UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

LOGISTICS AND COMMUNICATIONS
DIVISION

APRIL 30, 1980

B-198551

The Honorable Richardson Preyer
Chairman, Subcommittee on Government
Information and Individual Rights
Committee on Government Operations
House of Representatives

Dear Mr. Chairman:

Subject: Central Agencies' Compliance With OMB Circular A-71, Transmittal Memorandum No. 1 (LCD-80-56-I)

Your December 21, 1979, letter requested us to perform a followup evaluation of the implementation of the recommendations in our January 23, 1979, report, "Automated Systems Security--Federal Agencies Should Strengthen Safeguards Over Personal and Other Sensitive Data" (LCD-78-123). In a subsequent letter dated January 17, 1980, you requested that a preliminary report be provided to the Subcommittee by May 1, 1980.

As discussed with your office, this letter summarizes actions taken by the Office of Management and Budget (OMB) in its leadership role relating to agencies' automated systems security programs and actions taken by key central agencies--the Department of Commerce, the General Services Administration (GSA), and the Office of Personnel Management--to comply with the requirements of OMB Circular A-71, transmittal memorandum No. 1, entitled "Security of Federal Automated Information Systems." Our conclusions concerning the effectiveness of these actions and our assessment of the status of implementation of automated systems security programs at agencies will be covered in our final report. Since our work is still continuing at the central agencies, we are not making recommendations at this time.

OMB ACTIONS

OMB issued transmittal memorandum No. 1 to Circular A-71 on July 27, 1978. The memorandum required Federal executive departments and agencies to establish automated security programs and to submit the plans for implementing their program to OMB by November 24, 1978. We recommended in our January 1979 report on automated systems security that OMB, as part of its leadership functions, have independent reviewers knowledgeable in computer security critique the adequacy of agencies' security plans as required by the memorandum.

Evaluations of agencies' plans

Consistent with the recommendation in our 1979 report, OMB assembled a small, multidisciplined task team of four persons, each from a different agency, to review the computer security plans submitted by the agencies. The task team met in December 1978 and developed a list of criteria to evaluate agencies' plans.

The task team's evaluations of agencies' plans showed substantial differences existed in how agencies interpreted the memorandum's requirements and approaches to strengthening their computer security. OMB decided further clarification and action was needed. As a result, the task team developed an agency computer security program checklist. The checklist was sent to executive departments and agencies in January and February 1979, and the agencies were requested to resubmit plans to OMB, in conformity with the checklist, by February 28, 1979.

The first task team disbanded after developing the computer security checklist, so OMB assembled a new team to evaluate the second set of security plans. The second plans, however, were evaluated primarily by one individual. (A second individual helped for 2 weeks but was then recalled to his parent agency). Working mainly by himself, the evaluator critiqued the second responses from March through December 1979. The critiques were sent to the respective departments and agencies and identified those areas in the plans that the evaluator believed needed additional attention. The two most frequently identified weaknesses in the second plans submitted by agencies were the lack of provisions for personnel security (that is, screening of individuals participating in the design, operation, or maintenance of computer systems) and inadequate contingency plans.

Reorganization at OMB

On January 9, 1980--about 1 month after the evaluations were completed on agencies' second security plans--OMB announced the reorganization of its Information Systems Policy

Division and Regulatory Policy and Reports Management Division into the Office of Regulatory and Information Policy. The new Office has three divisions--Regulatory Policy, Reports Management, and Information Policy. Each Division is responsible for playing a Government-wide policy role, as well as reviewing agencies' implementation of Federal regulatory policies, reports management policies, and information policies.

OMB has organized and staffed the divisions on an agency/functional basis: the Regulatory Policy Division was assigned agencies that placed heavy regulatory burdens on the private sector; the Reports Management Division was assigned agencies that had large volumes of public reporting; and the Information Policy Division was assigned agencies that had the majority of the Government's data processing and telecommunications systems.

The new Office will include a "desk officer" responsible for monitoring the implementation of regulatory, reports management, and information management activities in each assigned department or agency. OMB believes that this decentralized approach will better assist agencies because the desk officers will be familiar with the particular assigned agencies' operations as they apply to the full range of information or regulatory policies.

