Memorandum

Date JUL 5 1994

From June Gibbs Brown
Inspector General

Subject Physical Security over Data Processing Operations at the Centers for Disease Control and Prevention (A-04-92-03501)

To Philip R. Lee, M.D.
Assistant Secretary for Health

The attached final report presents the results of our review of physical security over data processing at the Centers for Disease Control and Prevention (CDC).

We performed our review in response to a request from the Chairman, Committee on Government Operations, House of Representatives. Our objective was to evaluate the adequacy of physical security over data processing at CDC's headquarters and satellite facilities in the Atlanta, Georgia metropolitan area.

Our review showed that CDC had not placed enough importance on ensuring the physical security of its data processing operations. Specifically, we found significant deficiencies in several areas such as the adequacy of facilities, access controls, plans for disaster recovery and continuity of operations and security training for employees and contractor staff. These deficiencies created unnecessary risks that could effect CDC's accomplishment of its missions.

We are recommending that the Public Health Service (PHS) direct the CDC to continue its efforts to enhance the security over data processing operations. Specifically, CDC should correct the facilities' deficiencies noted during our review in a cost-effective manner, develop and implement comprehensive organizationwide policies and procedures regarding security, and establish a program to provide appropriate security awareness and emergency response training to employees and contractor staff.

In formal comments to the draft of this report, PHS officials concurred with our recommendations and discussed a number of actions initiated by CDC officials to correct the deficiencies noted in our report and enhance the security over data processing operations.

We would appreciate being advised within 60 days on the status of corrective actions taken or planned on our recommendations.

Should you wish to discuss the issues raised in this review, please call me or have your staff contact Michael R. Hill, Assistant Inspector General for Public Health Service Audits, at (301) 443-3582.

Attachment

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

PHYSICAL SECURITY OVER DATA PROCESSING OPERATIONS AT THE CENTERS OF DISEASE CONTROL AND PREVENTION

JUNE GIBBS BROWN
Inspector General

JULY 1994
A-04-92-03501

Memorandum

Date JUL 5 1994

From June Gibbs Brown
Inspector General

Subject Physical Security over Data Processing Operations at the Centers for Disease Control and Prevention (A-04-92-03501)

To Philip R. Lee, M.D.
Assistant Secretary for Health

This final report presents the results of our review of physical security over data processing at the Centers for Disease Control and Prevention (CDC). Automated information systems at CDC include a wide range of administrative, medical, and scientific data of critical importance for the successful accomplishment of the agency's mission. Our objective was to evaluate the adequacy of physical security over data processing at CDC's headquarters and satellite facilities in the Atlanta, Georgia metropolitan area. The Government requires a level of security to protect the confidentiality, integrity, and availability of information.

Our review showed that CDC had not placed enough importance on ensuring the physical security of its data processing operations. Specifically, we found significant deficiencies in several areas such as the adequacy of facilities, where serious construction deficiencies in CDC's computer center create unnecessary security risks. We also found weak access controls, where there was little control over employee access to the computer center. Plans for disaster recovery and continuity of operations were not tested and up-to-date, and CDC had not provided sufficient security training to its employees.

We are recommending that the Public Health Service (PHS) direct the CDC to continue its efforts to enhance the security over data processing operations. Specifically, CDC should correct the deficiencies noted during our review, develop and implement organizationwide controls over access to equipment and data, update and test disaster recovery and contingency plans, and establish a program to provide appropriate security awareness and emergency response training to employees and contractor personnel.

In their comments to the draft report, PHS officials concurred with our recommendations and advised us on the status of the many actions taken by CDC officials to enhance the physical security over data processing operations. The PHS comments and the specific actions initiated by CDC are attached in their entirety as an Appendix to this report.

BACKGROUND

The CDC's mission is to promote health and quality of life by preventing and controlling disease, injury, and disability. The CDC works with State and local health departments and other partners in prevention using surveillance, health statistics, epidemiology, disease identification in the laboratory, behavioral risk reduction, technology transfer, and prevention strategies and programs.

