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?