07/03/2003

To: CIO-COUNCIL

Subject: [CIOCL] Note from OMB re: Guidance on Certification and Accreditation

NOTE TO CHIEF INFORMATION OFFICERS

FROM: MARK FORMAN
ADMINISTRATOR, OFFICE OF E-GOVERNMENT AND IT

SUBJECT: GUIDANCE TO ASSIST AGENCIES WITH CERTIFICATION AND ACCREDITATION EFFORTS

One essential step toward securing the Federal government's operations and assets is the full certification and accreditation of all systems. Both existing systems and new systems (prior to becoming operational) must be certified and accredited.

This guidance is designed to assist agencies with their certification and accreditation efforts and leverages the annual IT security review work conducted with the NIST Self-Assessment Tool. This guidance also aligns with the upcoming NIST guidance (800-37) on certification and accreditation.

As you know, certification and accreditation of systems is monitored for major systems through the budget process (as reported in agency's business cases). Operational IT systems are considered "at-risk" if they are not fully certified and accredited. Additionally, certification and accreditation of all systems (major and other) is tracked via performance measures through the annual Federal Information Security Management Act report.

Please contact Kamela White, kgwhite@omb.eop.gov, with any questions.

Certification and Accreditation – What an Agency Can Do Now

As NIST works to finalize its new guideline on certification and accreditation, many agencies are asking for interim guidance to address the OMB Circular A-130, Appendix III requirement and Federal Information Security Management Act (FISMA) policy compliance requirement for a management official to authorize operation of an information system based on implementation of its system security plan. This requirement, commonly referred to as *accreditation*, is based on a review of the management, operational, and technical security controls in an information system. This evaluation or certification, made in support of the security accreditation, helps assess the effectiveness of the security controls. The FISMA agency annual reports are due in September; however, the NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," is not expected to be finalized until December 2003. Therefore, provided below is a synopsis of the major C&A activities, which have been divided into four phases, that agencies should implement to comply with the OMB Circular A-130 C&A requirement.

Initiation Phase:
A certification review occurs after the risks to the system have been assessed, the security plan has been developed and approved, and the security controls are implemented and tested. The development of the system security plan implies that all sections contained in NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems" are adequately covered and readily identifiable. The need for determining the sensitivity of the information (risk level) as it relates to high, medium, and low needs for the confidentiality, integrity and availability of the data, a contingency plan, incident response plan, etc. are required sections in NIST SP 800-18 and must be part of the system security plan. Agencies will find the draft of *Standards for Security Categorization of Federal Information and Information Systems* (draft Federal Information Processing Standard 199) helpful in determining sensitivity levels. (See http://csrc.nist.gov/publications/drafts.html). A certification review is the last step after all of the above activities are completed and approved by agency management. A diagram is attached depicting the major information system security activities that occur during the system development life cycle.

Security Certification Phase:
The certification review should contain sufficient supporting documentation describing what has been tested and the results of the tests. If the test results identify security controls requiring implementation or modification, a plan of action and milestone (POA&M) documenting the security controls to be implemented must be developed as well. Agencies may also use another certification review methodology provided the set of requirements covered in 800-26 are addressed. Security controls that are implemented imply that the security control has reached level 3 (implementation) of 800-26. Until NIST SP 800-37 is finalized, we advise agencies if they have a low risk General Support System (GSS) (that means all applications residing on the GSS are low risk too or the application borders are adequately protected) a self assessment using the questions in NIST SP 800-26, "Security Self-Assessment Guide for Information Technology

Systems" is considered an adequate certification review. All other system types and risk levels must have an independent review using the questions in 800-26 or consistent with the questions in 800-26. The table below provides a synopsis of the types of certification reviews required for each system type and risk level.

Type of Certification Reviews

System Type	Low Risk	Medium Risk	High Risk
General Support System	*self-assessment or independent review*	*independent review*	*independent review*
Major Application	*independent review*	*independent review*	*independent review*

Security Accreditation Phase:
The certification documentation must contain proof that the activities contained in the questions in NIST 800-26, Appendix A, Section 4. Authorize Processing (Certification & Accreditation have been accomplished. The certification documentation or a subset of the information is presented to the authorizing management official for accreditation, interim accreditation, or no accreditation. The authorizing official is the senior management official or executive with the authority to approve the operation of the information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation) or agency assets. Through security accreditation, the authorizing official assumes responsibility and is accountable for the risks of operating the information system in a specific environment. The authorizing official must have the authority to oversee the budget and business operations of the information systems within the agency and is often called upon to approve security requirements documents, security plans, memorandums of agreement (MOA), memorandums of understanding (MOU), and any authorized or allowable deviations from security policies.

