-CERT are: to improve warning and response to incidents, facilitate communication of response information across all infrastructure centers, develop and distribute new security tools and methodologies to detect and reduce vulnerabilities.[21]

1. What will be the relationship between US-CERT and the continuing role of CERT/CC? How will DHS partner with the private sector for computer attack detection and response?

2. A prime stated goal of US-CERT is to improve warning and response times and generally to increase the flow of critical security information throughout the Internet community. What metrics does the Department apply to measure its performance, and what benchmarks and timetables has it established to measure its success?

3. The success of US-CERT will depend on the willingness of organizations of non-federal infrastructure sectors to participate by promptly supplying information about cybersecurity incidents. However, reports indicate a significant reluctance by some sectors to share information with a federal entity like US-CERT. For example, the director of a partnership of IT vendors and users has written that the DHS concept is based on a "faulty, weak legacy" because companies are reluctant to belong to formal government-sponsored information-sharing organizations because of fears that proprietary data would not be protected. He wrote of DHS's expectation that the private sector will join with their data: "There is no chance of this happening. . . . The continuing failure of DHS to understand these basic [privacy] requirements is distressing."[22] Moreover, John Pescatore, a leading cybersecurity expert with the Gartner Group, has stated that one reason companies are reluctant to share their proprietary information is that the government's own inadequate computer security puts proprietary information at risk;[23] and it seems likely that the poor status of DHS's own

[21] http://www.us-cert.gov/capabilities.html

[22] "Cybersecurity Consortium Gets Insurer's Backing" *Computerworld* (http//www.computerworld.com) October 20, 2003.

[23] "Cybersecurity Debate Heats Up" *Computerworld* (http//www.computerworld.com)

(continued...)

computer security, as described in Congressional oversight reports, is likely to further erode confidence.

a. What has been US-CERT's success in gaining the necessary cooperation from non-federal participants? What metrics does the Department apply to measure this participation, and what benchmarks and timetables has it established to measure its success?

b. What steps is the Department taking to reassure potential participants in its US-CERT information-sharing program that proprietary information will be secured?

4. In addition to creating a single point-of-contact such as US-CERT, the National Strategy stated that the federal government would complete the installation of the Cyber Warning and Information Network (CWIN) to key government cybersecurity-related network operations, and would explore linking CWIN to private-sector information sharing and analysis centers.

a. What is the status of efforts to install CWIN to government network operations?

b. What is the status of linking CWIN to private-sector centers?

c. How will US-CERT coordinate with CWIN in crisis management for cyberspace?

The working group responsible for devising ways to share information among companies, part of the NIAC, gave a report at its January 2004 meeting indicating the great amount of work remaining to be done in this area. According to news reports, the head of the working group stated: "Everyone understands the need for information sharing, but we haven't defined to whom and for what purpose," including whether companies not affiliated with critical infrastructure should see cyber alerts at all.[24]

5. To what extent does NIAC's lack of progress in defining the key elements of inter-company information-sharing, including to whom and for what purpose information should be shared, reflect DHS's own lack of progress on this subject, and to what extent has DHS made greater progress that the private-sector members of NIAC is not aware of or privy to?

[23] (...continued)
December 12, 2003.

[24] "Cyber Security: Council Officials Discuss Progress On Information Sharing" *National Journal's Technology Daily* (http//nationaljournal.com) January 16, 2004.

6. Who within government or the private sector will decide what companies should, and what companies should not, receive cyber alerts generated by the federal government or with its assistance or cooperation, and how can DHS assure that those decisions are made without improper competitive impact upon companies excluded from access to this vital information?

7. On March 18, 2004, the National Cyber Security Partnership issued tentative recommendation for on cybersecurity early warning, including the creation by year-end of an Early Warning Alert Network to enable prompt and reliable distribution of information and crisis communications among business and government entities, and the establishment by 2006 of a National Crisis Coordination Center to share threat and vulnerability data within and among different industries. What is DHS's schedule for evaluating, responding to, and, if appropriate, implementing these recommendations?