In recent years, increased emphasis on program activities in such areas as immunization, Human Immunodeficiency Virus and Acquired Immunodeficiency Syndrome education, breast and cervical cancer prevention, and tuberculosis elimination has resulted in significant CDC growth. The budget request for CDC programs in Fiscal Year (FY) 1995 was over $1.98 billion--77 percent higher than CDC's funding level in FY 1990. The CDC has also grown significantly in terms of staff. The CDC's staffing will exceed 6,500 in FY 1995, an increase of almost 31 percent from FY 1990.

Information systems are an integral part of CDC's operations. Primary responsibility for data processing operations at CDC is assigned to the Information Resources Management Office (IRMO). As shown in CDC's Organization, Mission and Functions statement, IRMO's responsibilities include managing the operations of CDC's mainframe computer center and developing and coordinating the implementation of a security program for CDC's decentralized automated information systems on an organizationwide basis. The IRMO was authorized approximately 120 positions and a budget of about $15 million for data processing operations in FY 1993.

Data processing operations are carried out in virtually every organizational component of CDC. The mainframe computer center is based on an IBM 9021-580 central processing unit, which supports a wide range of input/output devices and peripheral equipment. Other CDC centers, institutes and offices can access the mainframe through approximately 5,500 personal computers linked to the computer center through more than 120 local area or wide area networks. Automated information systems at CDC include a wide range of administrative, medical, and scientific data of critical importance for the successful accomplishment of the agency's mission.

The Government requires a level of security to protect the confidentiality, integrity, and availability of information. The Paperwork Reduction Act of 1980 established a mandate for Federal agencies to carry out information management activities in an efficient, effective and economical manner.

The Computer Security Act of 1987 subsequently provided additional guidance to Federal agencies operating automated information systems (AIS) and required agencies to establish security plans based on certain minimum acceptable practices.

The Office of Management and Budget (OMB) issued Circular A-130 in December 1985 to provide Governmentwide policies and procedures regarding information management. Appendix III to Circular A-130 established a minimum set of controls to be included in security programs and internal control systems.

In accordance with the requirements of applicable statutes and OMB Circular A-130, the Department of Health and Human Services (Department) issued its Information Resources Management (IRM) Manual to set forth departmentwide policies regarding data processing operations. Chapter 6 of the IRM manual, issued in July 1982, established minimum standards for the security of departmental information systems and assigned responsibilities to departmental officials to comply with those standards. In December 1991, the Department also issued its Automated Information Systems Security Handbook, providing a comprehensive description of the Department's approach to security over information processing operations. It sets forth the Department's basic security policy, as follows:

> "DHHS will implement a department-wide AIS security program to assure that each automated information system has a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure, or modification of the information contained in the system. Each system's level of security must protect the confidentiality, integrity, and availability of the information.
>
> "Each operating division shall administer an AIS security program that meets statutory, regulatory, and departmental requirements and the needs of the OPDIV and the public."

This criteria places responsibility upon PHS management officials to ensure the adequacy of security programs for all component units, including CDC.

In addition to this review, two other reports addressing the security of CDC's data processing operations have been issued in recent years. In December 1991, a consultant retained by CDC's National Center for Health Statistics (NCHS) issued a report addressing the security over CDC data processing. While the report presented only limited specifics, the consultant expressed concerns over the security environment at

CDC's headquarters computer center, as shown by the following excerpts.

> "...the information security posture at CDC - Atlanta is unsatisfactory. The physical site for the...mainframe is among the worst the author has seen in either the public or private sectors. The hardware on which all centralized processing at CDC is dependent is in continuing jeopardy.
>
> "The plans for a new mainframe site provide a new location in the 1996/97 period, a time far longer than seems defensible in light of the current security situation and the continuing evolution of new security problems....
>
> "The current information security posture at Atlanta is sufficiently poor to constitute a potential source of considerable embarrassment...."

The CDC did not completely agree with the consultant's conclusions. However, CDC's formal assessment by its IRMO Director acknowledged that the consultant's report

> "...points out the widely known and accepted fact that the physical facilities which currently support the CDC Atlanta mainframe have limitations which need to be addressed.... I believe (the) report correctly indicates some weaknesses in CDC's security program...."

The IRMO Director recommended that CDC obtain an updated risk analysis of the mainframe computer center.

