U.S. DEPARTMENT OF LABOR
GENERAL CONTROLS REVIEW OF
SELECTED FINANCIAL SYSTEMS
DETAILED FINDINGS AND RECOMMENDATIONS
REPORT TO THE CIO
September 30, 2000

U.S. Department of Labor
Office of Inspector General
Report Number: 22-01-010-07-001
Date Issued: February 28, 2001

FINDINGS AND RECOMMENDATIONS

REPORTABLE CONDITIONS

To assess the general controls and security over the Electronic Data Processing (EDP) systems that support the financial statements of the Department of Labor (DOL), we conducted reviews using the guidance of the General Accounting Office's (GAO) Federal Information System Controls Audit Manual (FISCAM). The FISCAM is divided into six general control categories: (a) entitywide security program planning and management (SP), (b) access controls (AC), (c) application software development and change control (CC), (d) system software (SS), (e) segregation of duties (SD), and (f) service continuity (SC). In order to provide coverage of the DOL's financial systems, we developed a 5-year strategy based on the functional areas of the financial statements. All systems were scheduled to receive at least one full FISCAM review and some were scheduled for follow-up reviews in the SP & AC areas only. For FY 2000, we performed various levels of review over 12 financial systems within 6 agencies using the FISCAM, as further explained below and within the agency specific sections of this report. The reportable conditions we noted were:

- DOL Needs to Strengthen Controls to Protect Its Information
- DOL Needs to Fully Implement a Systems Development Life Cycle Methodology
- DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

1. DOL Needs to Strengthen Controls to Protect Its Information

During our FY 2000 audit and our continuing review of prior audit issues over the past 3 years, we have found that DOL's systems environment is exposed to various weaknesses in management's procedures for assessing risks, implementing an effective security framework, periodically monitoring its framework, timely resolving issues identified or reported upon, and effectively implementing and maintaining its access controls.

The Department has taken several key steps in strengthening its Information Systems security architecture during the last year. The Department is updating its policies and procedures, issuing guidance and tracking agency compliance. However, the general areas where weaknesses were noted are:

- agencies' ability to periodically perform risk assessments;
- entitywide Security programs and associated weaknesses in developing, implementing and monitoring Local Area Network (LAN), distributed systems, and mainframe environments;
- establishment of a Security Management Structure and Clear Assignments of Responsibilities;
- implementation of Effective Security-Related Personnel Policies and Procedures;

- certification and Accreditation of appropriate general support and major application systems;
- resource owner's identification of authorized users and their access authorized;
- adequate logical controls over the configuration of security parameters, data files, and software programs; and
- monitoring controls.

The GAO report, *GAO/T-AIMD-00-314*, highlights several critical factors about an agency's entitywide security program plan and access controls. GAO's report states, "Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than react to individual problems in an ad-hoc manner only after a violation has been detected or an audit finding reported." The report further states that, "For access controls to be effective, they must be properly implemented and maintained."

Management's Response

The Department takes a "risk-based" approach to protecting its vital information systems. In June 1999, the Department established a Critical Infrastructure Protection Plan (CIPP) as required by Presidential Decision Directive 63 (PDD-63). The CIPP is an action plan that identifies roles and responsibilities, and provides the general time line for milestones, critical path, and supporting security activities for those systems whose loss or misuse would result in a severe impact on the country's critical sectors. An analysis of the Department's systems was completed to identify those systems that were critical to mission operations. The system inventory was further refined by applying the critical asset identification criteria provided by GSA. The security functions addressed in the CIPP include critical infrastructure asset identification; vulnerability assessment; mitigation planning; emergency management; security policy administration; resource requirements, recruitment, retention, education and awareness; and interagency coordination requirements.