C. <u>Continuity and Contingency Planning.</u> Contingency planning is an essential part of cybersecurity. Without adequate planning and training, critical sectors of the economy and vital governmental services may not be able to withstand a cyber-related attack. PDD-63 in 1998 and the *National Plan* in 2000 stated national policy that the federal government must establish measures for the continuity and recovery of its own operations during a cyber attack and should work with critical infrastructure sectors to ensure that their continuity and recovery plans address information attack as well. The 2003 *National Strategy* assigned to DHS the responsibility of coordinating the development of cybersecurity contingency plans involving industry, and for working with state and local governments to encourage their IT security programs. As to federal government agencies, OMB is responsible for overseeing agencies' contingency planning, but DHS is expected to conduct exercises to test civilian agencies' contingency planning and to explore coordination of public and private incident management, response, and recovery capabilities.

1. Has a plan for recovering Internet functions in case of a cyber attack been completed? If not, please provide a timetable, including a final deadline, for completion of this plan, and a schedule for periodic updates of this plan.

2. For each sector of critical infrastructure identified in the *Cyberspace Strategy* and the recent HSPD 7, what is the status of the Department's efforts to coordinate the development of cybersecurity contingency plans? Please provide a timetable, including a final deadline, for completion of these plans, and a schedule for periodic updates of such plans.

3. Does DHS have any program underway to work with state and local governments in developing contingency plans for continuity of state and local government services in case of cyber attack? If so, please describe the program, and please provide a timetable,

including final deadlines, for completion of these plans, and a schedule for periodic updates of such plans.

D. **Cybersecurity Awareness and Training.** The *National Cyberspace Strategy* describes the importance of promoting comprehensive national awareness to enable all sectors – businesses, government, the general workforce, and the general population – to maintain the security of computer systems for which they are responsible. DHS is assigned key responsibilities in this area, including: working with other organizations to facilitate a comprehensive awareness campaign (pages 38 - 41), and implementing and encouraging the establishment of programs to advance training of cybersecurity professionals and to develop security professional certification programs (pages 41 - 42).

1. What progress has the Department made towards facilitating the comprehensive education and awareness campaign described in the *Strategy*? What steps have been completed, what steps remain to be completed, and what is the timetable for their completion?

2. What progress has the Department made towards implementing and encouraging the establishment of security professional certification programs as described in the *Strategy*? What steps have been completed, what steps remain to be completed, and what is the timetable for their completion?

3. On March 18, 2004, the National Cyber Security Partnership issued tentative recommendation for on cybersecurity education and awareness programs. What is DHS's schedule for evaluating, responding to, and, if appropriate, implementing these recommendations?

E. **Privacy Protection.** Several aspects of a cybersecurity program can raise concerns about whether personal privacy will be adequately protected. For example, the monitoring of the Internet and other telecommunications networks for indication of security incidents as part of the security response system can raise privacy concerns if the monitoring entity can review the content of the communications being monitored. Technology that protects against intrusions, when cast too broadly, might profile innocent activity.[25] Moreover, the voluntary sharing of non-public information by carriers and other operators of critical infrastructure, which may be necessary to cybersecurity threats and vulnerabilities, can also raise the potential for violations of privacy if personal information is shared. Like the 2000 *National Plan for Information Systems Protection* that preceded it, the *Cyberspace Strategy* recognizes these privacy concerns and states that, in developing cybersecurity programs, "care must be taken to respect privacy interests" and asserts that, as part of the strategy to

[25] *National Plan for Information Infrastructure Protection* 2000 Page vii.

secure cyberspace, the DHS privacy officer will consult regularly with privacy advocates and others to ensure consideration of privacy issues in development of the security response system. (Pages 14, 15, 20). More generally, the *Strategy* promises: "The federal government will continue to regularly meet with privacy advocates to discuss cybersecurity and the implementation of this Strategy." (Page 54.)

