March 20, 2003

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 too little action has been taken to permanently safeguard the nation's critical infrastructure and key assets and to urge you to step up efforts to secure these infrastructures. Though much lip service has been given to the importance of protecting our critical infrastructure – our financial, transportation and communications networks, our energy systems and water supplies, chemical plants and hazardous materials, emergency services and public health systems, in short those systems essential to the country's economy, national security, and public safety – actual progress appears to have been exceedingly slow. Few of the tasks necessary to identify, assess, and protect core infrastructures and assets appear yet to have been accomplished, and experts believe that in many ways our critical infrastructure – 85 percent of which is under the control of the private sector – remains as vulnerable today to intentional disruption as it was before the September 11, 2001 attacks. Unfortunately, the Administration's recently released *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* – despite its name – fails to provide a forceful strategy for securing these infrastructures.

As you know, this is not a new issue. As early as 1996, Congress, through that year's Defense Department Authorization Bill, required that the President report to Congress on a national policy to protect the nation's information infrastructure from attack. That same year, President Clinton established the President's Commission on Critical Infrastructure Protection ("PCCIP"), which the following year released a report that laid out an initial strategy for action. Building on the PCIIP's report, President Clinton issued Presidential Decision Directive No. 63 ("PDD-63") in May 1998. PDD-63 set forth a goal of achieving the ability to protect the nation's critical infrastructure from intentional 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, under PDD-63, each critical infrastructure sector was assigned to a lead agency that was given responsibility for working with private sector representatives to develop a protection plan for that sector. The recommendations for protection of each sector were ultimately to be used to build a National Infrastructure Assurance Plan. Version 1.0 of such a plan, focusing primarily on cyberspace protections within the federal government, 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. The Governmental Affairs Committee held a series of hearings in the fall and winter of 2001-02 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 information, 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 (OHS) 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. . . ." The *National Strategy for Homeland Security* issued by OHS in July 2002 further emphasized the importance of this endeavor, identifying the protection of critical infrastructures and key assets as one of six critical mission areas. And the priority of protecting critical infrastructure is codified in the Homeland Security Act, which provides for an Under Secretary for Information Analysis and Infrastructure Protection in the new Department of Homeland Security (DHS) and gives this individual the specific responsibility to "carry out comprehensive assessments of the vulnerabilities of the key resources and critical infrastructure of the United States, including the performance of risk assessments to determine the risks posed by particular types of terrorist attacks within the United States."

Thus, I was very troubled to see that, after all the planning efforts that have gone before and the very real threat under which we remain, the *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereinafter, "*Physical Protection Strategy*") issued on February 14, 2003, still speaks only in the broadest and vaguest generalities as to what must be done to protect the country's critical infrastructure and key assets. Nowhere does this document list any specific actions to be taken to identify, assess, and protect critical infrastructures or provide any timetable for accomplishing these tasks. Instead, the document relies on self-evident platitudes about the importance of building partnerships and glowing promises about what DHS intends to do in the future. Vague goals stand in for any specific action plan. At this late date, such an approach is inadequate.

Indeed, evidence abounds of the immediate need for action in any number of areas. According to a recent report by the Brookings Institution, for example, the Environmental Protection Agency has identified 123 U.S. plants that store toxic chemicals which, if released, could endanger one million people or more (the Surgeon General has suggested that casualties could be even higher). At the same time, the *Physical Protection Strategy* itself acknowledges that "there is currently no clear, unambiguous legal or regulatory authority at the federal level to help ensure comprehensive, uniform security standards for chemical plants," and that "a significant percentage of companies that operate major hazardous chemical facilities do not abide by voluntary security codes developed by other parts of the industry."

A report issued last fall by the Council on Foreign Relations' Task Force chaired by former Senators Gary Hart and Warren B. Rudman provides another example of this sort of vulnerability, pointing out that "an adversary intent on disrupting America's reliance on energy need not target oil fields in the Middle East. The homeland infrastructure for refining and distributing energy to support the daily lives of Americans remains largely unprotected from sabotage." The report notes that some of this infrastructure lies offshore in the Gulf of Mexico, on the continental shelf and within the territories of our North American neighbors, and "a coordinated attack on several key pumping stations – most of which are in remote areas, are not staffed, and possess no intrusion-detection devices – could cause mass disruption" to oil flows.

And in a February 16, 2003 Op-Ed in the *Washington Post,* Fred Millar, a member of the D.C. Local Emergency Planning Commission, highlights the vulnerability of our transportation systems, noting that the release of material from a single ammonia tank truck in a populated area could cause a disaster on the scale of the one that occurred in Bhopal, India and that the chlorine gas from a single 90-ton rail tank car could release a toxic cloud more than 40 miles long. Despite these hazards, Mr. Millar reports that only 26 people had by then been hired by the Transportation Security Administration to address truck and rail security.