In addition to the critical asset activities outlined in the CIPP, the Department updated its overall entity-wide "DOL Cyber Security Program Plan" in October 1999, to address potential risks to all departmental information resources. The Cyber Security Program Plan built upon existing capabilities, but represented a major refocusing of the Department's efforts to protect information resources and the information they process for better mission performance. The Cyber Security Program provides a unified approach to the security of information resources, integrates a variety of technical and management disciplines, and provides security throughout the life cycles of systems and the information they support. Security objectives, processes, resource requirements, roles and responsibilities, and potential issues are identified within the Cyber Security Program Plan. The security functions addressed in the Cyber Security Program include administration of security policy and guidance, risk management, contingency planning, vulnerability analysis and

penetration testing, incident response and reporting, and computer security awareness and training.

The Office of the Chief Information Officer has provided risk assessment training and guidance to the agencies in order to achieve the milestones outlined within the Cyber Security Program Plan and CIPP. In accordance with Federal guidance, and as required by the CIPP and Cyber Security Program Plan, each agency applied the systematic approach, documented in the Computer Security Handbook, to complete system security plans and risk assessments for those systems identified as critical assets, major applications or general support systems.

System security plans identify roles and responsibilities, and contain detailed information about the system environment, management controls, operational controls, and technical controls needed to protect the information processed by the system from unauthorized access. Risk assessments identify roles and responsibilities, and contain detailed information pertaining to the sensitivity and criticality of the system, asset component identification and loss impact, potential threats and vulnerabilities, and evaluation and selection of safeguards to protect the system.

The system security plans and risk assessments were reviewed by the Office of the Chief Information Officer to ensure compliance with Departmental guidance. In December 2000, each departmental agency completed development of agency-centric "Cyber Security Program Plans" that address full implementation requirements outlined within the CIPP and departmental Cyber Security Program.

The Department updated its Information Technology (IT) Architecture and included security standards within the Technical Reference Model, of the Information Technology Architecture, in March 2000.

The Department established a Systems Development and Life Cycle Management Methodology[1] in July 2000, to provide systematic design, development, and documentation standards for information technology systems, including the application of security measures throughout a system's life cycle. The Department also updated its Computer Security Handbook to provide guidance for developing and implementing agency-specific cyber security programs, system security plans, contingency plans, vulnerability assessments, incident response and reporting, and security awareness and training. The Computer Security Handbook also established the Department's Emergency Incident Response Team.

The Office of the Chief Information Officer conducted its annual computer security awareness training for Department of Labor employees in October 2000, and provided specialized information technology security training for information technology professionals.

Budgetary support for achieving infrastructure improvements and systems protection was

[1] www.dol.gov/dol/cio/public/programs/it/itamain.htm

obtained through the Department's Information Technology Capital Planning and Management process. Through this process, departmental information technology security, privacy and related requirements were identified, quantified in terms of cost and benefits, and managed through the Systems Development and Life Cycle program. The Department established an integrated multi-year budget, which specifically includes "Security and Privacy," beginning in FY 2001 to ensure adequate financial resources are available to strengthen the Department's Cyber Security program.

The Office of the Chief Information Officer is in the process of formulating departmental guidance to implement the recently enacted "Government Information Security Reform," (P. L. 106-398, October 30, 2000), and OMB "Guidance On Implementing the Government Information Security Reform Act."[2] Together, implementation of these new initiatives will continue to ensure that DOL systems are operated in a way that is secure against threat and loss.

2. DOL Needs to Fully Implement a Systems Development Life Cycle Methodology

During our FY 2000 audit and our continuing review of prior audit issues over the past three years, we have found that changes to the system were not properly controlled. The Department has issued its Systems Development Life Cycle (SDLC) Manual and agencies are updating systems to comply with the manual. However, the general areas where weaknesses were noted are:

- Program modifications were not properly authorized
- Testing and approval of new and revised software changes were not performed, evidenced, or formally conducted
- Access to software libraries was not strictly controlled
- Critical system documentation was not developed or updated

The GAO report, *GAO/T-AIMD-00-314*, states, "Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are to ensure that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and to ensure that different versions are not misidentified."

