EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

June 17, 2004

M-04-15

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: Development of Homeland Security Presidential Directive (HSPD) - 7 Critical Infrastructure Protection Plans to Protect Federal Critical Infrastructures and Key Resources

On December 17th, 2003, the President signed HSPD-7, "Critical Infrastructure Identification, Prioritization and Protection" (Attachment A). This HSPD supersedes Presidential Decision Directive/NSC-63 of May 22, 1998, "Critical Infrastructure Protection", and establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

HSPD-7 instructed Federal departments and agencies (agencies) to prepare plans for protecting physical and cyber critical infrastructure and key resources (CI/KR), owned or operated, including leased facilities by July 31, 2004. OMB has been working with agencies on this requirement and agency Chief Information Officers received official distribution of draft guidance on April 27, 2004. This memorandum, developed in consultation with the Homeland Security Council (HSC) and the Department of Homeland Security (DHS), includes the required format for agencies to use when submitting internal critical infrastructure protection (CIP) plans. Pursuant to the guidance provided herein, these plans must address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities. In particular, planning must include protection priorities, the agency's ability to ensure continuity of business operations during a physical or cyber attack, and, where current capabilities are lacking, plans of action and milestones to achieve the necessary level of performance.

Upon submission, security plans will be subject to an interagency review coordinated by DHS. The goals of these reviews include ensuring consistent planning and protection of Federal CI/KR across the Federal government. DHS will prepare a written evaluation of each agency's physical security plan and provide that evaluation within 120 days of the agency's submission of the plan. Agency cyber security plans will be reviewed in a manner consistent with reviews of cyber security reports submitted under the Federal Information Security Management Act and current guidance. These efforts will inform DHS' efforts to develop the National Infrastructure Protection Plan, as it will provide the data for a more detailed analysis of CI/KR. DHS' planning effort will outline the methodology for determining what government facilities are priorities for protection.

Agencies are requested to submit internal CIP plans utilizing the reporting instructions contained in Attachment B. A consolidated plan must be prepared at the Departmental or "parent" agency level and cover all agency sub-elements to the extent they own or operate critical infrastructures or key resources. The July 31, 2004 report must be submitted by the Deputy Secretary or equivalent official.

Agencies will soon receive additional instructions regarding the means for securely transmitting these internal CIP plans. At a minimum, agency-specific information in the internal CIP plans should be safeguarded as sensitive and should receive the full measure of protection afforded by Exemption 2 of the Freedom of Information Act, 5 U.S.C. sec. 552, if an agency ever receives a FOIA request for such information. Further background material on FOIA Exemption 2 is contained in the Department of Justice's FOIA Update, Vol. X, No. 3, at 3-4 (Protecting Vulnerability Assessments Through Application of Exemption Two"), which is available at http://www.usdoj.gov/oip/foia_updates/Vol_X_3/page3.html

Agencies should refer to the classification standards contained in Executive Order No. 12958 "Classified National Security Information" to determine whether information contained in the internal CIP plan is classified. Section 1.5 of the Executive Order contains classification categories that include:

> United States Government programs for safeguarding nuclear materials or facilities; or vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security

Questions concerning the attached reporting instructions should be referred to Kim Johnson, of OMB's Office of Information and Regulatory Affairs' Information Policy and Technology Branch at (202) 395-7232 or Kim_A._Johnson@omb.eop.gov.

Attachments:

A) HSPD-7 "Critical Infrastructure Identification, Prioritization and Protection"
B) Format of Internal Department/Agency CIP Plans

Directive on Critical Infrastructure Identification, Prioritization, and Protection

December 17, 2003

Homeland Security Presidential Directive/ HSPD–7

Subject: Critical Infrastructure Identification, Prioritization, and Protection

Purpose

(1) This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

Background

(2) Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence.

(3) America's open and technologically complex society includes a wide array of critical infrastructure and key resources that are potential terrorist targets. The majority of these are owned and operated by the private sector and State or local governments. These critical infrastructures and key resources are both physical and cyber-based and span all sectors of the economy.