OMB advised us that many of the desk officers know little about automatic data processing in general or automated security in particular. OMB, realizing that these officers need training and help from people knowledgeable about automated security, plans to conduct such training during May and June 1980. Effective monitoring by trained OMB staff is necessary if the intent of the memorandum--security of automated information systems--is to be met.

KEY AGENCY ACTIONS

The memorandum assigned Government-wide responsibilities for certain functions to ensure effective automated information security to three agencies: the Department of Commerce, GSA, and the Office of Personnel Management. These agencies were directed to report to OMB by the end of September 1978 with plans for meeting their responsibilities under the memorandum.

Department of Commerce

The memorandum required the Department of Commerce to develop and issue computer security standards and guidelines to ensure the security of automated information. The Department sent its plan for meeting the memorandum's requirements to OMB on October 20, 1978. The plan listed 36 standards the Department believed were needed to meet its responsibilities under the memorandum. The Department's plan called for the National Bureau of Standards to publish the standards over the following timeframes: 1 in fiscal year 1977; 4 in fiscal year 1980; 5 in fiscal year 1982; 8 in fiscal year 1983; 12 in fiscal year 1984; and 6 in fiscal year 1985. Included in these planned publications were to be guidelines for implementing physical security, evaluating the security status of Federal computer installations, and certifying systems' security controls. The National Bureau of Standards is also developing security guidelines for contingency planning and for risk analyses. A guideline dealing with the security controls in application programs is expected to be issued before the end of fiscal year 1980.

GSA

The memorandum required GSA to issue policies and regulations for the physical security of computer rooms and to ensure that agency procurement requests for computers, software, and related services include appropriate security requirements. GSA sent its plans for meeting the memorandum's requirements to OMB on October 11, 1978, and on November 24, 1978. In the November plan, GSA discussed its intention to revise the Federal Procurement Regulations and the Federal Property Management Regulations to include the memorandum's requirements and established March and April 1979 target completion dates for these revisions.

GSA has drafted, circulated for comment, and evaluated and incorporated the comments on the following three proposed regulation revisions: Federal Property Management Regulations 101-35.3 series on the security of Federal automatic data processing and telecommunications; Federal Property Management Regulations 101-36.7 series on environment and physical security; and Federal Procurement Regulations 1-4.11 on security requirements in contracts. GSA did not send out this request for comments until October 1979. GSA officials, however, attributed the delay in reaching their targeted completion dates primarily to the "wider than originally planned" audience asked to comment on the draft revisions. (Less than 40 recipients were initially targeted but the final distribution for comments comprised almost 500 names and organizations.)

Office of Personnel Management

The memorandum required the Office of Personnel Management to establish personnel security policies for Federal personnel associated with or having access to data in Federal computer systems. The Office of Personnel Management's October 26, 1978, responses to OMB included Federal Personnel Management (FPM) Letter 732-7 on a "Personnel Security Program for Positions Associated with Federal Computer Systems." The letter's requirements became effective on November 14, 1978. The letter presented guidelines agencies could use when establishing their personnel security programs. Three sensitivity designations--developed, in part, from then existing FPM guidance--were presented as a basis for determining what level of investigation should be made on personnel working in a computer systems environment.

FPM Letter 732-7 indicated that the Office of Personnel Management's authority did not permit extending the letter's coverage to contractor employees and that agencies would have to prepare their own policies to handle such situations. A number of agencies, however, questioned whether authority existed for them to screen and investigate contractor employees who would not have access to classified data. Acting on the agencies' concerns, the Office of Personnel Management requested, and received, an opinion on the issue from the Department of Justice. The Office of Personnel Management subsequently issued FPM Bulletin 732-2, dated January 11, 1980, summarizing the Department of Justice's opinion that Federal agencies have the authority to screen contractor employees as long as the screening is done consistent with the due process of law.

- - - -

We will be pleased to discuss the central agencies' activities with you. Our continuing work will concentrate primarily on evaluating the executive departments' and agencies' progress in implementing the security plans required by transmittal memorandum No. 1 and other guidance. We expect to provide you with the results of our review by November 30, 1980.

Sincerely yours,

RW Gutmann

R. W. Gutmann
Director