[2] Office of Management and Budget, "Guidance On Implementing the Government Information Security Reform Act," M-01-08, January 16, 2001, www.whitehouse.gov/omb/memoranda/m01-08.pdf

Management's Response:

The Department's Systems Development and Life Cycle (SDLC) Management Manual, was issued in July 2000. The SDLC serves as the mechanism to assure that developing, modifying, or enhancing systems meet established user requirements and support DOL critical success factors. It sets forth a standard and logical process for managing IT system development activities and acquisition approvals that are controlled, measured, documented, and ultimately improved while responding to Federal guidance and regulations. The SDLC represents a seven-phase structured approach to developing and managing IT projects from the initial concept to disposition (retirement). The concepts presented are the foundation for the life cycle management approach adopted by the DOL to improve the quality of their information technology systems.

The concepts included within the SDLC address strategic planning, business process reengineering, roles and responsibilities, and provide a detailed description of each life cycle phase and the corresponding documentation produced as a result of completing each phase. The seven phases each system would progress through are conceptual planning, planning and requirements definition, design, development and testing, implementation, operations and maintenance, and finally, the disposition phase used to retire legacy systems. As noted by the Office of the Inspector General, the Department is in the process of fully implementing the SDLC. Implementation of the SDLC will ensure program modifications are authorized, testing and approval of new and revised software changes are performed, access to software libraries are controlled, and critical system documentation is developed or updated.

3. DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

During our FY 2000 audit and our continuing review of prior audit issues over the past three years, we have found that the Department has several weaknesses that would impair the Department's ability to effectively respond to a disruption in business operations as a result of a disaster or another event causing an extended service interruption. The Department issued guidance to address service continuity in its Computer Security Handbook. However, the general areas where weaknesses were noted are:

- Risks assessments have not been finalized that identify critical operations and resources (people, hardware, software, data, etc.).
- Alternate data processing and telecommunications facilities have not been identified for all the critical financial systems reviewed.
- Agencies are in the process of drafting or revising contingency plans; however, contingency plans have an "IT" focus and do not fully take into account the business operations activities.

The GAO report, *GAO/T-AIMD-00-314* states, "Service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and crucial, sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in the disaster simulation exercises."

Management's Response:

The Department has established a multi-year strategy and program management plan for its Continuity of Operations (COOP). As articulated in the COOP, the Department must have a viable capability that ensures the emergency delegation of authority; safekeeping of vital resources, facilities, and records; improvisation or emergency acquisition of the resources necessary for business resumption; capability to perform work at alternate work sites until normal operations are resumed; and the ability to be operational at alternate facilities, with or without warning within a specified amount of time after activation.

In addition to meeting COOP requirements, the Department must have a Continuity of Government (COG) Plan for discharging its Department's role in maintaining the integrity of critical constitutional functions of the Government in the event of a threat to national security.

In response to Federal guidance, the Department completed draft COOP and COG plans and submitted those plans to the Federal Emergency Management Agency (FEMA) in October 1999. The consolidated FEMA/NSC assessment of Government-wide emergency preparedness, released in September 2000, concluded that DOL plans are a good start but work is needed to develop the detailed procedures and training program that will make the plans truly viable. COG details are highly classified, but unclassified versions of the draft COOP and COG plans were provided to the Office of the Inspector General (OIG) for review. However, the OIG request for COOP and COG information did not occur until after completion of the field work for the general controls review of selected financial systems. Therefore, the Department expects this reportable condition will be significantly updated once the OIG has completed its review of the COOP and COG plans and associated activities.

In addition to the over-arching COOP and COG plans, the Departments' Computer Security Handbook, updated in April 2000, provides departmental guidance for developing agency-specific cyber security programs and system security plans. As noted above, the Handbook specifically addresses contingency planning. The Office of the Chief Information Officer will continue to assist agencies with their CIPP and Cyber Security Program Plans to fully implement the operation guidance contained within the Computer Security Handbook.

OFFICE OF THE CHIEF FINANCIAL OFFICER (OCFO)

We tested general controls and security over EDP systems of the OCFO as they pertain to the following critical financial applications:

- Department of Labor Accounting and Related Systems (DOLAR$)
- Integrated Payroll System (IPS)

GAO's Federal Information System Controls Audit Manual (FISCAM) was used to guide testing. The scope of testing included the six FISCAM general controls sections: (1) Entitywide Security Program Planning and Management (SP), (2) Access Controls (AC), (3) Application Software Development and Change Control (CC), (4) System Software (SS), (5) Segregation of Duties (SD), and (6) Service Continuity (SC). In addition, prior year issues reported by management as being closed during the period under review were also tested using the FISCAM.

