United States General Accounting Office 132998

GAO

Testimony

For Release
on Delivery
Expected at
2:00 p.m. EST
Tuesday,
May 19, 1987

Information System Security
In Federal Civilian Agencies

Statement of
Thomas P. Giammo
Associate Director,
Information Management and Technology Division

Before the
Subcommittee on Transportation, Aviation and
Materials
Committee on Science, Space, and Technology
House of Representatives

132998

038937

Mr. Chairman and Members of the Subcommittee:

We are pleased to be here today to provide the Subcommittee information on our review of the practices used by federal civilian agencies in identifying and incorporating appropriate security controls in automated information systems. I have with me Dr. Harold J. Podell, Group Director from the Information Management and Technology Division, and Mr. Raymond J. Wyrsch, Senior Attorney from our Office of General Counsel.

Mr. Chairman, the work we are reporting on today is a follow-on to the review of the security for information systems at 17 agencies that we performed at the request of this Subcommittee in 1985. In that work, we examined the security of 25 automated information systems that had already been put into operation. We identified significant deficiencies in the controls of those systems that exposed them to abuse, destruction, error, fraud, and waste. An important finding of that work was that the origin of some of these deficiencies could be traced back to the development of the systems: appropriate security controls had not been successfully incorporated into many of the systems at the time they were planned, specified, and built.

Our present review is in response to a July 30, 1985, request from the Chairman of the Committee. We were requested to review how well civilian agencies are currently assuring that appropriate security controls are being successfully incorporated into their mission-critical, sensitive systems that are now being developed.

Mr. Chairman, our review suggests that the practices currently being used by civilian agencies in the development of mission-critical, sensitive systems will not assure that the appropriate security controls are being successfully incorporated into these systems. Specifically, we reviewed the practices currently being used at nine civilian agencies in the development of nine specific systems. We found that the practices in use at all nine agencies had permitted decisions critical to the specification, design, and construction of all nine systems to be made without adequate management consideration of important security issues.

Consequently, we believe that the systems currently in development at many civilian agencies (and intended to be used at least through the 1990s) are likely to possess many of the same security deficiencies we had previously found in the older systems already in operation. There is sufficient reason for concern that automated information systems of the future are likely to be only marginally better secured than those of the current generation. There is even more reason for concern, however, when one realizes that the automated information systems being developed today are likely to play an increasingly significant role in the essential business of our civilian agencies.

I would like to address the basis for these observations in greater detail, Mr. Chairman.

INFORMATION SECURITY

CRITERIA

We began our review by surveying existing federal guidance relating to the practices that should be used in the development of federal information systems. On the basis of our initial analysis, we concluded that the body of existing guidance was not a suitable basis for assessing whether agency practices provided appropriate security controls during the development of systems. Most of the relevant civilian guidance addresses general aspects either of the development process or of security concerns -- little effective guidance exists that comprehensively addresses how an agency should incorporate security considerations into the system development process. This absence in itself is a significant finding. We believe that this lack of specific federal guidance is an important contributing cause of the universality of the problems we found in this area. Therefore, rather than relying exclusively on the letter of existing federal guidance as the basis of our evaluation, we explicitly formulated our own criteria by applying the general principles given in that guidance to the specific activities needed to build security into an automated information system. In doing so, we followed accepted system development procedures.

The essence of these criteria turns out to be just common sense -- we believe that agency management must consider security requirements and constraints when making critical decisions about overall system architecture, detailed design, testing, and implementation. Simply put, for each of the critical decision points in the development of an automated information system, we identified important security-related information that management should have prior to making those decisions. In our review, we checked to see if this information was available to management and if it was considered in reaching the critical system development decisions. Unless we had positive evidence of this, we judged that agency management's ability to assure that appropriate security controls were being incorporated was significantly reduced.