I am therefore requesting a complete account of the Administration's efforts to protect our nation's critical infrastructure and to evaluate its vulnerabilities. Please provide me with the following information by April 3, 2003:

A. Asset Inventory

1. The *National Strategy for Homeland Security* identifies thirteen sectors of critical infrastructure: agriculture; food; water; public health; emergency services; government; the defense industrial base; information and telecommunications; energy; transportation; banking and finance; chemicals and hazardous materials; and postal and shipping. It also identifies five categories of key assets (*i.e.,* assets that may not be vital to continuity of critical services at the national level, but the attack on which could result in significant loss of life and property or, because of their symbolic power, substantial damage to national morale and confidence): national monuments and icons; nuclear power plants; dams; government facilities; and commercial key assets. For each critical infrastructure sector and each key asset category, please provide the following information:

    a. Has an inventory to identify the critical assets and systems of this sector, or the key assets of this category, been undertaken?

    b. If so, has the inventory been completed?

    c. If an inventory has been undertaken but not completed, what is the status of that inventory?

d. If no asset inventory has been undertaken, is one planned? If no asset inventory is planned for this sector or category, please explain why not.

e. Please provide a timetable, including a final deadline, for completion of the inventory.

2. Plans from PDD-63 to the *Physical Protection Strategy* agree that there must ultimately be a national compilation of critical infrastructures across all sectors and an assessment of their vulnerabilities. Please provide a timetable for when a comprehensive, cross-sector asset inventory will be completed.

3. Many states and localities are conducting their own inventories of the critical assets within their jurisdictions. How are federal inventories being coordinated with those that may be occurring at the state and local level? Have you obtained, or do you plan to obtain, information from states and localities about those assets they have identified as critical infrastructure or key assets? Have you provided, or do you plan to provide, DHS's asset inventories in a given jurisdiction to state or local authorities within that jurisdiction?

B. Vulnerability Assessment

1. For each critical infrastructure sector and each key asset category, please provide the following information:

a. Have vulnerability assessments been undertaken for assets in this sector or category?

b. If so, have these assessments been completed?

c. If vulnerability assessments have been undertaken but not completed, what is the status of those assessments? What proportion of the sector's or category's assets have been evaluated thus far?

d. If vulnerability assessment have not been undertaken, are ones planned? If no vulnerability assessments are planned, please explain why not.

e. Please provide a timetable, including a final deadline, for completion of the vulnerability assessments.

2. Please provide a timetable for completion of a comprehensive, cross-sector vulnerability assessment.

3. How are federal vulnerability assessments being coordinated with any state and local assessments? How will information about vulnerability assessments be shared between the federal government and state and local authorities?

C. Risk Assessment

1. For each critical infrastructure sector and each key asset category, please provide the following information:

   a. Have risk assessments been undertaken for this sector or category?

   b. If so, have the assessments been completed?

   c. If risk assessments have been undertaken but not completed, what are the status of those assessments?

   d. If risk assessments have not been undertaken, are they planned? If no risk assessment is planned, please explain why not.

   e. Please provide a timetable, including a final deadline, for completion of the risk assessments.

2. Please provide a timetable for completion of a comprehensive, cross-sector risk assessment.

3. How are federal risk assessments being coordinated with any state and local assessments? How will information about risk assessments be shared between the federal government and state and local authorities?

D. Protective Measures

1. For each critical infrastructure sector and each key asset category, please provide the following information:

   a. Based on what you have learned thus far in assessing the risks and vulnerabilities in this sector or category, what measures have been taken to protect or reduce the vulnerabilities of this sector's or category's critical infrastructure and key assets?

   b. Please provide a timetable, including final deadlines, for the completion of:
      i. A plan for protective action in this sector or category
      ii. Implementation of that plan

2. Please provide a timetable for completion of a comprehensive, cross-sector plan for protective action to reduce the vulnerabilities of critical infrastructure and key assets.

3. How are federal protective measures plans being coordinated with any state and local governments?

E. Heightened Alert Status

1. When the national threat alert level is raised to "orange," as it was last month and was again this week, what are the specific additional steps taken to secure critical infrastructure and key assets? Please describe the steps taken for each critical infrastructure sector and each key asset category.

2. If specific additional steps are not taken in any sector or category in response to the recently elevated threat level, please explain why not.

3. When the threat alert level is raised to "orange," what do DHS or others in the federal government do to ensure that relevant private sector entities take adequate measures to protect critical infrastructure and key assets? To what extent, if any, do DHS or others in the federal government monitor, direct, or assess private sector actions?

F. Reliance on the Private Sector

As noted above, it has been estimated that 85 percent of the United States' critical infrastructure, as well as many of its key assets, are privately owned. A terrorist attack on private property may well impose costs beyond the mere loss of that property to its owner, either directly – *e.g.,* injuries to other individuals caused by the malicious use of hazardous materials stolen from a private facility – or indirectly – *e.g.,* the symbolic loss to the nation of an important commercial landmark. Nonetheless, the *National Strategy for Homeland Security* appears to conclude that, in most instances, free market forces are sufficient to ensure that these private sector assets are adequately safeguarded. Thus, for example, the *National Strategy for Homeland Security* states that "[p]rivate businesses and individuals have incentives to take on expenditures to protect property and reduce liability that contribute to homeland security," and that "[p]roperly functioning insurance markets should provide the private sector with economic incentives to mitigate risks," presumably because businesses that take additional measures to protect against attack would be eligible for lower insurance rates.