The DOLAR$ and IPS applications reside on a mainframe located at the SunGard Data Center in Voorhees, New Jersey; thus, our scope was limited to the EDP controls that are the responsibility of OCFO as they relate to the mainframe processing of DOLAR$ and IPS. The following outlines the controls deemed out of scope and were not tested:

- Controls that are the responsibility of DOL's contractor, SunGard. SunGard supports and maintains the mainframe operating system and physical environment used to process and store DOLAR$ and IPS application data. These controls are covered as part of the SunGard SAS 70 review.
- The OASAM Data Center, located at the Frances Perkins Building, in Washington, DC, contains telecommunications equipment used by the OCFO to connect to the SunGard Mainframe. Therefore, issues associated with physical security, data center operations and service continuity are reported in the OASAM section of this report.

1. DOL Needs to Strengthen Controls to Protect Its Information

<u>Current Year Findings and Recommendations</u>

a. IDMS Security Parameters And Monitoring

During the FY 2000 audit, we found that the OCFO has not implemented adequate logical controls over the IDMS database for DOLAR$. Specifically, it was found that:

- Password parameters are weak:
  - minimum password length is only two characters,
  - users are not required to change their passwords,
  - password history files are not being maintained,
  - special characters are not required to be used when composing passwords, and

- lockout parameters are ineffective to disable an ID after a predetermined number of unsuccessful login attempts.

- Monitoring controls are weak:
  - IDMS access violations are not reviewed, and
  - changes to IDMS profiles (adding, modifying and deleting IDMS IDs and access privileges) are not reviewed.

Inadequate controls over the establishment of password parameters may lead to the risk of passwords being easily guessed allowing an unauthorized user the ability to gain access to systems resources. Lacking controls to monitor changes or violations in the system creates a risk that improper or illegal access to the database will go undetected. Establishing such precautions mitigates any fraud or misuse of the system by allowing all access to be tracked and properly logged for further analysis and investigation.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- NIST 800-12: *An Introduction to Computer Security*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient policies and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged", and the emergency access. In addition, SSPs should include specific technical standards (security settings, critical system configuration, etc.) for each general support system and major application.***

Management's Response:

The DOLAR$ SSP will be updated to incorporate these items of concern about passwords and how the OCFO plans to improve on them. The DOLAR$ SSP will also include monitoring practices and procedures for user IDS. The OCFO expects to have these items included in the DOLAR$ SSP by the end of the second quarter of FY 2001.

OIG's Conclusion:

We concur with management's plan to correct this weakness. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

b. Logical Controls to Prevent or Detect Unauthorized Access

During the FY 2000 audit, we found that policies and procedures over the authorization, modification, and periodic monitoring of users (end users, contractors, production support, etc.), having logical access to the IPS environment (application, operating system, databases, utilities, etc.), require improvement. Specifically, the following weaknesses were identified:

- Access had not been revoked or removed from the system 2 of 23 IDS deemed obsolete (e.g., had not been accessed between 60 days and 7 years).
- Multiple IDS' had been granted to 7 of the 23 users selected for testing.
- Periodic reviews of access privileges are not performed.
- An excessive number of users' IDS (an estimated 200) were maintained on the system in a "revoked" status.
- Consistent password intervals were not being used. Specifically, 3 of the 23 IDS tested did not have their password interval set to 30 days.

Without clearly defined policies, procedures and assignment for security administration, security administrators may not fully be aware of management's security objectives and may not be consistently performing the necessary procedures required to provide effective control. Specifically,

- Undocumented or out-of-date access request forms may compromise the integrity of the system by granting access that is not consistent with management's security objectives, authorized intent, or user job responsibilities.
- Inadequate controls over the monitoring and removal of obsolete or inactive IDS from the system increases the risk of unauthorized access to system resources.
- Inadequate monitoring of access violations and changes to user profiles increases the risk that unauthorized attempts to gain access to system resources or unauthorized modification of user access will go undetected.