Continuous Monitoring Phase (formally Post Accreditation Phase):
FISMA requires assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency. Each MA and GSS requires oversight and monitoring of the security controls in the information system on an ongoing basis until the need for security reaccreditation occurs, either because of specific changes to the information system (event-driven) or because of Federal or agency policies requiring reauthorization of the information system at a specified timeframe.

There are numerous C&A process related steps that are not included in this brief synopsis but must still be addressed. If an agency ensures their C&A program addresses at a minimum the items mentioned above, then there will be easy alignment when NIST SP 800-37 is finalized. The guidelines provided in FIPS 102, "Guideline for Computer Security Certification and Accreditation" provides an abundance of guidance on the many steps of a comprehensive C&A program. It can be used until NIST SP 800-37 is finalized.

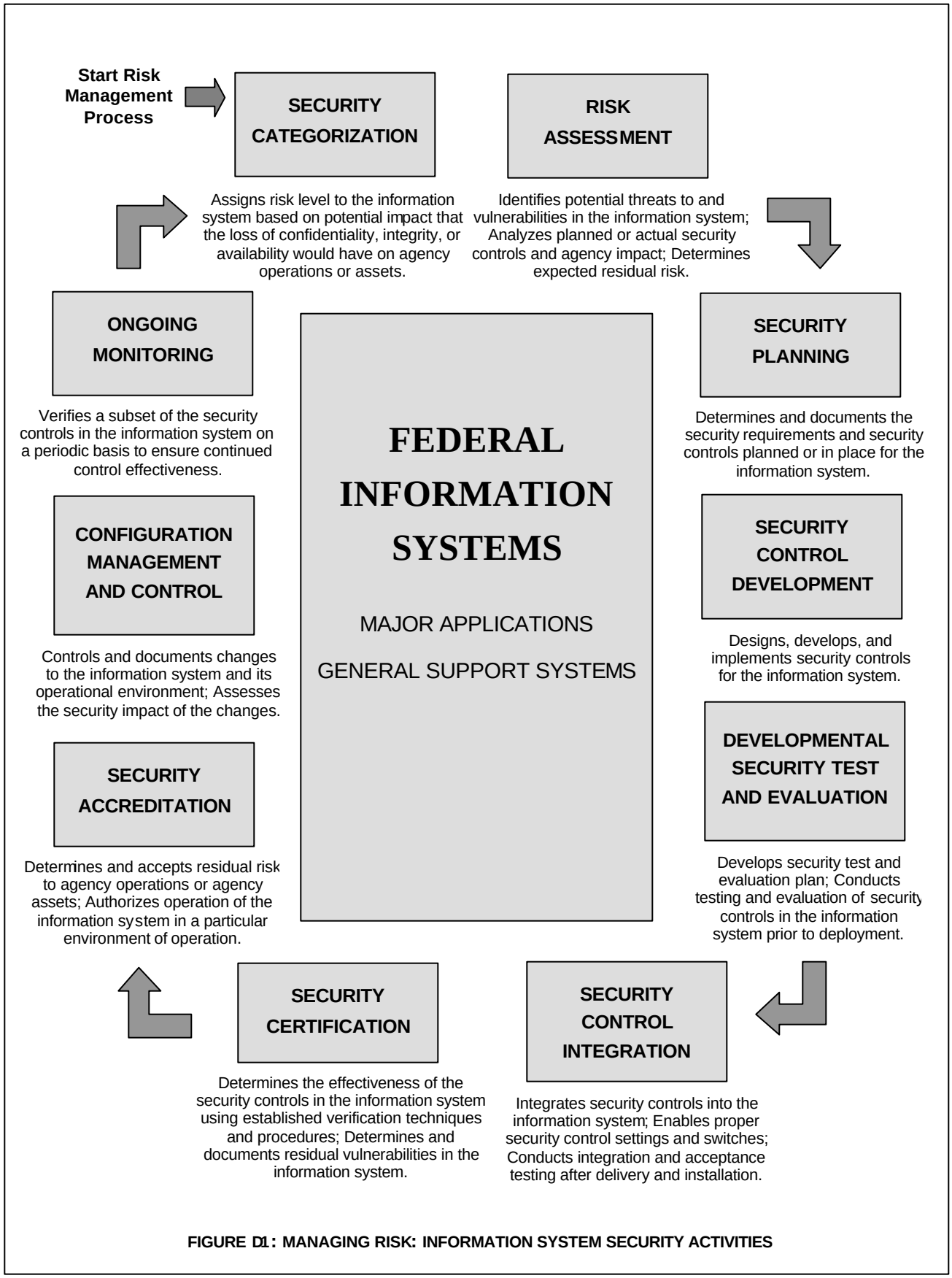

FIGURE D-1: MANAGING RISK: INFORMATION SYSTEM SECURITY ACTIVITIES