A January 2003 report from the Brookings Institution observes, however, that "[p]rivate markets will often not provide adequate protection against terrorist attack on their own, since individual citizens and businessmen tend to worry more about the immediate challenge of making a profit than about the extremely unlikely possibility that their properties and facilities will be attacked" – a point underscored by a recent survey by the Council on Competitiveness

that found that 92 percent of surveyed executives of the nation's largest companies did not see their companies as potential terrorism targets and that only 53 percent reported spending more on security. Moreover, even though the Terrorism Risk Insurance Act, which mandated that insurers make terrorism insurance coverage available, was passed in November 2002, recent articles in both the *Washington Post* (February 25, 2003) and the *New York Times* (March 8, 2003), reported that only a small minority of commercial policy holders apparently have thus far chosen to buy such insurance. This may in part be the result of the fact that the cost of such insurance (which is not regulated by the new law) can be prohibitively high. In addition, businesses, including small businesses, may not have expertise in homeland security matters and may need guidance from the federal government or others with that expertise as to the appropriate actions they need to take to effectively protect the infrastructure and assets under their control. Accordingly, please provide the following information:

1. What is the basis for concluding that in many cases, the free market will adequately assure that private parties provide sufficient security for critical infrastructure and key assets? Please identify those areas where you believe that free market forces are most likely to be sufficient.

2. The *National Strategy for Homeland Security* observes that "[g]overnment should fund only those homeland security activities that are not supplied, or are inadequately supplied, in the market." How do you intend to identify those activities that are being adequately supplied in the market and those that are not? Have you already done so? If not, when do you expect such an analysis to be completed?

3. The *Physical Protection Strategy* acknowledges that "[t]he private sector may also require incentives to stimulate investment." In what areas do you believe that the private sector will "require incentives" to invest in physical security for critical infrastructure? What form should such incentives take? How do you plan to assess the level of incentives required to achieve adequate security? What incentives, if any, are you planning to propose be adopted?

4. The Environmental Protection Agency's (EPA's) top aide for homeland security recently was quoted as follows: "We've been concerned since 9-11 about the vulnerability of chemical sites as possible targets for attack." In addition, a GAO report released this week (GAO–03-439) notes that chemical facilities may be attractive targets for terrorists and that the release of certain chemicals can pose a grave threat to the surrounding population. GAO nonetheless finds that that there are no federal laws which explicitly require an owner of a chemical facility to assess its vulnerabilities or take steps to protect the facility and, moreover, that, while some federal departments may have provided some assistance to industry in preparedness effort, "no agency monitors or documents the extent to which chemical facilities have implemented security measures." As a result, the GAO report concludes, despite voluntary efforts on the part of industry, "the extent of security preparedness at U.S. chemical facilities is unknown."

a. In an October 6, 2002 letter to the *Washington Post,* you and EPA Administrator Christine Todd Whitman, wrote that chemical facilities "must be required" to perform comprehensive vulnerability assessments and act to reduce those vulnerabilities and that "[v]oluntary efforts alone are not sufficient to provide the level of assurance Americans deserve." Do you continue to believe that "voluntary efforts alone are not sufficient" in addressing the vulnerabilities of hazardous chemical facilities? What requirements would you impose on the owners of chemical facilities in order to reduce the vulnerabilities of such facilities? Does the Administration intend to submit a legislative proposal to Congress that would implement such requirements? If so, when?

b. In what areas other than hazardous chemical facilities do you believe that "voluntary efforts alone are not sufficient"? What requirements do you propose to impose in these areas?

5. To the extent that it has been left to private owners to determine whether and how to protect critical infrastructure or key assets, will DHS or others in the federal government monitor or evaluate the adequacy of those efforts? If so, please describe how such monitoring and/or evaluation will be accomplished.

G. Nuclear Weapons Facilities

1. In a March 14, 2002 letter from Secretary of Energy Spencer Abraham to the Director of the Office of Management and Budget (OMB), Secretary Abraham requested $379.7 million to better secure the nation's nuclear weapons facilities. In the letter, Secretary Abraham notes that the Energy Department stores "vast amounts of materials that remain highly volatile and subject to unthinkable consequences if placed in the wrong hands" at a variety of sites, and warns that "[f]ailure to support these urgent security requirements is a risk that would be unwise." Nonetheless, OMB turned down the bulk of the request, supporting only $26.4 million for additional security efforts. Since that letter, what, if anything, has been done to provide increased protection for the extremely dangerous nuclear materials stored at Energy Department sites? What role will DHS play in ensuring that such materials are adequately secured?

2. In a follow-up letter to OMB, the Energy Department's CFO explains that the Department was told that it could not get additional security funding until a revised "Design Basis Threat," a document outlining the basis for physical security measures, was completed. Has this document now been completed? If not, what measures are being taken in the interim to protect those sites where nuclear weapons are designed, built and stockpiled? If so, has the requested additional funding, or any part thereof, now been provided?

I look forward to your responses on these issues. Please feel free to contact Beth Grossman of my staff at (202) 224-9256 if you have any questions.

Sincerely,

Joseph I. Lieberman
Ranking Member