(4) Critical infrastructure and key resources provide the essential services that underpin American society. The Nation possesses numerous key resources, whose exploitation or destruction by terrorists could cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction, or could profoundly affect our national prestige and morale. In addition, there is critical infrastructure so vital that its incapacitation, exploitation, or destruction, through terrorist attack, could have a debilitating effect on security and economic well-being.

(5) While it is not possible to protect or eliminate the vulnerability of all critical infrastructure and key resources throughout the country, strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur. In addition to strategic security enhancements, tactical security improvements can be rapidly implemented to deter, mitigate, or neutralize potential attacks.

Definitions

(6) In this directive:

(a) The term ''critical infrastructure'' has the meaning given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

(b) The term ''key resources'' has the meaning given that term in section 2(9) of the Homeland Security Act of 2002 (6 U.S.C. 101(9)).

(c) The term ''the Department'' means the Department of Homeland Security.

(d) The term ''Federal departments and agencies'' means those executive departments enumerated in 5 U.S.C. 101, and the Department of Homeland Security; independent establishments as defined by 5 U.S.C. 104(1); Government corporations as defined by 5 U.S.C. 103(1); and the United States Postal Service.

(e) The terms ''State,'' and ''local government,'' when used in a geographical sense, have the same meanings given to those terms in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101).

(f) The term ''the Secretary'' means the Secretary of Homeland Security.

(g) The term ''Sector-Specific Agency'' means a Federal department or agency responsible for infrastructure protection activities in a designated critical infrastructure sector or key resources category. Sector-Specific Agencies will conduct their activities under this directive in accordance with guidance provided by the Secretary.

(h) The terms ''protect'' and ''secure'' mean reducing the vulnerability of critical infrastructure or key resources in order to deter, mitigate, or neutralize terrorist attacks.

Policy

(7) It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could:

(a) cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction;

(b) impair Federal departments and agencies' abilities to perform essential missions, or to ensure the public's health and safety;

(c) undermine State and local government capacities to maintain order and to deliver minimum essential public services;

(d) damage the private sector's capability to ensure the orderly functioning of the economy and delivery of essential services;

(e) have a negative effect on the economy through the cascading disruption of other critical infrastructure and key resources; or

(f) undermine the public's morale and confidence in our national economic and political institutions.

(8) Federal departments and agencies will identify, prioritize, and coordinate the protection of critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit them. Federal departments and agencies will work with State and local governments and the private sector to accomplish this objective.

(9) Federal departments and agencies will ensure that homeland security programs do not diminish the overall economic security of the United States.

(10) Federal departments and agencies will appropriately protect information associated with carrying out this directive, including handling voluntarily provided information and information that would facilitate terrorist targeting of critical infrastructure and key resources consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

(11) Federal departments and agencies shall implement this directive in a manner consistent with applicable provisions of law, including those protecting the rights of United States persons.

Roles and Responsibilities of the Secretary

(12) In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources.

(13) Consistent with this directive, the Secretary will identify, prioritize, and coordinate the protection of critical infrastructure and key resources with an emphasis on critical infrastructure and key resources that could be exploited to cause catastrophic health effects or mass casualties comparable to those from the use of a weapon of mass destruction.

(14) The Secretary will establish uniform policies, approaches, guidelines, and methodologies for integrating Federal infrastructure protection and risk management activities within and across sectors along with metrics and criteria for related programs and activities.

(15) The Secretary shall coordinate protection activities for each of the following critical infrastructure sectors: information technology; telecommunications; chemical; transportation systems, including mass transit, aviation, maritime, ground/surface, and rail and pipeline systems; emergency services; and postal and shipping. The Department shall coordinate with appropriate departments and agencies to ensure the protection of other key resources including dams, government facilities, and commercial facilities. In addition, in its role as overall cross-sector coordinator, the Department shall also evaluate the need for and coordinate the coverage of additional critical infrastructure and key resources categories over time, as appropriate.

