SEP 22 2000

MEMORANDUM FOR: BERNARD E. ANDERSON
Assistant Secretary
for Employment Standards

/ S /

FROM: JOHN J. GETEK
Assistant Inspector General
for Audit

SUBJECT: OFCCP Information System Security Needs Improvement
Letter Report No. 09-00-005-04-001

During a Region IX computer security controls review, we noted several weaknesses that require Office of Federal Contract Compliance Programs (OFCCP) headquarters action to correct. We met with OFCCP officials on July 19, 2000, to discuss these weaknesses and the corrective actions identified in this letter report. On September 18, 2000, OFCCP provided comments on a draft report. These comments are summarized in this report and attached in their entirety as Attachment A.

Specifically, we are recommending that the OFCCP Information System (OFIS) headquarters personnel (1) assign security responsibility, (2) develop security plans, and (3) properly reauthorize application processing. OFCCP generally agreed with the recommendations and stated that corrective actions either had or would be taken. Additionally, we are issuing a separate letter report to the regional director recommending specific action to correct weaknesses within the regional director's purview.

Introduction and Background

The OFCCP administers laws and regulations that prohibit discrimination by Federal contractors and subcontractors. To assist in accomplishing this mission, OFCCP developed two information systems: (1) the Case Management System (CMS) and (2) the Executive Management System (EIS). Specifically, the CMS is used to measure program performance. CMS is a data entry and reporting tool that provides a display of data concerning the processing of both compliance reviews and complaints. The EIS allows users and managers to access data that track the accomplishments of individual organizational units.

For security purposes, the CMS and the EIS are considered to be a single processing application referred to as the OFIS. The security of the OFIS is governed by OMB Circular A-130. This Circular was issued to provide uniform governmentwide information resources management policies as required by the Paperwork Reduction Act of 1980.

Objective, Scope, and Methodology

Our audit objective was to determine whether OFIS Region IX has adequate and effective management, operational, and technical security controls in place to prevent unauthorized disclosure or modification of sensitive data, or disruption of critical services of its information systems.

Based on the results of our work at Region IX, we expanded our scope to include certain computer security controls at OFCCP headquarters that impacted Region IX security controls. Our review was limited to general controls, including security plan development, risk assessment and contingency planning. This report covers only the issues that are the responsibility of OFCCP headquarters.

We interviewed OFCCP headquarters, Region IX and contractor personnel who were involved in operating and using the information systems. We also obtained and reviewed (1) available security documents from the Office of the Chief Information Officer, (2) training files for OFCCP headquarters and Region IX personnel and (3) security documentation in the OFCCP Region IX and headquarters offices.

The principal criteria used during our audit were:

- OMB Circular A-130: Management of Federal Information Resources.

- Federal Information System Controls Audit Manual (FISCAM), (GAO/AIM-12.19.6).

- National Institute of Standards and Technology (NIST) Special Publications:

    - An Introduction to Computer Security: The NIST Handbook, NIST Special Publication 800-12.

    - Generally Accepted Principles and Practices for Securing Information Technology Systems , NIST Special Publication 800-14.

- Guideline for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18.

We conducted our fieldwork from January 10, 2000, through June 23, 2000. We held an exit conference with OFCCP headquarters on July 19, 2000. At that meeting, we discussed our findings and recommendations. We have incorporated OFCCP comments into this letter report.

We performed our work in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Our audit included such tests of policies and procedures and other auditing procedures we considered necessary in the circumstances.

Audit Results

OFCCP Needs to Improve Security Program for OFCCP Critical Systems

OFCCP needs to improve its security program for the OFIS to better protect the agency's critical systems. OFCCP has not assigned security responsibility, developed security plans for its major application or properly reauthorized application processing, as outlined in OMB Circular A-130. Although OFCCP headquarters officials told us some effort has been applied to these areas, they did not provide documentation to support the level of effort claimed. A systematically and comprehensively planned adequate, cost-effective security program for the OFIS is necessary to protect OFCCP sensitive mission data from vulnerability.