This may diminish the integrity and reliability of data and increase the risk of destruction or inappropriate disclosure of sensitive data.

The following criterion was used in reporting this finding:

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

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure that agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient polices and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and emergency access. A recertification should be conducted of all IDS on the system, the business need documented, password interval adjusted appropriately, obsolete and/or revoked IDS removed, and a unique (single) ID assigned to each user.***

Management's Response:

- Inactive IDS of the last few users for which obsolete data was on record have been removed from all systems. The SSPs will include the appropriate guidelines for monitoring and managing revoked and removed access privileges.
- The OCFO SSPs will include guidelines for issuing multiple user ids to individual users.
- The OCFO SSPs will include the schedule for periodic reviews of access privileges.
- The SSPs will include the appropriate guidelines for monitoring and managing revoked and removed access privileges.
- The OCFO has completed the recertification of DOLAR$ and IPS users and now has comparable data on user and access authority on file. The SSPs will include the appropriate forms and guidelines for maintenance of these forms.
- The OCFO SSPs will include guidelines for password interval conventions.

OIG's Conclusion:

We concur with management's actions and plans to correct these weaknesses. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Status of Prior Year Findings and Recommendations

Risk Assessment

During our FY 1998 audit (OIG Report No. 12-99-002-13-001), we found the OCFO developed a risk assessment as part of the Y2K preparedness strategy. However, the risk assessment does not consider data sensitivity and integrity, the range of risks to the entity's systems and data, and resource classifications for the OCFO's systems (DOLAR$ and IPS). In addition, the issue could

not be fully considered resolved until the CIO implements the SSP as noted in the OIG's FY 98 recommendation. We made the following recommendation to the Chief Information Officer and Assistant Secretaries:

- ***ensure entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, and access monitoring.***

During our FY 2000 audit, we found that the OCFO has performed a Vulnerability Assessment/Risk Analysis for DOLAR$ on August 14, 2000, entitled "Final Report - DOLAR$ Risk Assessment," using the guidance provided by The Vulnerability Assessment Methodology Guide that has been included as Appendix B of the Computer Security Handbook, and the RiskWatch software. The IPS Risk Assessment, though not fully completed during the period under review, was under final approval by the OCFO. The IPS Risk Assessment is being created following the same methodology as DOLAR$. Management plans to address resource classification (e.g., Integrity, Availability, and Confidentiality) in their Security Plans which will be complete in the 1st quarter of FY 2001. Therefore, this recommendation is **resolved and open**. Closure is dependent on our review of the IPS Risk Assessment.

Management's Response:

The report correctly notes the status of SSPs as of the end of the fiscal year. Subsequent to that date, the OCFO formally submitted the SSP for DOLAR$, including the formal risk assessments, by the end of the first quarter, has to-date received two cycles of CIO-recommended clarifications to that plan, and will resubmit the next version to the CIO by the end of the second quarter. The IPS-related material has been submitted to the CIO and we are waiting for the CIO's response. Pending receipt and evaluation of the CIO's response, we expect to have the final round of submissions for IPS by the end of the third quarter.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Entitywide Security Program Plan

During our FYs 1998 and 1999 audits (OIG Report No. 12-99-002-13-001 and 12-98-002-13-001), we found the security plans for the OCFO were currently in draft and management was still in the process of finalizing the document. In addition, a policy was not in place requiring the plan to be updated periodically, when the systems environment changes, a security incident occurs, etc. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, access monitoring, and***
- ***ensure computer security plans are developed and implemented for all departmental systems.***

During our FY 2000 audit, we found that the DOLAR$ and IPS System Security Plan (SSP) are currently being developed using guidance from the Department of Labor Computer Security Handbook. According to management, completion of the DOLAR$ SSP is expected by the 1st Quarter of FY 2001. Therefore, these recommendations are **resolved and open**. Closure is dependent on our review of the DOLAR$ and IPS System Security Plan.

