REVBLT.TXT
NCSL BULLETIN
OCTOBER, 1990

REVIEW OF FEDERAL AGENCY COMPUTER SECURITY AND PRIVACY PLANS (CSPP): A SUMMARY REPORT

Sensitive information and information resources have become increasingly important to the functioning of the federal government. The protection of such information is integral to the government serving the public trust. Concern that federal agencies were not protecting their information caused Congress to enact Public Law 100-235, "Computer Security Act of 1987" (the Act). The Act reaffirmed the National Institute of Standards and Technology's (NIST) computer security responsibilities. These responsibilities include developing standards and guidelines to protect sensitive unclassified information. Other responsibilities include providing new governmentwide programs in computer security awareness training and security planning.

The Act required federal agencies to conduct educational programs to increase staff awareness of the need for computer security. The first-year activity included agencies identifying their computer systems containing sensitive information. These agencies prepared and submitted security plans for those systems to the NIST and National Security Agency (NSA) review team for advice and comment. This document summarizes a report on the review of the computer security and privacy plans that were submitted by federal agencies.

How The Reviews Were Conducted

The Office of Management and Budget (OMB) issued OMB Bulletin 88-16, "Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information," to guide agencies on preparing and submitting computer security plans. The bulletin specified the information that was to appear in each plan. The bulletin further requested that agencies identify systems as major application or general ADP support systems. Finally, the bulletin provided the agency the option of identifying any needs for guidance or technical support. This option also included making any comments the agency thought appropriate. Although a four-part format appeared, agencies were able to use latitude as long as all pertinent information was present. This permitted agencies with existing programs to submit current related documents. Submission of an agency overview was optional and most agencies chose not to provide one.

The joint NIST/NSA review team examined 1,583 plans for 63 federal civilian agencies and 27,992 plans from 441 Department of Defense (DoD) organizations. Most DoD submissions consisted mainly of accreditation documentation prepared for other computer security planning purposes. During the review process, the review team recorded data about the systems for analysis. The conclusions made in this report stem principally, but not exclusively, from the civilian agency submissions.

Major Findings

The review team arrived at a number of conclusions about the plans and the plan review process, seeing both many positive signs and some areas for improvement. These findings include:

- The civilian agency CSPPs basically conformed with the guidance given by OMB Bulletin 88-16. Many controls to protect sensitive systems were already in place or planned. These controls appeared consistent with identified system functions, environment, and security needs. However, some respondents appeared to have just "checked the boxes," perhaps presenting a falsely optimistic picture.

- Many agencies appeared to report on isolated systems rather than all systems subject to the Computer Security Act and OMB Bulletin 88-16.

- Agencywide guidance on how to prepare the plans was not clear. There was also some question whether a high-level official reviewed the plans. Also unclear is the distribution of agency-level computer security policy and guidance. Further, most plans did not reflect the joint involvement of ADP, computer security, and applications communities in computer security planning.

- Significantly, the plans rarely addressed the security concerns on networking, interfaces with other systems, and the use of contractors and their facilities. This may reflect a general confusion about the boundaries and limits of responsibility for a given system.

- Many plans equated sensitivity only with privacy or confidentiality and did not fully address requirements for integrity and availability.

- Most plans did not communicate an appreciation for the

role of risk management activities in computer security planning.

- Although most agencies said they had computer security awareness and training, many did not show that all applicable employees received periodic training.

- Finally, the CSPP submission and review effort raised the level of federal awareness regarding the need to protect sensitive information and the importance of computer security planning.

Recommendations for Agencies

Based on the needs that became apparent during the plan review, the review team recommends the following:

- Agency management should ensure that computer security has the highest level of management involvement. This involvement is also important in the computer security planning process. Computer security benefits from the multiple perspectives of and input from agency information resources management, computer security, and functional, user, and applications personnel.

- Agency management should identify and describe the security needs of their systems which contain sensitive information.

- Agency management should recognize the importance of computer security and its required planning. This recognition should be aggressively communicated to their staffs, perhaps using their computer security and awareness training programs as one of the vehicles.

- Agencies should incorporate computer security planning with other information systems planning activities.

- Agencies should consider the protection requirements for integrity and availability on an equal basis with that of confidentiality.