In December 1992, a number of additional weaknesses in the security over CDC's mainframe computer center were identified in a risk analysis report prepared by the Federal Systems Integration and Management Center under a contract with CDC. While security of the computer center was rated as adequate on an overall basis, a breakdown of the reported results by specific category indicated several problem areas, as follows.

Category	Rating[1]
Environmental Security	Deficient
Physical Security	Less Than Adequate
Security Management	Less Than Adequate
Communications/Network Security	Less Than Adequate
Software Security	Adequate
Personnel Security	Adequate
Media/Information Security	Adequate
Procedural Security	Adequate
Hardware Security	Favorable

The risk analysis identified 28 specific deficiencies and vulnerabilities and proposed 22 specific enhancements to CDC's security environment. Several of the recommended enhancements addressed more than one of the identified deficiencies.

SCOPE

Our objective was to evaluate the adequacy of physical security over data processing at CDC's headquarters and satellite facilities in the Atlanta, Georgia metropolitan area. We performed this assignment in response to a request from the Chairman, Committee on Government Operations, House of Representatives to review CDC's information resources management activities. We initiated several reviews of these activities, including the review of physical security over data processing operations. To fulfill our objective, we planned and carried out our review in three phases:

- an analysis of laws, regulations, policies and guidelines to identify the specific requirements applicable to security controls at CDC, such as the Privacy Act of 1974, the Computer Security Act of 1987, OMB Circular A-130, Federal Information Resources Management Regulations, the Department's Automated Information Systems Security Program Handbook, and publications issued by the National Bureau of Standards;

---

[1] Risk analysis ratings relate to "acceptable arrangements" based on identified threats and vulnerabilities in each security discipline. Ratings of "Deficient" or "Less Than Adequate" show that in-place countermeasures were not sufficient to meet all identified threats and/or did not meet minimal acceptable arrangements. An "Adequate" rating indicates that minimal acceptable arrangements were in place and a "Favorable" rating shows that in-place countermeasures exceeded minimal arrangements.

- a review of CDC's organizational and management structure to ensure proper understanding of the relationships between IRMO and other CDC components making up its user community, the responsibilities placed on each component with respect to maintaining a security program, and the policies and procedures guiding implementation of that program; and

- an evaluation of the security environment in place within both IRMO and the user community. Our evaluation included: reviews of policies and procedures developed and implemented within IRMO; interviews with officials and staff of several other CDC components who rely upon information processing; and tours of IRMO's computer center and user facilities.

We performed our review in accordance with generally accepted government auditing standards. Field work on the review was performed at various times from April 1992 through November 1993 at CDC's headquarters and judgmentally selected satellite facilities in the Atlanta metropolitan area. The satellite facilities inspected during our review representing four of the six locations where CDC leased office space were:

Freeway Park - Building 1600
Executive Park - Buildings 16, 18, 26 and 35
Koger Center - Davidson and Rhodes Buildings
Scottish Rite Building

These satellite facilities were selected from locations housing CDC components with representatives serving on CDC's IRM steering committee and the security subgroup of that committee. The individual employees who provided us with information and conducted tours of the satellite facilities were recommended by IRMO officials.

We did not assess the security environment at CDC operations outside the Atlanta area, nor did we compare the security environment at CDC to that of any other organizations.

RESULTS OF REVIEW

Our work disclosed a number of serious deficiencies in the physical security over mainframe data processing and microcomputer operations. The most significant deficiencies were found with the adequacy of facilities, access controls, plans for disaster recovery and continuity of operations, and security training.

FACILITIES

The CDC's mainframe computer center is housed in the subbasement of an aging facility with insufficient space and is poorly designed for its current function. While IRMO officials have made a number of improvements in recent years, serious construction deficiencies in CDC's computer center create unnecessary security risks and increase the danger to employees in the event of a fire or other disaster.

Appropriate design and construction of data processing facilities is necessary for the provision of adequate physical security. In addressing facility construction, Chapter 6 of the Department's ADP Systems Manual sets out minimum standards in such areas as construction, fire safety and emergency response and charges each agency with the responsibility to:

> "...determine the most cost-effective method for securing the system given the vulnerability of the facility to penetration..., the sensitivity of the data processed and the value of the resources to be protected."