1. What consultation has the privacy officer undertaken with privacy advocates and others, and what consultation is planned, to ensure consideration of privacy issues in development of the security response system? Please identify the privacy advocates and experts, the dates on which consultation has taken place or is planned, and subject matter of the consultation, and how the views of the privacy advocates and experts have been, or are planned to be, taken into consideration in development of the security response system?

2. What design features of the security response system being developed and implemented by the Department ensure the protection of personal privacy?

3. In addition to what is described in answer to the foregoing questions regarding the security response system, what other consultation have DHS or other agencies undertaken, and what consultation is planned, with privacy advocates and experts as part of implementing the overall *Cyberspace Strategy*? Please identify the privacy advocates and experts, the dates on which consultation has taken place or is planned, and subject matter of the consultation, and how the views of the privacy advocates and experts have been, or are planned to be, taken into consideration by the federal government.

F. <u>Research and Development.</u>

Vigorous and carefully prioritized research and development must be an important part of our national cybersecurity effort. For example, new technologies will be needed to modernize and secure the Internet and telecommunications networks for future growth and advanced applications. Improved best-practices and methodologies are needed to evaluate and improve the security of both new and existing software and systems. Emerging technologies must be evaluated so that their security implications are understood and addressed.

DHS has several key responsibilities in coordinating and implementing a national research and development agenda for cybersecurity. While the Director of the Office of Science and Technology Policy (OSTP) has overall responsibility for coordinating the development of the federal government's cybersecurity R&D agenda, the *National Cyberspace Strategy* assigns DHS the lead responsibility for ensuring coordination and cooperation of R&D

among academia, industry, and the government. (Pages 34-35.) The *Strategy* specified no steps, timetables, or benchmarks for measuring success towards achieving these goals.

Moreover, the Department's Science and Technology Directorate has committed itself to a significant R&D agenda, including the development of a DHS cybersecurity R&D center to support the operational needs of the Department's Information Analysis and Infrastructure Protection (IAIP) Division in protecting critical infrastructure. As envisioned by the Department, this new center would enable partnerships with academia, private industry, and national laboratories, thereby bridging the gap between critical infrastructure companies and research-and-developers. Based on these partnerships, the center would develop strategic R&D programs and create testing and evaluation programs to address specific gaps in U.S. cybersecurity capabilities.[26]

Unfortunately, this critical cybersecurity R&D Center apparently remains more promise than reality. Although the DHS Under Secretary for Science and Technology Dr. Charles E. McQueary testified in May 2003 that the Center would be established through Fiscal Year 2003 funding, this vitally important initiative has yet to be established.[27]

1. Coordination with non-federal R&D; Establishment of Cybersecurity R&D Center. The Cyberspace Strategy provides that, to further cybersecurity, DHS will ensure that adequate mechanisms exist for coordination of R&D among academia, industry, and government. (Page 35.) Moreover, Dr. McQueary has stated that the planned DHS Cyber Security Research and Development Center would "enable partnerships with academia, private industry and national laboratories," would "accomplish technology transfer to the companies with specific needs," and would "engage the critical infrastructure companies through mechanisms such as industry associations and

[26] Statement of Dr. Charles McQueary, Under Secretary, Science and Technology Directorate, DHS, before the House Science Committee May 14, 2003; Answers by Dr. McQueary to post-hearing questions, before the House Science Committee (http//commdocs.house.gov/committees/science/hsy86992.000/hsy86992_0f.htm) May 14, 2003, pages 44-45, 158. "House Committee Wants Data on Cyber R&D Funds" *Government Computer News* (http//www.gcn.com) May 26, 2003.

