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

THE DIRECTOR

July 15, 2011

M-11-27

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jacob J. Lew
Director

SUBJECT: Implementing the Telework Enhancement Act of 2010: Security Guidelines

President Obama signed into law the Telework Enhancement Act of 2010 (the Act; Public Law 111-292) on December 9, 2010, to improve telework across the Federal government. As part of its telework program, each agency must ensure that adequate information and security protections for information and information systems are used while teleworking. This memorandum provides guidelines on security requirements for the implementation of the Act, as required by 5 U.S.C. § 6504(c).

Telework provides multiple benefits for the Federal government, including resource savings, improved sustainability, employee recruitment and retention, as well as supporting the continuity of operations. With the passage of the Act, more Federal workers will soon begin to work from home or at shared government spaces to improve productivity, reduce the overhead costs and real estate footprint of the Federal government, and continue to deliver timely services to the public.

Telework leverages innovative technologies to allow Federal employees to work from any location to improve productivity, assure continuity of operations, and respond to the changing needs of the workforce. Some Federal agencies are testing effective telework models found in the private sector, such as "hoteling" stations. These stations provide laptop connections and can double or triple the number of workers in a work space; this maximizes space, reduces costs, and should be applied government-wide whenever possible.

The Administration has set up central resources across agencies that provide guidance and best practices for effective telework management, implementation, and monitoring. [1] The Office of Personnel Management (OPM) has recently issued a *Guide to Telework in the Federal Government.* [2] OPM, in collaboration with each agency, will compile and submit an annual report on the telework programs of each agency, beginning with the first report submitted 18 months after enactment of the law (June 2012), and annually thereafter.

---

[1] http://www.telework.gov
[2] http://www.telework.gov/guidance_and_legislation/telework_guide/telework_guide.pdf

Telework also provides Federal employees the ability to continue working during inclement weather, emergencies, or situations that may disrupt normal operations. However, telework is only as effective as the technologies used to support it, which is why it is critical for agencies to take immediate action to ensure that their employees are properly equipped.

If not properly implemented, telework may introduce new information security vulnerabilities into agency systems and networks. To prevent security incidents, agencies are responsible under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347; 44 U.S.C. § 3541-49) to provide protection for information and information systems commensurate with risk. Agencies must continue to follow Office of Management and Budget (OMB) policies, National Institute of Standards and Technology (NIST) standards and guidelines, and Department of Homeland Security (DHS) security reporting requirements. NIST has issued standards and guidelines to assist with the protection of remote devices; agencies should refer to NIST's security telework site for more information (http://csrc.nist.gov/telework).

Agencies are expected to implement security telework policies to best suit their unique needs. At a minimum, agency policies must comply with FISMA requirements and address the following:

- controlling access to agency information and information systems;
- protecting agency information (including personally identifiable information) and information systems;
- limiting the introduction of vulnerabilities;
- protecting information systems not under the control of the agency that are used for teleworking;
- safeguarding wireless and other telecommunications capabilities that are used for teleworking; and
- preventing inappropriate use of official time or resources that violates subpart G of the Standards of Ethical Conduct for Employees of the Executive Branch by viewing, downloading, or exchanging pornography, including child pornography.

Agency chief information officers (CIOs) must identify a technical point of contact to DHS (FISMA.FNS@dhs.gov) to aid with the implementation of telework security requirements. This point of contact will serve as a technical manager and must have operational and technical expertise to implement the Act within the agency.

Please direct questions on the security requirements referenced in this memo to the Cybersecurity Performance Management Office, Federal Network Security Branch, DHS at FISMA.FNS@dhs.gov or 703-235-5045. For NIST-policy related questions, please email telework@nist.gov.