The most significant deficiencies noted during our review relate to CDC's ability to respond to emergency situations such as a fire. For example, the computer center is protected by a precharged, wet pipe water sprinkler system, with water pipes positioned directly above CDC's mainframe computer. The sprinkler system increases the potential for significant damage to the computer and related equipment in case of a fire and increases the risk to IRMO staff as they would be forced to spread plastic sheeting over the equipment before evacuating the center. Further, given the subbasement location, the potential for damages due to water leaks from the sprinkler system or air conditioning systems for the computer room or higher floors is increased.

We also noted that the computer room is not equipped with appropriate emergency power-off switches to disconnect electrical power to hardware and other equipment. Thus, in an emergency situation, such as a fire, operators would have to go to several different locations to power down the system.

Without emergency power-off switches, the air conditioning and lighting systems are not automatically shut down in an emergency. This deficiency increases the potential dangers of a fire by allowing smoke to circulate throughout the computer center during a fire, and could contribute to worsening the effects of a fire if water were to come into contact with the overhead lighting fixtures or other electrical systems. Without the capability to take appropriate actions on a timely

basis, there is little assurance that relatively minor problems can be controlled before they cause major disruption or destruction of data processing operations.

Emergency lighting throughout the computer center is very limited with some rooms having no emergency lighting at all. The lack of adequate lighting is particularly critical for the safety of CDC staff given the conditions cited above.

ACCESS CONTROLS

The CDC has not established adequate controls limiting access to data processing operations at either its computer center or satellite facilities. Further, a lack of physical security controls at many locations coupled with lax compliance with existing controls by CDC employees significantly increase the risks to CDC personnel, equipment and information.

Both the ADP Systems Manual and Automated Information Systems Security Program Handbook present departmental policies that information files, as well as data processing equipment, be protected against unauthorized access. Departmental policy, for example, limits the extent of sensitive information that may be maintained by a Department's operating division (OPDIV) to that required by law or essential to its mission, and then requires that the OPDIV:

> "...establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual...."

Further,

> "Each facility manager should establish physical and administrative controls to prevent unauthorized entry into the operations, data storage, library and other support areas."

Mainframe Computer Center

Since the computer center is located in the subbasement served by both elevators and stairways, the area is easily accessible from other sections of the building during normal working hours. In addition, we observed that doors allowing hallway access to such critical areas as the power supply and telecommunications room were unlocked at the time of our initial tour.

The relative ease of access to the subbasement is particularly important because three access doors into the building were left unlocked during normal working hours. These unlocked doors increase the risk that individuals, either staff or members of the public, could successfully cause significant damage to vital equipment or threaten the safety of CDC employees.

Access to the computer center itself is controlled by a card-key system. We found that IRMO could not account for all the card-keys issued to employees and contractors, nor could they adequately explain why some card-keys had been issued. Some CDC officials with little or no need for access to the computer room had apparently been issued card-keys based on their overall management responsibilities. Other employees had been issued duplicate card-keys with no explanation why the additional keys were needed. Blocks of card-keys had been issued to contractors, with little or no apparent control over assignment of the cards to individual employees or periodic monitoring to ensure that the keys could be properly accounted for or safeguarded.

Within the computer center, a lack of adequate space mandates that IRMO's data storage library be maintained in the computer room rather than in a separate room with its own security controls. Accordingly, all individuals having access to the computer room, including those CDC and contractor personnel operating the computer, also have virtually unlimited access to CDC's data files.

Satellite Facilities

Controls over physical access to many of CDC's satellite locations were clearly inadequate, and we noted only limited adherence to controls that had been implemented. Controls over access to CDC's satellite facilities are particularly critical since many components are located in commercial buildings that remain accessible to the public.

While some components located in satellite facilities had stationed personnel at entry points to identify visitors and restrict access to sensitive areas, the information processing activities of other components were essentially accessible to anyone walking into the building. The CDC had not implemented adequate access controls to ensure the protection of employees or other resources even at locations where there had been a forced entry by protesters or robbers.

Adherence with basic security controls appeared lax in some locations. For example, we noted employees at several locations did not regularly wear their identification badges as required, and several computers were left unattended after

employees had logged onto the system. We also noted that system printers at some locations were located in unsecured areas, potentially allowing unauthorized personnel access to Privacy Act information or other sensitive data protected by law or regulatory requirements.