(16) The Secretary will continue to maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission. The organization's mission includes analysis, warning, information sharing, vulnerability reduction, mitigation, and aiding national recovery efforts for critical infrastructure information systems. The organization will support the Department of Justice and other law enforcement agencies in their continuing missions to investigate and prosecute threats to and attacks against cyberspace, to the extent permitted by law.

(17) The Secretary will work closely with other Federal departments and agencies, State and local governments, and the private sector in accomplishing the objectives of this directive.

Roles and Responsibilities of Sector-Specific Federal Agencies

(18) Recognizing that each infrastructure sector possesses its own unique characteristics and operating models, there are designated Sector-Specific Agencies, including:

(a) Department of Agriculture—agriculture, food (meat, poultry, egg products);

(b) Health and Human Services—public health, healthcare, and food (other than meat, poultry, egg products);

(c) Environmental Protection Agency—drinking water and water treatment systems;

(d) Department of Energy—energy, including the production refining, storage, and distribution of oil and gas, and electric power except for commercial nuclear power facilities;

(e) Department of the Treasury—banking and finance;

(f) Department of the Interior—national monuments and icons; and

(g) Department of Defense—defense industrial base.

(19) In accordance with guidance provided by the Secretary, Sector-Specific Agencies shall:

(a) collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector, including with key persons and entities in their infrastructure sector;

(b) conduct or facilitate vulnerability assessments of the sector; and

(c) encourage risk management strategies to protect against and mitigate the effects of attacks against critical infrastructure and key resources.

(20) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance.

(21) Federal departments and agencies shall cooperate with the Department in implementing this directive, consistent with the Homeland Security Act of 2002 and other applicable legal authorities.

Roles and Responsibilities of Other Departments, Agencies, and Offices

(22) In addition to the responsibilities given the Department and Sector-Specific Agencies, there are special functions of various Federal departments and agencies and components of the Executive Office of the President related to critical infrastructure and key resources protection.

(a) The Department of State, in conjunction with the Department, and the Departments of Justice, Commerce, Defense, the Treasury and other appropriate agencies, will work with foreign countries and international organizations to strengthen the protection of United States critical infrastructure and key resources.

(b) The Department of Justice, including the Federal Bureau of Investigation, will reduce domestic terrorist threats, and investigate and prosecute actual or attempted terrorist attacks on, sabotage of, or disruptions of critical infrastructure and key resources. The Attorney General and the Secretary shall use applicable statutory authority and attendant mechanisms for cooperation and coordination, including but not limited to those established by presidential directive.

(c) The Department of Commerce, in coordination with the Department, will work with private sector, research, academic, and government organizations to improve technology for cyber systems and promote other critical infrastructure efforts, including using its authority under the Defense Production Act to assure the timely availability of industrial products, materials, and services to meet homeland security requirements.

(d) A Critical Infrastructure Protection Policy Coordinating Committee will advise the Homeland Security Council on interagency policy related to physical and cyber infrastructure protection. This PCC will be chaired by a Federal officer or employee designated by the Assistant to the President for Homeland Security.

(e) The Office of Science and Technology Policy, in coordination with the Department, will coordinate interagency research and development to enhance the protection of critical infrastructure and key resources.

(f) The Office of Management and Budget (OMB) shall oversee the implementation of government-wide policies, principles, standards, and guidelines for Federal government computer security programs. The Director of OMB will ensure the operation of a central Federal information security incident center consistent with the requirements of the Federal Information Security Management Act of 2002.

(g) Consistent with the E-Government Act of 2002, the Chief Information Officers Council shall be the principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, operation, sharing, and performance of information resources of Federal departments and agencies.

(h) The Department of Transportation and the Department will collaborate on all matters relating to transportation security and transportation infrastructure protection. The Department of Transportation is responsible for operating the national air space system. The Department of Transportation and the Department will collaborate in regulating the transportation of hazardous materials by all modes (including pipelines).

(i) All Federal departments and agencies shall work with the sectors relevant to their responsibilities to reduce the consequences of catastrophic failures not caused by terrorism.

(23) The heads of all Federal departments and agencies will coordinate and cooperate with the Secretary as appropriate and consistent with their own responsibilities for protecting critical infrastructure and key resources.

