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

June 17, 2004

THE DIRECTOR

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been working with agencies on this requirement and agency Chief Information Officers received official distribution of draft guidance on April 27, 2004.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
C) Department/Agency Funding Levels for Critical Infrastructure Protection Per FY 2005 Homeland Security and Overseas Combating Terrorism Database