DISASTER RECOVERY AND CONTINUITY OF OPERATIONS

The CDC has not updated and tested the disaster plan for its mainframe computer center as necessary to minimize the disruption of vital services in the event of fire, flood, or other disaster. Further, the various centers, institutes and offices composing CDC's user community have not developed their own contingency plans for continuing operations if IRMO's services were materially disrupted. As a result, there is little assurance that CDC could effectively recover from a disaster and continue to fulfill its missions without significant delays.

Contingency planning is an integral part of an adequate security program for any data processing operations. Although contingency plans will not prevent a natural disaster such as a fire, flood, tornado or the like, they can significantly mitigate the effects of such a disaster.

Appendix III to OMB Circular A-130 recognizes the importance of sound contingency planning, as follows:

> "Agencies shall maintain disaster recovery and continuity of operations plans for all information technology installations. The objective of these plans should be to provide reasonable continuity of data processing support should events occur that prevent normal operations at the installation. For large installations and installations that support essential agency functions, the plans should be fully documented and operationally tested periodically at a frequency commensurate with the risk and magnitude of loss or harm that could result from disruption of information technology support.
>
> "Agencies shall establish policies and assign responsibilities to ensure that appropriate contingency plans are developed and maintained by end users of information technology applications. The intent of such plans is to assure that users can continue to perform essential functions in the event their information technology support is interrupted."

The CDC maintains a Disaster Recovery and Contingency Plan for IRMO's computer center operations, and performed two partial tests of that plan in August and December 1991. We noted, however, that sections of the plan dealing with the transfer of data processing operations to contingency sites in the event of a disaster were either not feasible or had not been tested.

As shown in section 5 of CDC's plan, the primary contingency site for use in the event of a disaster is the NCHS computer center in Research Triangle Park, North Carolina. However, CDC's system has recently been upgraded and is no longer compatible with the NCHS system. As a result of the upgrades, application files cannot be run on the NCHS computer without a high risk of erroneous data conversion.

Consequently, it is no longer viable to consider the NCHS computer center for off-site processing, even on a contingency basis. Further, CDC management plans to close the NCHS computer center and transfer the data processing operations to Atlanta, invalidating any consideration of the facility as a contingency site.

The CDC has also proposed PHS' Parklawn Computer Center as a secondary contingency site. While the Parklawn facility may offer greater compatibility with CDC from an operational viewpoint, we found no evidence that CDC had reached a formal agreement with PHS for use of the Parklawn Computer Center in a disaster situation. Further, there is no evidence of any tests to determine the actual viability of using Parklawn as a contingency site.

The deficiencies in IRMO's disaster recovery plan make it more important that its user community plan appropriate actions in the event of a disruption. Yet, we found no evidence that users had developed any specific plans for continuing operations if the computer center were damaged or destroyed.

SECURITY TRAINING

The CDC had not provided an adequate training program to ensure that all employees understand the need for adequate security controls and their individual roles in maintaining adequate security. In addition, neither CDC employees nor contractor personnel working in the computer center had received adequate training regarding emergency response procedures such as fire fighting and safety, equipment shut down, or evacuation. This lack of appropriate training creates unnecessary risks to CDC's data processing operations and increases the danger to CDC employees in the event of a fire or other disaster.

The requirement for adequate training in the area of security is set forth in a number of criteria applicable to the Department, PHS and CDC. For example, Appendix III to OMB Circular A-130 states that:

> "Agencies shall establish a security awareness and training program to assure that agency and contractor personnel involved in the management, operation, programming, maintenance, or use of information technology are aware of their security responsibilities and know how to fulfill them. Users of information technology systems should be apprised of the vulnerabilities of such systems and trained in techniques to enhance security."

The Department's ADP Systems Manual provides detailed standards for required security training programs, including the following:

> "The heads of the OPDIVs, shall, as a minimum,...Develop an employee ADP systems security training, orientation and awareness program to ensure the employee's understanding of (departmental security policies) and his/her responsibility for complying with these policies."

The manual continues to require certain specific training for some employees, such as mandating the training of fire emergency response teams and the performance of fire drills at least annually.

The CDC has not provided adequate training to comply with these criteria. Although CDC includes a security awareness segment in its initial employee orientation, there has been no consistent effort to provide comprehensive training regarding security requirements or techniques to employees on an organizationwide basis.