Management's Response:

As previously noted, the OCFO expects to issue its final DOLAR$ SSP by the end of the second quarter and the IPS SSP by the end of the third quarter. We expect to complete the entitywide OCFO security plan by the end of the first quarter of FY 2002.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 and the FY 2002 audits.

Security Management Structure and Security Responsibilities

During our FY 1998 audit (OIG Report No. 12-99-002-13-001), we found that an independent group responsible for security administration had not been established within the OCFO. We also found that there is no overall system security manager for DOLAR$. We made the following recommendation to the Chief Information Officer and Assistant Secretaries:

- ***ensure entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, access monitoring.***

During our FY 2000 audit, we found that the DOLAR$ and IPS SSPs will include a security management structure that clearly assigns security responsibilities over its systems and various programs. DOLAR$ has a formal Application Security Manager; OCFO has a designated overall System Security Administrator. The DOLAR$ SSP is currently being developed using guidance from the Department of Labor Computer Security Handbook. Completion of the DOLAR$ SSP is expected by the 1st Quarter of FY 2001. Therefore, this recommendation is **resolved and open**. Closure is dependent on our review of the DOLAR$ and IPS System Security Plans.

Management's Response:

The OCFO has been establishing a formal systems security infrastructure featuring an overall agency security official and clearly delineating individual roles and responsibilities across the entire organization. The infrastructure will meet or exceed all DOL-published security standards. Target date for completion is the end of FY 2001.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Security-Related Personnel Policies

During our FYs 1998 and 1999 audits, (OIG Report No. 12-99-002-13-001 and 12-00-002-13-001), we found that the OCFO needed to improve the effectiveness of its security controls related to personnel policies and procedures. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure that employees are required to attend training and maintain the appropriate documentation (e.g., lists of employees as of the training course date, attendance sheet of employees taking the course, topics, agendas, handouts, etc., provided during the program),*** **and**
- ***ensure that background checks are conducted for all Government employees and contractor management personnel with high levels of system access.***

During our FY 2000 audit, we found the following:

- The OCFO has completed the sensitivity level assessment of positions to determine if they are of High, Moderate or Low risk, to ensure that individuals have the appropriate background screening.
- Clearances are currently being processed for personnel identified.
- According to Management, 5-year reinvestigation will be scheduled, as necessary. Therefore, all reinvestigation have not been completed or are in progress.
- The OCIO provides annual and refresher security awareness training to all employees. Most recently, the CIO's memorandum entitled Computer Security Awareness Video, dated December 16, 1999, was released disseminating copies of the video "Safe Data: It's Your Job" to all agencies. According to Management, viewing of this video satisfies the OMB Circular A-130 requirement to provide security awareness training to all employees on a regular basis. Records documenting employees' attendance were not available for review to evidence that OCFO employees attended this training.
- According to Management, Confidentiality Agreements will be signed, as necessary. Therefore, all Confidentiality Agreements have not been complete or are in progress.

- According to Management, Position Descriptions (PDs) will be updated, as necessary. Several PDs' descriptions were reviewed as part of the audit and noted that new descriptions had been created for some positions. However, others were not updated. Therefore, management is still in the process of ensuring that outdated PDs are updated.

These recommendations are **resolved and open**. Closure is dependent on our review of the OCFO's security controls related to personnel policies and procedures for the FY 2001 financial statement audit.

Management's Response:

- The OCFO has targeted the end of FY 2001 to initiate all critical background investigations. The positions that require background investigations will be incorporated into the appropriate SSPs.
- The OCFO SSPs, all of which expect to be completed by the end of FY 2001, will include the periodic reinvestigation schedules.
- The OCFO entitywide SSP, due by the end of the first quarter of FY 2002, will include the OCFO security awareness and training program.
- The OCFO SSPs, all of which expect to be completed by the end of FY 2001, will include the requirements of confidentiality agreements with contractors. The OCFO has already begun this practice with their two major support contract companies.
- The OCFO has targeted the end of FY 2001 to complete all critical position description changes.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 and FY 2002 audits.