(24) All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

Coordination with the Private Sector

(25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:

(a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and

(b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.

National Special Security Events

(26) The Secretary, after consultation with the Homeland Security Council, shall be responsible for designating events as ''National Special Security Events'' (NSSEs). This directive supersedes language in previous presidential directives regarding the designation of NSSEs that is inconsistent herewith.

Implementation

(27) Consistent with the Homeland Security Act of 2002, the Secretary shall produce a comprehensive, integrated National Plan for Critical Infrastructure and Key Resources Protection to outline national goals, objectives, milestones, and key initiatives within 1 year from the issuance of this directive. The Plan shall include, in addition to other Homeland Security-related elements as the Secretary deems appropriate, the following elements:

(a) a strategy to identify, prioritize, and coordinate the protection of critical infrastructure and key resources, including how the Department intends to work with Federal departments and agencies, State and local governments, the private sector, and foreign countries and international organizations;

(b) a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources;

(c) a summary of initiatives for sharing critical infrastructure and key resources information and for providing critical infrastructure and key resources threat warning data to State and local governments and the private sector; and

(d) coordination and integration, as appropriate, with other Federal emergency management and preparedness activities including the National Response Plan and applicable national preparedness goals.

(28) The Secretary, consistent with the Homeland Security Act of 2002 and other

applicable legal authorities and presidential guidance, shall establish appropriate systems, mechanisms, and procedures to share homeland security information relevant to threats and vulnerabilities in national critical infrastructure and key resources with other Federal departments and agencies, State and local governments, and the private sector in a timely manner.

(29) The Secretary will continue to work with the Nuclear Regulatory Commission and, as appropriate, the Department of Energy in order to ensure the necessary protection of:

(a) commercial nuclear reactors for generating electric power and non-power nuclear reactors used for research, testing, and training;

(b) nuclear materials in medical, industrial, and academic settings and facilities that fabricate nuclear fuel; and

(c) the transportation, storage, and disposal of nuclear materials and waste.

(30) In coordination with the Director of the Office of Science and Technology Policy, the Secretary shall prepare on an annual basis a Federal Research and Development Plan in support of this directive.

(31) The Secretary will collaborate with other appropriate Federal departments and agencies to develop a program, consistent with applicable law, to geospatially map, image, analyze, and sort critical infrastructure and key resources by utilizing commercial satellite and airborne systems, and existing capabilities within other agencies. National technical means should be considered as an option of last resort. The Secretary, with advice from the Director of Central Intelligence, the Secretaries of Defense and the Interior, and the heads of other appropriate Federal departments and agencies, shall develop mechanisms for accomplishing this initiative. The Attorney General shall provide legal advice as necessary.

(32) The Secretary will utilize existing, and develop new, capabilities as needed to model comprehensively the potential implications of terrorist exploitation of vulnerabilities in critical infrastructure and key resources, placing specific focus on densely populated areas. Agencies with relevant modeling capabilities shall cooperate with the Secretary to develop appropriate mechanisms for accomplishing this initiative.

(33) The Secretary will develop a national indications and warnings architecture for infrastructure protection and capabilities that will facilitate:

(a) an understanding of baseline infrastructure operations;

(b) the identification of indicators and precursors to an attack; and

(c) a surge capacity for detecting and analyzing patterns of potential attacks.

In developing a national indications and warnings architecture, the Department will work with Federal, State, local, and non-governmental entities to develop an integrated view of physical and cyber infrastructure and key resources.

(34) By July 2004, the heads of all Federal departments and agencies shall develop and submit to the Director of the OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans shall address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

(35) On an annual basis, the Sector-Specific Agencies shall report to the Secretary on their efforts to identify, prioritize, and coordinate the protection of critical infrastructure and key resources in their respective sectors. The report shall be submitted within 1 year from the issuance of this directive and on an annual basis thereafter.

(36) The Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs will lead a national security and emergency preparedness communications policy review, with the heads of the appropriate Federal departments and agencies, related to convergence and next generation architecture. Within 6 months after the issuance of this directive, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall submit for my consideration any recommended changes to such policy.

