M-99-20

June 23, 1999

M-99-20

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM:Jacob J. Lew
DirectorSUBJECT:Security of Federal Automated Information Resources

A number of agencies have recently experienced the intentional disruption of their Internet website operations. The impact of these disruptions has ranged from minor nuisance to significant interruption of service.

The purpose of this memorandum is to remind agencies that, consistent with the principles embodied in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," they must continually assess the risk to their computer systems and maintain adequate security commensurate with that risk. Therefore, as soon as practicable, please conduct a review of your security practices to ensure that you have in place a process that permits program officials and security managers to understand the risk to agency systems and take necessary steps to mitigate it. This process should include specific procedures to ensure the timely implementation of security patches for known vulnerabilities, especially for those systems that are accessible via the Internet. Installing such patches is a proven way of avoiding disruptions to systems. Please report back to me within 90 days on your agency's process along with the name of the official responsible for its implementation.

There are a number of security resources available to assist agencies in meeting their security responsibilities. Under the Computer Security Act of 1987, the National Institute of Standards and Technology (NIST) is responsible for issuing specific guidance to agencies regarding security controls for unclassified systems. A complete collection of that guidance, may be found at NIST's Computer Security Resources Clearinghouse website (http://csrc.nist.gov). Among other issuances, NIST's Information Technology Laboratory (ITL) produces a periodic bulletin that provides up-to- date, thoroughly researched information on significant security issues. The subject of the May 1999 bulletin is especially timely -- computer attacks and prevention measures.

An important security resource for agencies maintaining externally accessible systems is GSA's Federal Incident Response Capability (FedCIRC). FedCIRC issues security advisories and offers free baseline services such as incident response and other, fee-based services such as on-site recovery

and audit trail analysis. Additional information on FedCIRC's activities is available at their website (http://www.fedcirc.gov).

To assist agencies in complying with Circular A-130, Appendix III, I encourage each agency to avail themselves of NIST's and GSA's expertise in this important area and ensure that the ITL Bulletin and GSA's advisories are widely distributed throughout each agency and recommended actions are pursued as appropriate.

Please direct any questions your staff might have on this memorandum to Glenn Schlarman. He may be reached at 202-395-3514 or gschlarm@omb.eop.gov.