- Agencies should assess risks, and select and implement realistic controls throughout the system life cycle. This involves awareness of technology changes with

regard to system hardware and software. This awareness also requires a knowledge of new technology and new methods for protecting and recovering from system threats. In addition, agencies should fully document in-place controls to ease periodic reevaluation, internal audit, and oversight agency review.

- Agencies should implement certification and accreditation programs. There is a lack of awareness of guidance regarding certification and accreditation, including FIPS PUB 102, "Guideline for Computer Security Certification and Accreditation." There is also a lack of knowledge of the certification requirements in OMB Circular A-130, "Management of Federal Information Resources." Agencies may use OMB Circular A-130 as the basis for these programs.

- Agencies should clarify the boundaries and limits of responsibility for each system, and should include, in any planned risk assessment activity, full consideration of the telecommunications and networking environment and relationships with contractors and other organizations.

- Agencies should stress security awareness and training for their employees. This includes all employees involved in the design, management, development, operation, or use of federal computer systems containing sensitive information.

- Agencies should develop computer security policy and operative guidance. Such policy and guidance should fully reflect and comprehensively address an encompassing view of computer security. The Computer Security Act, OMB Circular A-130, and OMB Bulletins 88-16 and 89-17, "Federal Information Systems and Technology Planning," and their successors all contain this view. The policy should directly address the full scope of computer security planning and risk management activities. It must incorporate an application system perspective and give more detailed consideration to confidentiality, integrity, and availability protection requirements.

What NIST is Doing

NIST is evolving a strategy for helping federal agencies in identifying and protecting sensitive information systems. This

strategy shifts emphasis to the implementation of computer security plans, particularly those developed under OMB Bulletin 88-16. It provides for visits by OMB, NIST, and NSA staff. This group will provide direct comments, advice, and technical aid focused on the agency's implementation of the Act.

In addition to the agency visits described above, NIST has initiated the following computer security projects to help agencies more easily and effectively comply with the Computer Security Act:

- NIST will develop standardized specifications and language for federal government computer security services contracts.

- NIST will develop a guidance document on computer security in the ADP procurement cycle.

- NIST has recently published guidance on the use of Trusted Systems.

- NIST will develop guidance on computer security planning.

- NIST has developed, and will continue to operate, a computer incident response center in order to address viruses, worms, and other malicious software attacks.

- NIST will support and coordinate computer security resource and response centers nationwide.

- NIST will enhance and operate the National Computer Systems Laboratory (NCSL) Computer Security Bulletin Board System.

- NIST will operate the NIST/NSA Risk Management Laboratory and prepare further guidelines on risk management.

- NIST will develop guidance and recommendations on assuring information integrity in computer systems.

In addition to the above plans, NIST has already developed a number of guidelines and other resources to help federal managers secure their computer systems.

Future Directions

Federal managers have computer security requirements that are similar to their counterparts in the private sector. We believe that private sector organizations can learn and benefit from the federal experience in implementing the Computer Security Act. In both environments, a vigorous computer security awareness program is important at all levels in the organization. Also, in both environments, the active involvement of user, management, ADP, and computer security communities in computer security planning could help end some of the existing and potential barriers to effective computer security. Such collective involvement would also help ensure cost-effective control measures commensurate with system function, system sensitivity, security requirements, and analyzed and considered risks.

Agencies need to be aware of developments taking place in the national and international standards arena on system interoperability and data interchange. These developments will impact information system product availability, protection requirements, and protection alternatives as agencies do their near-, mid-, and long-term IRM and computer security planning.

Finally, because agency awareness of problems is fundamental to the solution, this project has been valuable. Computer security officers say that the CSPP preparation and review activity has raised the level of awareness in all parts of their organizations and has made it easier for them to promote computer security. The CSPP review project significantly raised the level of federal awareness about the protection of sensitive information and the importance of computer security planning. In the final analysis, this contribution may be among the most meaningful results of the project.

The complete report of the CSPP review project will be published as an NIST Interagency Report (NISTIR), and will be available from the National Technical Information Service (NTIS) U.S. Department of Commerce, 5285 Port Royal Road, Springfield, VA 22161. Telephone: (703) 487-4650 FTS 737-4650. For information about the report findings, contact Dennis Gilbert, National Institute of Standards and Technology, A216, Technology Building, Gaithersburg, MD 20899. Telephone: (301) 975-3872.