OMB Circular A-130 requires several basic attributes as fundamental for providing adequate security for the application. Specifically, Appendix III of OMB A-130 requires, as a minimum, agency security programs for major applications to include assigning security responsibility, developing a security plan, reviewing security periodically, and reauthorizing application processing.

OFCCP has not complied with these requirements. Specifically, the OFCCP has not:

- **Assigned OFIS system security to a management official knowledgeable about the system, its use, and the personnel involved.**

- **Developed a security plan for the OFIS covering such features as application rules, specialized training, personnel security, contingency planning, technical controls, information sharing, and public access controls.**

- **Performed a review of the security controls in the OFIS at least every 3 years.**

Our review of the OFIS documentation and interviews with OFCCP employees involved in operating the systems identified:

- **No employee was able to define their individual responsibilities over system security.**

! No employee using the OFIS systems had received any security awareness training.

! No contingency plan had been documented for backup planning or disaster recovery.

Because of these weaknesses, employees or contractors may be violating security standards and not be aware of it. In Region IX, for example, we found that a contractor was storing backup tapes of OFCCP sensitive data at a personal residence. Neither the contractor nor OFCCP personnel realized the security breach this posed. If behavior rules had been developed, and security training provided, this might not have occurred. To ensure appropriate system security, OFCCP should develop a security program for the OFIS that incorporates all control requirements in OMB Circular A-130, Appendix III.

According to OFCCP officials, they have begun work on an extensive security program which will correct the weaknesses noted.

Recommendations

We recommend the Assistant Secretary for Employment Standards ensure OFCCP officials:

1. Assign OFIS security responsibility to an OFCCP management official in accordance with OMB Circular A-130.

2. Require OFCCP users of the OFIS to obtain security training.

3. Complete the security program development for the OFIS.

ESA Comments on Draft Report

On September 18, 2000, ESA provided written comments on the draft report. The comments are included in their entirety in Attachment A. In response to the finding and recommendation ESA stated:

> At the time the audit was conducted, OFCCP had not completed its security risk assessment, nor had it completed a System Security Plan for OFIS. Both of these activities were under way and were completed in August. Since their completion, both the OFIS Vulnerability Assessment Report and System Security Plan (SSP) have been submitted to the Office of the Chief Information Officer and the OIG.
>
> As part of the development of the OFIS SSP, OFCCP management designated a Program Security Officer, in writing, who is responsible for the security of OFCCP information systems.

ESA also agreed to provide security training and stated:

> OFCCP concurs with the OIG finding that training regarding desktop security was not provided for the CMS and EIS systems. OFCCP is not responsible for such training. The ESA Division of Information Technology Management and Services (DITMS), which is responsible for the entire infrastructure on which OFCCP systems operate, is in the process of developing an ESA-wide Computer Security Awareness Training Programs to be implemented in FY 2001.

ESA did not agree that a security breach involving storage of back-up tapes at a personal residence applied to OFCCP and requested that we change the audit report.

OIG Evaluation of the OFCCP Comments

ESA's response to the first recommendation to designate an OFCCP management official responsible for OFIS security is sufficient to resolve and close this recommendation.

ESA's response to the second recommendation resolves the recommendation but we will keep the recommendation open until the ESA-wide Computer Security Awareness Training Program is developed and implemented.

Regarding the security breach, while we confirmed that the back-up tapes being stored at a personal residence do not contain OFIS operational data, they do contain OFCCP user identification and password information which we believe is sensitive and should not be stored at a personal residence of an ESA contractor. Therefore, we did not change the report.

We request a response to this report within 60 days. If you have any questions regarding this report, please contact Linda G. Darby, Regional Inspector General for Audit, at (415) 975-4030.

Attachment

Attachment A

OFCCP Comments on the Draft Report