The lack of organizationwide training showed the greatest impact at those CDC components located in satellite facilities around the metropolitan area. Our visits to selected satellite facilities showed there was little standardization of security controls among CDC components, with specific procedures followed by each office apparently dependent upon the experience and expertise of individual employees. For example, we noted that procedures followed by different components to maintain back-up files for their microcomputer operations ranged from full use of IRMO's contracted off-site storage contract to simply storing back-up disks next to the computer. Further, practices in such areas as password control, encryption, labeling and control of hard copy printouts varied significantly.

More comprehensive training is also required for CDC and contractor personnel within the computer center, particularly in the area of emergency response. The CDC has developed emergency response procedures to be followed by computer room personnel in the event of a fire or other disaster. However, the procedures were not posted in the computer room nor had computer room personnel been provided with adequate training to ensure that the specified procedures were followed. In fact, we were told that computer center staff did not regularly participate in organizationwide fire or evacuation drills conducted by CDC.

CONCLUSIONS AND RECOMMENDATIONS

At the time we began our review, CDC had not established an adequate physical security environment for its data processing operations. As a result, there was only limited assurance that the data processing capabilities and information essential to support the mission of CDC were adequately protected.

The conditions we identified during our review existed in our view because CDC has not placed enough importance on ensuring the integrity of its data processing operations. Specifically, CDC had not corrected known deficiencies in its physical security environment, implemented adequate controls over access to equipment and data, updated and tested its disaster recovery and contingency plans, or provided appropriate security awareness and emergency response training for employees and contractor personnel.

We are recommending that PHS direct CDC to continue its efforts to enhance the security over data processing operations by:

- correcting the facilities deficiencies noted in our review in a cost effective manner--considering the construction of the new computer center scheduled for completion in April 1995;
- developing and implementing organizationwide controls over access to equipment and data;
- updating and testing its disaster recovery and contingency plans; and
- establishing a program providing appropriate security awareness and emergency response training for all employees and contractor personnel.

PHS COMMENTS

In formal comments to the draft of this report, PHS officials concurred with our recommendations and discussed a number of actions initiated by CDC officials demonstrating an increased emphasis on the security of data processing operations. In addition to the action taken in response to specific deficiencies, CDC has named a full time Information Systems Security Officer and has established a permanent subcommittee on Information Security with 30 members representing various CDC components. Also, CDC had contracted for construction of a new mainframe computer center which will incorporate many security measures not possible at the current center. We believe CDC's actions will significantly enhance the security over data processing on an organizationwide basis. For details on the actions planned or taken by CDC to correct these deficiencies and implement our recommendations, see Appendix.

- - - - -

We would appreciate being advised within 60 days on the status of corrective actions taken or planned on our recommendations. Please refer to Common Identification Number A-04-92-03501 in all correspondence related to this report. Should you wish to discuss the issues raised by our review and our recommendations, call me or have your staff contact Michael R. Hill, Assistant Inspector General for Public Health Service Audits, at (301) 443-3582.

APPENDIX

DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Rockville MD 20857

MAY 4 1994

MEMORANDUM

From: Deputy Assistant Secretary for Health Management Operations

Subject: Office of Inspector General (OIG) Draft Report "Physical Security Over Data Processing Operations at the Centers for Disease Control and Prevention (CDC)," A-04-92-03501

To: Inspector General, OS

Attached are the PHS comments on the subject OIG draft report. We concur with the report's recommendation. Our comments describe the actions taken or underway to address the report's findings and recommendation. In addition, we offer several technical comments for your consideration.

Anthony L. Itteilag

Attachment

IG	
SAIG	✓
PDIG	
DIG-AS	✓
DIG-EI	
DIG-OI	
AIG-MP	
OGC/IG	
EXSEC	✓
DATE SENT	5-5

COMMENTS OF THE PUBLIC HEALTH SERVICE (PHS) ON THE OFFICE OF INSPECTOR GENERAL DRAFT REPORT "PHYSICAL SECURITY OVER DATA PROCESSING OPERATIONS AT THE CENTERS FOR DISEASE CONTROL AND PREVENTION (CDC)." A-04-92-03501

OIG RECOMMENDATION

We recommend that PHS direct the CDC to continue its efforts to enhance the security over data processing operations by:

- correcting the facilities deficiencies noted in our review in a cost effective manner--considering the construction of the new computer center scheduled for completion in April 1995;
- developing and implementing organizationwide controls over access to equipment and data;
- updating and testing its disaster recovery and contingency plans; and
- establishing a program providing appropriate security awareness and emergency response training for all employees and contractor personnel.