Not surprisingly, the criteria we used corresponds to the "good practices" set out in several individual agency guidance documents and a draft report of the President's

Councils on Management Improvement, and on Integrity and Efficiency.

AGENCY PRACTICES REDUCE ASSURANCE THAT APPROPRIATE SECURITY CONTROLS ARE SUCCESSFULLY INCORPORATED

We reviewed the practices currently being used at nine agencies in the development of nine specific mission-critical, sensitive systems. (I will submit for the record the identification of the nine agencies and the systems studied.) We solicited informal agency comment from responsible officials on our findings at each agency. We received comments from seven of the nine agencies. We have not, however, yet submitted our completed reports for official agency comment. While it is possible that these agency comments may affect our understanding of specific points that we are reporting on today, they are not likely to significantly alter our overall conclusions.

As a result of our review, we found that the practices at the nine agencies in general did not meet our criteria for providing reasonable assurance that appropriate security controls were being successfully incorporated into the development of the nine systems. Moreover, we observed significant problems that were common among the agencies studied, suggesting that these problems might be common to most civilian agencies.

Developing An Information System Security Foundation

Our most significant finding is that all nine of the system development projects we reviewed made important decisions concerning the overall system architecture, and six of the nine proceeded to system design without adequate consideration by management of security needs. Consideration of security needs might have influenced these basic system development decisions.

The early activities of a system development process are focused on the determination of the system's functional requirements and on an identification and assessment of the major design approaches available to meet these requirements. It is considered to be good practice (and within the intent of federal guidance) that agencies go through a formal, documented process to assure that the overall system architecture and the system approach arrived at represent accountable management decisions that are based on a knowledgeable consideration of the costs and benefits for the range of feasible alternatives.

None of the agencies we reviewed, however, treated information security as one of the system's integral functional requirements. In particular, we found that the agencies were significantly weak in making overall assessments of their systems' potential vulnerability to threats, such as identifying the major security control approaches and conducting initial assessments of the economic, operational, and technical feasibility of these approaches. Specifically, six of the nine agencies either did not address, or inadequately addressed, the sensitivity of the information to be handled by the system. Most of the agencies (eight of the nine) did not perform any analysis of risk to the proposed system. That is, only one of the agencies analyzed the potential risks to the system. We also found only one attempt at a cost/benefit analysis of security alternatives and that analysis was missing the applicable security benefits.

INITIAL INFORMATION SECURITY PROBLEMS HINDERED SUBSEQUENT DEVELOPMENT

Later security-related development activities are intended to assure that appropriate security controls are specified, developed, and tested. Without a thorough understanding of a system's security requirements and alternatives, however, we believe that the effectiveness of these activities was either nullified or significantly reduced in most of the cases we studied. For example, seven of the agencies had progressed in the system development process to the point of identifying where security controls were to be located in the system. In each of these cases, we judged that agency management could provide no positive assurance that they had appropriately identified the location of controls, because they could not demonstrate where the systems were vulnerable.

Additional weaknesses were evident in subsequent security development activities, where some important security-related procedures were not performed at all. For example, three of the four agencies that had reached the construction phase of system development were writing and testing software without plans and procedures to test security.

We are preparing a report that will document the overall results of our review of agency practices. In addition, we will provide separate reports to each of the nine agencies we studied concerning security development practices for the specific systems under development at their agencies. We also are continuing our analysis of deficiencies in existing governmentwide policies, standards, and guidelines that may contribute to the observed weaknesses, and we are planning to report to you on this subject later this year.

I will close by saying that there is a need for agency managers to take the initiative in providing security controls during the development of mission-critical, sensitive systems. In taking this initiative, agencies have to look beyond literal compliance with existing federal policy, standards, and guidance to treat system security requirements with the same rigor and thorough consideration called for in the treatment of other functional requirements.

This completes my prepared statement. We have brought along information regarding our review of the nine specific system development projects we studied. We will be pleased to answer your questions regarding these systems or regarding system development practices in general.