Accreditation and Security Reviews

During our FY 1998 and FY 1999 audits (OIG Report No. reports 12-99-003-13-001 and 12-00-003-001), we found that the OCFO had not periodically assessed the appropriateness of security policies and compliance with them. Specifically, we found that DOLAR$ and IPS:

- have not been authorized or accredited by the system manager whose mission is supported by the application, and
- have not undergone an independent applications review or audit in the last 3 years.

We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure that agencies are in compliance with the security handbook by verifying that all financially significant applications support systems have been properly accredited and that independent functional reviews are conducted at least every 3 years, and***
- ***ensure that all departmental systems are accredited by the program management.***

During our FY 2000 audit, we found that the DOLAR$ SSP is expected to be implemented during the 1st quarter of FY 2001 and will include the authorizing and accrediting of the DOLAR$ system. Management presented two reviews of the DOLAR$ application. Anderson Consulting, Inc. (October 23, 1997), and Troy Systems, Inc. (September 30, 1998), conducted the reviews. The scope of the reviews only covered assessing and making recommendations surrounding the security policies and procedures of the DOLAR$ outdated security plan. Management is in the process of addressing the recommendations made in these reviews as it completes the DOLAR$ SSP. DOLAR$ has not undergone an independent application controls review or audit. Therefore, these recommendations are **resolved and open**. Closure is dependent upon our review of a current independent application controls review or audit for DOLAR$ and IPS.

Management's Response:

DOLAR$ and IPS SSPs, as discussed earlier, will include the date of authorization and name and title of the management official authorizing processing, by the end of FY 2001. Based on discussion following last year's audit, the OCFO committed to obtaining an independent review of the accounting and payroll systems operations. These reviews are expected to begin by the end of FY 2001.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 and FY 2002 audits.

Logical Controls to Prevent or Detect Unauthorized Access

During our FY 1998 and FY 1999 audits (OIG Report No. 12-99-003-13-001 and 12-00-003-001), we found that policies and procedures over the authorization, modification, and periodic monitoring of users (end users, contractors, production support, etc.), having logical access to the DOLAR$ environment (application, operating system, databases, utilities, etc.), required improvement. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure that agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient polices and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition,***

IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access, and

- ***ensure all departmental Computer Security Plans have polices and procedures for user access, physical access, and monitoring of sensitive and critical resource access.***

During our FY 2000 audit, we found that the DOLAR$ user community is relatively small and responsibility for requesting and deleting access has been with the Department's finance offices. The Office of Accounting and Payment Services (OAPS) recently implemented a periodic recertification process that includes a comparison between a user's actual access level and a user's granted access level. Additionally, there are updates made periodically because of changes within the staff. The changes within the staff bring about changes in user duties, which cause modification in user access level, whether it may be temporary or permanent.

The OCFO recognizes the need to institutionalize the process of continually reviewing DOLAR$ users to ensure they have a business need to access DOLAR$. The OCFO will issue and implement policies and procedures to:

- require that all current users, including those with read only access, complete and that supervisors approve a new form requesting access to DOLAR$;
- require on a 3-year cyclical basis beginning with FY 2001 that all users complete and that supervisors approve a new form requesting DOLAR$ access;
- require that all obsolete user IDS are removed from DOLAR$;
- control the use of multiple IDS granted to individual users;
- evaluate on a continuing basis the level of access to DOLAR$; and
- establish criteria for removing revoked IDS from the system.

These recommendations are **resolved and open**. Closure is dependent upon our review of the new OCFO policies and procedures to control access to DOLAR$.

