Federal Chief Information Officers Council

Executive Committee

Chair
Sally Katzen

Vice Chair
James Flyzik

Capital Planning and IT Management Chairs

Joseph Leo
Daryl White

Federal IT Workforce Chairs

Gloria Parker
Ira Hobbs

Enterprise Interoperability and Emerging IT Chairs

Lee Holcomb
Edwin Levine

Outreach Chairs

David Borland
Paul Brubaker
Marty Wagner

Security, Privacy and Critical Infrastructure Chairs

Fernando Burbano
John Gilligan
Laura Callahan
Roger Baker

E-Government Chairs

George Molaski
John Dyer
Alan Balutis

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: CHIEF INFORMATION OFFICERS COUNCIL
SALLY KATZEN, CHAIR & Deputy Director for Management, OMB
JAMES FLYZIK, VICE CHAIR & CIO, TREASURY

SUBJECT: Federal Information Technology Security Assessment Framework

The Chief Information Officers (CIO) Council's Federal Information Technology (IT) Security Assessment Framework provides a method for agency officials to determine the current status of their security programs relative to existing requirements and, where necessary, to establish a target for improvement. Consistent with Office of Management and Budget (OMB) policy, agencies must implement and maintain programs to adequately secure their information and system assets. This Framework was developed in cooperation by the CIO Council's Security, Privacy, and Critical Infrastructure Committee with OMB, and the National Institute of Standards and Technology (NIST). It is based upon requirements found in OMB's security policies, the General Accounting Office's Federal Information System Controls Audit Manual, and NIST's recommended security practices.

The attached Framework comprises five levels to guide agency assessment of their security status and assist in prioritizing efforts for improvement. A companion to the Framework, a NIST prepared self-assessment questionnaire, will provide specific questions that identify the control criteria against which agencies can determine the security status of an asset, a program, and the entire agency. This questionnaire will be issued early next year.

The importance of assessing the effectiveness of programs and security controls is key to achieving and maintaining adequate security. In fact, the recently enacted Government Information Security Reform Act, part of the FY 2001 Defense Authorization Act (P.L. 106-398), requires annual agency program reviews and Inspector General audits of information security programs and practices. Together with upcoming guidance on implementing the new Act, the Framework and forthcoming questionnaire will assist agencies in performing these reviews.

http://www.cio.gov
ciocouncil.support@gsa.gov

We recommend agencies allow sufficient time, at least six months, to perform assessments in light of these new reporting requirements. Questions on the Framework or the upcoming NIST questionnaire should be directed to Marianne Swanson, (301) 975-3293, marianne.swanson@nist.gov.

Sally Katzen
Chair, CIO Council

Jim Flyzik
Vice Chair, CIO Council

Attachment