PHS COMMENTS

We concur. CDC has taken and will continue to take corrective actions to address the findings identified in this OIG report and in CDC's internal reviews/analyses of security over data processing operations. Since CDC staff last met with the OIG auditors in November 1993, considerable progress has been made in planning for, initiating, and completing a number of corrective actions directly relevant to the OIG report's findings and recommendation. Though all corrective actions are not fully implemented, CDC's endeavors to improve this function are manifested in the efforts completed or underway. Among the actions CDC has taken or initiated are the following:

- Made changes to the existing physical facility, including: (1) modified systems to shut down air handlers when smoke is detected; (2) relocated water lines and installed shut-off valves for sprinkler systems; (3) installed air filters in the mixing boxes of the air handling units supporting the computer facility; (4) repaired and replaced as necessary the existing water-proof sheeting used to cover automatic data processing equipment in the event of liquid leakage; (5) improved accessibility to the fire sprinkler system main and clearly marked locations of two shut-off valves; and (6) relocated the operations break facility outside

the computer room. In addition, CDC is in the process of installing emergency power-off switches for the existing computer facility.

- Continued to work closely with the General Services Administration (GSA) and the new building contractor to ensure that safeguards for every physical facility deficiency noted in either the OIG review or the GSA prepared risk analysis are included in the design of the new computer facility.

- Appointed a full-time Information Systems Security Officer (ISSO) who is located in the Office of the Director, Office of Program Support. This action was another step in an ongoing process to maintain and improve the confidentiality, integrity and accessibility of agency data and the overall protection of the Federal Information Processing Systems (FIPS) used at CDC.

  The ISSO is responsible for leadership in reviewing procedures and policies related to information security, identifying sets of sensitive data and critical systems and stimulating the development of security plans, expanding computer security awareness programs, and strengthening information security training and training evaluation. The ISSO works closely with all Centers, Institutes and Offices and with the Information Resources Management Office (IRMO), assisting existing security personnel (IRM Coordinators are Centers/Institutes/ Offices level ISSOs) in performance and evaluation of risk analyses, security plans, etc. The ISSO also reviews information- and computer-related procurement actions for inclusion of appropriate security provisions.

- Continued the effort initiated by the Records Management Activity of the Management Analysis and Services Office to update the inventory of all sensitive data and critical systems at CDC. This effort began in the Summer of 1993 and the inventory update was recently completed. A report on the results is currently being drafted.

  Once the process is completed and verified, the systems will be reviewed for coverage under existing security plans. Where there is no coverage, new security plans will be developed. Also, where update of a security plan is indicated, the plan will be revised. The idea of a central registry of all sets of data and systems, which would include risk analyses, security plans, definition of stewardship responsibilities, and applicable records management schedules, is being explored. If such a registry were to be introduced, a mechanism for

automatically scanning for new data and systems would be an important adjunct.

- Established a 30-member permanent Subcommittee on Information Security to assist the ISSO in the review of all aspects of information security and to draft, as appropriate, proposed changes to procedures, standards, and policies which are applicable to automated information systems security CDC-wide.

  The Subcommittee held its first meeting in February 1994 where it was decided that all members should complete basic security training before beginning work on changing procedures and adopting standards and policies. Basic computer training was completed in April 1994. The next Subcommittee meeting is scheduled for May.

  The Subcommittee will continue to encourage Centers/ Institutes/Offices to develop specific disaster recovery plans, possibly using as a model the plan recently developed by the Agency for Toxic Substances and Disease Registry (ATSDR). The Subcommittee will be asked to review the entire area of security plans, which will include backup and storage strategies, disaster recovery plans, etc., and to act as stimuli within the Centers/Institutes/Offices to hasten their development. Testing of plans, beyond that of the mainframe, is not yet planned and will be presented to the Subcommittee for review and recommendation in appropriate sequence.

