



United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-261421

June 1, 1995

Mr. Bruce McConnell
Information Policy and Technology Branch
Office of Information and Regulatory Affairs
Office of Management and Budget

Dear Mr. McConnell:

This letter provides our comments on the proposed revision of Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems," as published in the Federal Register on April 3, 1995.

The proposed revision is an important step in recognizing and addressing the security challenges posed by an increasingly interconnected computing environment. In particular, we concur with the proposal's emphasis on holding management and users accountable for the security of their information resources. We specifically endorse the revision's requirements that

- agencies establish rules of behavior for each general support system and major application;
- agencies provide users specific system training prior to their being granted access to the system, rather than generic security training;
- agencies report material information security weaknesses, like other material internal control weaknesses, in their annual reports pursuant to the Federal Managers' Financial Integrity Act; and
- the National Institute of Standards and Technology assess vulnerabilities of new technologies and communicate its findings to agencies prior to the agencies' adoption of such new technologies.

However, we have suggestions in three areas that we believe are critical to ensuring that agencies identify the most significant risks to their systems and implement cost-effective controls to mitigate these risks.

GAO/AIMD-95-151R Revisions to OMB's Circular A-130

154368

RISK ASSESSMENTS

The revised Appendix III should provide greater emphasis on the importance of risk assessments as an essential element in ensuring adequate security of information resources. The revised appendix refers repeatedly to the need for security controls and control reviews to be risk-based, but it eliminates the requirement that agencies perform risk analyses, and it provides no guidance on how risk is to be determined. We agree with OMB's intent that agencies focus on risk management rather than risk measurement. However, by not including a specific risk assessment requirement, the revision may be interpreted as inappropriately de-emphasizing the importance of systematically identifying and ranking risks as a basis for evaluating the costs and benefits of specific safeguards.

The need for rigorous risk assessments is more important now than ever. As interconnected computer networks proliferate, their vulnerabilities increase. In addition, because of the increasing complexity of computer configurations, these vulnerabilities may be less apparent and more difficult to identify without a systematic analysis. For these reasons, the revised appendix should state that it is important for agency managers to assess risk not only prior to the approval of new system designs and whenever significant system changes occur, as required by the existing Appendix III, but on a continuing basis. Risk assessments are especially important for determining the controls that should be built into new systems. Our experience has shown that controls incorporated during system development are less expensive than those retrofitted to systems in operation.

In addition, the revised appendix should clearly describe the role of risk assessments in the context of an agency's overall security program. Risk assessments, as well as related security planning activities, are only the initial steps. Actually reducing risk requires that selected safeguards be properly implemented and monitored for effectiveness.

The National Institute of Standards and Technology's (NIST) recently issued handbook on computer security¹ contains guidance on computer security risk management that we believe provides a flexible framework for performing meaningful risk assessments. This guidance focuses on the objectives of performing such assessments, outlines the essential activities, and describes alternative assessment techniques, without prescribing risk measurement or documentation requirements that might be overly burdensome or provide little value. In addition, the handbook addresses the importance of limiting risk assessments in order to avoid unnecessarily expensive efforts.

¹An Introduction to Computer Security: The NIST Handbook, March 16, 1995.

REVIEWS OF SECURITY CONTROLS

We agree with the Appendix III requirement that security reviews be performed when systems are significantly modified and, at a minimum, every 3 years. However, we believe that, to be effective, these reviews should be conducted by (1) independent reviewers who report their findings directly to top agency management and OMB and (2) using a structured approach. Such requirements would help ensure that security controls were objectively and completely assessed, encourage agency management to take prompt corrective action, and further assist OMB in its oversight responsibilities.

The proposed revision, like the existing Appendix III, requires agencies to assess their computer security safeguards as part of their self-assessments of internal controls. However, our reviews have shown that, despite this requirement, serious security control weaknesses often have not been adequately identified and reported, and identified weaknesses often have not been corrected, resulting in serious security gaps.

A large segment of federal computer operations is already subject to annual independent security reviews by agency inspectors general (IG) as part of annual financial statement audits required by the Chief Financial Officers Act (Public Law 101-576). In 1994, this audit requirement was extended to virtually all major federal entities by the Government Management Reform Act (Public Law 103-356). Although the reviews of computer security controls associated with these audits pertain primarily to financial systems, they usually cover a large portion of each agency's general support systems and major applications. This is because program and financial systems often are supported by common data centers and communications networks, and program management systems often are the source of many detailed financial transactions. Controls associated with systems that are not covered by the annual financial statement audits could be reviewed as an extension of these audits, or reviews of the two set of systems could be coordinated.