(37) This directive supersedes Presidential Decision Directive/NSC–63 of May 22, 1998 (''Critical Infrastructure Protection''), and

any Presidential directives issued prior to this directive to the extent of any inconsistency. Moreover, the Assistant to the President for Homeland Security and the Assistant to the President for National Security Affairs shall jointly submit for my consideration a Presidential directive to make changes in Presidential directives issued prior to this date that conform such directives to this directive.

(38) This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

George W. Bush

Attachment B

Format of Internal Department/Agency CIP Plan

Agencies shall use the following definitions to identify Critical Infrastructure and Key Resources:

Critical Infrastructure and Key Resources

Under the Homeland Security Act, which references the definition in the PATRIOT Act, the term '**critical infrastructure'** (CI) means "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The term 'key resources' (KR) means "publicly or privately controlled resources essential to the minimal operations of the economy and government."

These definitions are broad and must remain so, to provide an appropriate degree of flexibility to the federal agencies and departments, state and local governments, and the private sector. This flexibility will enable these stakeholders to use their informed judgment in planning for the protection of critical infrastructure and key resources. To ensure consistency, this guidance provides more detailed descriptions of certain terms to assist agencies in developing and implementing their plans.

An **infrastructure** is a collection of assets. As used in this document, an **asset** is something of importance or value, and can include people, property (both tangible and intangible), information, systems, and equipment. A **system,** which is one type of asset, is a collection of resources made up of any combination of people, physical attributes (e.g., location, structure, etc.), or cyber components that perform a process.

Key resources represent individual targets whose destruction could cause large-scale injury, death, or destruction of property and /or profound damage to our national prestige and confidence. Key resources include such facilities as nuclear power plants, dams, government facilities, and commercial facilities.

An infrastructure is considered **critical**, or resource is considered **key,** if its destruction or damage causes significant impact on the security of the nation– national economic security, national public health, safety, psychology, or any combination.

An infrastructure or resource is considered **mission critical** if its damage or destruction would have a debilitating impact on the ability of the organization to perform its essential functions and activities.

The terms **protect** and **secure**, as defined in HSPD-7, mean reducing the vulnerability of CI/KR by deterring, mitigating, or neutralizing terrorist attacks. Thus, as used in this guidance,

protection includes all activities to identify CI/KR, assess vulnerabilities, prioritize CI/KR, and develop protective programs and measures, since these activities lead to the final act of implementing such protective strategies to reduce vulnerability. **Protective actions** include detection mechanisms or programs (e.g. surveillance systems that indicate a potential threat), deterrence actions (e.g., enhanced security that reduces the aggressor's likelihood of success and interest in the target); defensive actions (e.g., physical hardening or buffer zones, that prevent or delay an attack); and actions that reduce the value or incentive to an aggressor to attack (e.g., creating redundancies in a system and recovery programs that minimize consequences). Strategies for response and recovery are also important.

Format of July 31, 2004 reports

Departments/Agencies should provide one report that speaks to enterprise-wide priorities and mission.

Part I. Describe existing capability, to include current personnel and budget, for protecting Federal critical infrastructure and key resources

Note: In order to meet the objectives of these internal CIP plans, Departments and Agencies should first focus attention on identifying and reporting their current capabilities to protect critical infrastructure and key resources that they own or operate. Thereafter, D/As should develop and implement plans to close any gaps in current capabilities. OMB will not be able to approve internal CIP plans until all information is provided.

1. Background and introduction:
   - summary of the primary business functions and activities of the D/A;
   - summary of management structure of the organization, including responsibilities for internal CI/KR protection, information security, physical security, personnel security, and continuity of operations programs and activities;
   - summary of the locations and assets (including contractor assets) that support the primary business functions and activities of the organization.