  The Subcommittee will address security training in general through the identification and prioritization of subgroups within CDC and the particular security training needs for each subgroup. Finally, the Subcommittee will be asked to define a training evaluation plan in order to better assess training needs and priority populations.

- Continued to address the issue of accessibility to computers and data, and enhance existing security. All doors leading to the power supply and telecommunications rooms have been locked. An audible alarm has been installed at the rear of the computer center to limit use of the door except for emergency purposes. Car key controls are being added to buildings at satellite locations for exterior entrance and access to the main computer center of each building. There are plans to have forced entry alarms installed on all exterior doors.

  The Physical Security Activity maintains a complete and accurate list of all employees and contractors issued card keys with procedures for duplication and voidance of

keys in place. This list is available as requested by programs to monitor authorizations for card keys. In addition, the ISSO works closely with the Physical Security Activity to ensure appropriate issuance and use of card keys and identification badges.

- Formalized its relationship with GSA and the GSA contractor providing the disaster recovery contingency "hot-site," revised its disaster recovery plan, and is currently planning for the first formal test of using the contractor's facility to recover and support CDC's mainframe computer operations.

  Regarding disaster recovery, CDC developed its Local Area Network (LAN) architecture with considerable redundancy, resulting in a wide-area network (CDC-Net) availability of 98.5 percent or better over the past 24 months. The IRMO maintains a backup physical replacement in the event that a single LAN installation fails. In addition, given that there are over 120 separate LANs in production operation, dispersal of users across neighboring LANs could ameliorate short-term impact of even a major focal problem.

- Ensured that procedures are in place that include backup capability for data and text files and network file servers, and uploading of microcomputer data sets for storage on the CDC mainframe. Although not required, use of off-site storage is encouraged for backup sets and IRMO maintains a contract with a commercial off-site storage facility for this purpose.

- Reviewed procurement requests in relation to the newly revised Department of Health and Human Services (DHHS) Automated Information Systems Security Program Handbook, Release 2.0, which is still in draft form. As a result, there has been widespread distribution of the Handbook and considerable discussion of required security activities. The resulting increased awareness among mid-level managers, along with the heightened awareness among senior staff stimulated by the DHHS mailing to all Senior Executive Service staff and Flag Officers in mid-1993, has created an atmosphere of significant interest in the topic of information security and a general review of current procedures.

  In addition, security awareness is enhanced in the following ways. All LAN users (effectively all PC users) are required to use a password of a minimum six characters, to change that password at least every 90 days, and are prevented from re-using previous passwords.

All new employees receive a segment on security awareness as part of the orientation process. All training performed by CDC on the use of specific software packages includes a segment on security awareness. The recently received DHHS package on security self assessment has been distributed to the security Subcommittee and will be considered for universal access via a menu selection on LAN menus.

In pursuit of effective security training for defined groups, database staff, LAN administrators and selected mainframe support staff receive mission specific security training as part of ongoing operational training, as new versions are researched and evaluated prior to implementation, and as new products are evaluated for addition to or replacement of existing software.

The CDC has continued its efforts to enhance security over data processing operations. We believe that the many security related actions CDC has taken during the two-year period since inception of the review demonstrate the emphasis currently being given to computer security at CDC.

TECHNICAL COMMENTS

1. Page 5, paragraph beginning "In November 1993, . . .", last sentence. While a contract for construction of the new building had been awarded in November 1993, actual construction had not begun at that time. However, completion is still scheduled for April 1995.

2. Page 8, ACTIONS TAKEN, first paragraph. The end of the second sentence should read: ". . . and installed new water detectors." The sentence currently reads, ". . . new smoke detectors."

3. Page 8, ACTIONS TAKEN, second paragraph. Please note that while a contract for construction of the new building had been awarded in November 1993, actual construction had not begun at that time.

4. Page 12, ACTIONS TAKEN, first sentence. The GSA was not constructing a new "hot-site" computer center. The GSA was finalizing a Government-wide contract with a commercial "hot-site" computer center vendor.

5. Pages 14 & 15, the last sentence beginning on page 14 and continuing on page 15: The reviewers were advised that a contract had been awarded and construction was about to begin, not that construction had begun.