[27] Presentation by Simon Szykman, Director, DHS Cyber Security R& D, at Georgia Institute of Technology "ATI 2004" workshop (http//gtisc.gatech.edu/ati2004/ppt/Szykman_ATI.ppt) January 21-23, 2004; "Homeland Security Science Division Will Also Tackle Cybersecurity" *National Journal's Technology Daily* (http//www.govexec.com) December 4, 2003.

consortia, bridging the gap and connecting companies and researchers and developers as required."[28]

a. What steps has DHS taken to ensure that adequate mechanisms exist for coordination of R&D among academia, industry, and government?

b. Please provide a timetable, including final deadlines, for establishing the Cyber Security R&D Center and for implementing its programs.

2. Facilitation of Public-Private Effort to Improve Software Development. According to the Cyberspace Strategy, DHS is responsible for facilitating "a national public-private effort to promulgate best practices and methodologies that promote integrity, security, and reliability in software development." (Page 35.)

a. What steps has DHS taken towards facilitating the promulgation of such best practices and methodologies?

b. Task forces were established at the Cybersecurity Summit on "Best Practices and Standards: Technical Standards and Common Criteria," and on "Security Across the Software Development Life Cycle: Secure Software." To what extent are these task forces charged with responsibility for promulgating best practices and methodologies for secure software, or to what extent will the task forces at least contribute to such an effort?

c. Please provide a timetable, including a final deadline, for the promulgation of safe software best practices and methodologies.

d. What benchmarks has DHS established for measuring its success in facilitating the promulgation of such best practices and methodologies? If DHS has not established such benchmarks, please provide a timetable, including final deadlines, for doing so.

3. Ensuring that Emerging Technologies Are Periodically Reviewed within the National Science and Technology Council. A key responsibility of DHS in the Cybersecurity Strategy is, in coordination with OSTP and other agencies, to facilitate communications among research and security communities to ensure that emerging technologies are

[28] Answers by Dr. Charles McQueary, Under Secretary, Science and Technology Directorate, DHS, to post-hearing questions, before the House Science Committee (http//commdocs.house.gov/committees/science/hsy86992.000/hsy86992_0f.htm) May 14, 2003. Page 158.

periodically reviewed by the appropriate body within the National Science and Technology Council, to consider implications for cybersecurity (and homeland security) and for the federal research agenda. (Page 35.)

a. What steps has DHS taken to facilitate the communications necessary to ensure review of emerging technologies?

b. What, if any, particular emerging technologies have undergone such review as a result of DHS's efforts? What technologies does DHS anticipate will undergo such review?

4. DHS's Cybersecurity Research and Development Program. The Director of DHS's cybersecurity R&D program has stated that a short-term priority is to execute the top R&D cybersecurity priorities of the IAIP Directorate.[29]

a. What are the top cybersecurity R&D priorities of the IAIP Directorate?

b. Please provide a timetable, including a final deadline, for the completion of each of those R&D priorities.

Another short-term R&D priority of the Department is to fulfill R&D research requirements for other operational divisions of the Department, such as the Coast Guard, the Secret Service, and the Transportation Security Administration. However, at least as of early December 2003, it was reported that these divisions had failed to define their cybersecurity requirements.[30]

c. What, if any, cybersecurity R&D requirements have been defined by operational divisions of the Department other than the IAIP Directorate?

d. Please provide a timetable, including a final deadline, for the completion of those R&D priorities.

e. Please provide a timetable, including a final deadline, for other divisions of the Department to complete the task of defining their cybersecurity R&D requirements.

[29] Presentation by Simon Szykman, Director, DHS Cyber Security R& D, at Georgia Institute of Technology "ATI 2004" workshop (http//gtisc.gatech.edu/ati2004/ppt/Szykman_ATI.ppt) January 21-23, 2004.

[30] "Homeland Security Science Division Will Also Tackle Cybersecurity" *National Journal's Technology Daily* (http//www.govexec.com) December 4, 2003.

I look forward to your responses to these questions. Please feel free to have your office contact Larry Novey of my staff at (202) 224-2627 if you have any questions.

Sincerely,

Joseph I. Lieberman
Ranking Member