2. Identify current capabilities for protecting internal CI/KR, covering the following activities:

   - Ability to identify Federally owned or operated (to include leased) CIR/KR assets
   - Ability to assess the vulnerabilities and interdependencies among assets
   - Ability to prioritize among Federal assets based on vulnerability, consequence, and threat information;
   - Overall capability to adequately protect against threats to Federal CI/KR assets;
   - Overall capability to respond to, and recover from, events that impair the ability to perform mission critical functions at or using Federal CI/KR assets .
   - Ability to identify gaps in carrying out any of the activities discussed above.

3. Please identify the process for determining budget and personnel requirements for CI/KR protection, response, and reconstitution activities. Does the D/A's FY04 appropriation and FY05 budget request include specific programs to protect the D/A's critical infrastructure? D/As should use the attached table to identify their CIP activities by appropriation account, along with their FY04 enacted and FY05 proposed resource levels. Attachment C includes funding levels for Critical Infrastructure Protection programs reported in the FY 2005 Homeland Security and Overseas Combating Terrorism Database and as part of the overall budget data collected in support of the FY 2005 budget development via MAX A-11. Your response to this memorandum must be consistent with the data submitted in previous collections. Small and

independent agencies may not have previously provided OMB with funding levels for CIP programs. For additional information, please see the note below:

Program/ Activity Name	Account Name	OMB Account Code	FY 2004 Enacted	FY 2005 Request

NOTE: Section 25.5 of OMB Circular A-11 (along with separate instructions) requires agencies to submit activity-level information for homeland security activities. This includes agency reporting on critical infrastructure protection activities and the broader *National Strategy for Homeland Security* Protecting Critical Infrastructure and Key Assets (PCKIA) mission area. In your July response to this memorandum, program and funding data should be consistent with the data that your agency reported in response to A-11. For example, your agency does not have to report every activity included in its A-11 response -- in fact, it should not, because those responses include activities focused outside the agency -- but for the activities that are included in response to both requests, the funding estimates should be the same. Your detailed response to A-11 for the FY06 Budget should include the set of activities provided in response to this memorandum, consistent funding estimates, and detailed activity level data.

4.Describe the process for ensuring independent oversight of CIP programs. Discuss whether the GAO or IG has conducted a review of CIP programs. If so, when were these reviews conducted? Were corrective actions identified and follow on actions taken by the Department/agency? Are corrective actions for IT systems considered critical infrastructure included in Federal Information Security Management Act (FISMA) plans of action and milestones?

Part II: List CI/KR owned or operated by the Department/Agency and Long Term Protection Strategy

Note: If Departments and agencies are not able to collect and report on the information requested below by July 31st, please provide anticipated timeframes for providing this information.

1. Please attach the prioritized list of internal Department/agency critical infrastructure and key resources. (Prioritization should be conducted based on an analysis and normalization of the risk data – i.e. vulnerability and consequences. See DHS' Guidance for Developing Sector-Specific Plans, Chapter 4 language on "Assessing Vulnerabilities and Prioritizing Assets")

2. Has the Department/agency developed a long term protective strategy to protect the critical infrastructure and key resources identified above and coordinated sufficiently with other entities, where applicable? Has the IG reviewed this plan? If so, when did this review occur? If weaknesses in the plan were identified, have corrective actions been taken? (See DHS' Guidance for Developing Sector-Specific Plans, Chapter 4 language on "Process for Developing Protective Programs")

3. Has the agency designed and implemented performance metrics for the CIP program? If so, please provide a copy of the metrics. Activities should be measured both by outputs and by outcomes. Agencies should use the metrics as a basis for improving program activities and reallocating resources as needed. (See DHS' Guidance for Developing Sector-Specific Plans, Chapter 4 language on "Measuring Progress")

4. Describe the status of all major initiatives that are underway or planned for addressing deficiencies including:
   - Improvements to capability to protect critical infrastructure and key resources;
   - Improvements to capability to respond to and recover from events that impair the ability to perform organization essential functions by using critical infrastructure or key resources

5. Indicate milestones for the initiatives described above. Provide the name of the assigned manager and target date for completing each milestone.

6. Are there specific management, technical, or operational challenges that must be overcome with regard to implementation of the Department/agency's CIP plan? How will the agency address these challenges?