Alternatives for conducting independent reviews include periodically hiring contractors or establishing an oversight group within the agency to perform the reviews. The important considerations are that (1) security reviews be done by an entity with enough independence to provide an objective assessment, (2) summary results be reported at a level high enough to ensure accountability, and (3) performance and reporting of security reviews of financial and nonfinancial systems be coordinated.

Regarding use of a structured approach for performing the reviews, the revised appendix should specify the topics that such reviews should cover so that agencies understand what scope of review is expected. Topics that are widely accepted as being within the scope of a comprehensive computer security review include management, operational,

B-261421

and technical controls over (1) system access, (2) system design, development, and maintenance, (3) operating system software, (4) service continuity, and (5) the input, processing, and output associated with individual applications.

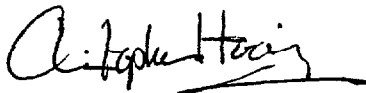
To help standardize such reviews and facilitate their performance, we are currently developing a methodology for assessing computer controls that includes these topics. We expect a working draft of the methodology to be available for our use, as well as for use by agency management and IGs, by Fall 1995.

PROTECTION OF SHARED INFORMATION

The revision requires agencies to ensure that information shared with others is appropriately protected but provides no guidance on how such assurance can be achieved. Briefly outlining suggested components of information sharing agreements and requiring that such agreements be documented would help ensure that agencies effectively implement this important requirement and follow established rules of behavior.

We appreciate the opportunity to comment on the proposed revision of Appendix III, and we hope that you find our suggestions useful. If you have any questions, please contact me at (202) 512-6208 or Jean Boltz at (202) 512-5247.

Sincerely yours,



Christopher Hoenic
Director, Information Resources
Management/ Policies and Issues

(510980)

REVIEWS OF SECURITY CONTROLS

We agree with the Appendix III requirement that security reviews be performed when systems are significantly modified and, at a minimum, every 3 years. However, we believe that, to be effective, these reviews should be conducted by (1) independent reviewers who report their findings directly to top agency management and OMB and (2) using a structured approach. Such requirements would help ensure that security controls were objectively and completely assessed, encourage agency management to take prompt corrective action, and further assist OMB in its oversight responsibilities.

The proposed revision, like the existing Appendix III, requires agencies to assess their computer security safeguards as part of their self-assessments of internal controls. However, our reviews have shown that, despite this requirement, serious security control weaknesses often have not been adequately identified and reported, and identified weaknesses often have not been corrected, resulting in serious security gaps.

A large segment of federal computer operations is already subject to annual independent security reviews by agency inspectors general (IG) as part of annual financial statement audits required by the Chief Financial Officers Act (Public Law 101-576). In 1994, this audit requirement was extended to virtually all major federal entities by the Government Management Reform Act (Public Law 103-356). Although the reviews of computer security controls associated with these audits pertain primarily to financial systems, they usually cover a large portion of each agency's general support systems and major applications. This is because program and financial systems often are supported by common data centers and communications networks, and program management systems often are the source of many detailed financial transactions. Controls associated with systems that are not covered by the annual financial statement audits could be reviewed as an extension of these audits, or reviews of the two set of systems could be coordinated.

Alternatives for conducting independent reviews include periodically hiring contractors or establishing an oversight group within the agency to perform the reviews. The important considerations are that (1) security reviews be done by an entity with enough independence to provide an objective assessment, (2) summary results be reported at a level high enough to ensure accountability, and (3) performance and reporting of security reviews of financial and nonfinancial systems be coordinated.

Regarding use of a structured approach for performing the reviews, the revised appendix should specify the topics that such reviews should cover so that agencies understand what scope of review is expected. Topics that are widely accepted as being within the scope of a comprehensive computer security review include management, operational,

B-261421

and technical controls over (1) system access, (2) system design, development, and maintenance, (3) operating system software, (4) service continuity, and (5) the input, processing, and output associated with individual applications.

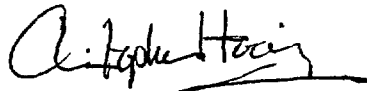
To help standardize such reviews and facilitate their performance, we are currently developing a methodology for assessing computer controls that includes these topics. We expect a working draft of the methodology to be available for our use, as well as for use by agency management and IGs, by Fall 1995.

PROTECTION OF SHARED INFORMATION

The revision requires agencies to ensure that information shared with others is appropriately protected but provides no guidance on how such assurance can be achieved. Briefly outlining suggested components of information sharing agreements and requiring that such agreements be documented would help ensure that agencies effectively implement this important requirement and follow established rules of behavior.

We appreciate the opportunity to comment on the proposed revision of Appendix III, and we hope that you find our suggestions useful. If you have any questions, please contact me at (202) 512-6208 or Jean Boltz at (202) 512-5247.

Sincerely yours,



Christopher Hoenig
Director, Information Resources
Management/ Policies and Issues

(510980)