Management's Response:

- The OCFO has completed the recertification of DOLAR$ and IPS users and now has comparable data on user and access authority on file. The SSPs will include the appropriate forms and guidelines for maintenance of these forms.
- Inactive IDS of the last few users for which obsolete data was on record have been removed from all systems. The SSPs will include the appropriate guidelines for monitoring and managing revoked and removed access privileges.
- The OCFO SSPs will include guidelines for issuing multiple user ids to individual users.
- The OCFO SSPs will include the schedule for periodic reviews of access privileges.
- The SSPs will include the appropriate guidelines for monitoring and managing revoked and removed access privileges.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Access Monitoring and Security Violations

During our FY 1999 audit (OIG Report No. 12-00-003-001), we found that the OCFO's security monitoring controls over the mainframe platform required improvement. We made the following recommendation to the Chief Information Officer and Assistant Secretaries:

- ***ensure that agencies are in compliance with the computer security handbook and that agency SSPs (for its GSS and MAs) include appropriate policies and procedures for the monitoring of inappropriate or unusual activity occurring on the system. Policies and procedures should include, but are not limited to management's determination of what constitutes a violation of the policy, the frequency of reviews, reporting and escalation processes, and maintenance of documentation (manual or automated) for audit trail purposes, etc.***

During our FY 2000 audit, we found that OCFO management was committed to ensuring that the DOLAR$ (and IPS) SSPs will include appropriate policies and procedures for the monitoring of inappropriate or unusual activity occurring on the system. Policies and procedures will include management determination of what should be recorded on logs and what constitutes a violation of the policy, frequency of reviews, reporting and escalation processes, and maintenance of documentation (manual or automated) for audit trail purposes, etc. During our review, we found a first draft of these procedures. Therefore, this recommendation is **resolved and open**. Closure is dependent upon our review of the final OCFO procedures.

Management's Response:

The OCFO SSPs, both of which expect to be completed by the end of FY 2001, will include appropriate policies and procedures for the monitoring of activity and security related reports.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

2. DOL Needs to Fully Implement a Systems Development Life Cycle Methodology

Current Year Findings and Recommendations

a. Change Control Policies and Procedures

During our FY 2000 audit of the IPS change control methodology and procedures, we found several weaknesses:

- IPSs change management methodology needs to be enhanced to comply with the U.S. Department of Labor's Systems Development and Life Cycle Manual.
- There is no evidence of appropriate authorization methods for software modifications within the IPS system.
- There is no evidence of test plan standards and proper reviews of test results corresponding to changes in the IPS system software.

Without controls over the modification of application software programs and the movement of programs and data among libraries, IPS runs the risk of unauthorized program and data changes. For example, improper changes could be incorporated into the program, causing processing irregularities, hampering further system development at a future time or causing security features to become inoperable.

The following criteria were used in reporting this finding:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure the SDLC process is followed by all DOL and contractor personnel who are developing, acquiring, or managing systems or making enhancements to existing systems.***

Management's Response:

IPS uses an application migration management system which does, in fact, indicate the who, what, and when of any change. The OCFO has updated documentation of the change control process in IPS. Change Control Request/Authorization numbers are now embedded in the comments of all

code modifications, providing an audit trail of the process from the authorizing official's request through to the migration of software from the test environment to the production environment.

The test environment provides ample means for programmers to test their code modifications against parallel data. Test results are reviewed for approval by the application team leader before being passed to the Division Chief for final approval and migration. The OCFO believes that this finding can be closed in FY 2001.

OIG's Conclusion:

We concur with management's actions and plans to correct these weaknesses. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit to ensure compliance with the Department's SDLC.

b. Critical Documentation

During our FY 2000 audit, we found that the OCFO has not updated or does not have application documentation for its critical systems (DOLAR$ and IPS) such as user manuals, maintenance manuals, operational manuals, etc., to reflect the systems' current operating environment. For example:

- The DOLAR$ User Manual has not been updated since 1987.
- Documented procedures for using "Easytrieve" to generate critical financial reports do not exist.

In the absence of adequate application instruction manuals, transactions can be incorrectly processed. Without instructions detailing the application's operation and security features, a user without adequate knowledge will have difficulty utilizing the application, increasing the risk of corrupting critical/sensitive data. Users could inadvertently grant inappropriate access and/or perform security violations. In the event that proficient users are unavailable, the agency may not be able to effectively operate the application or generate critical reports.

The following criteria were used in reporting this finding:

- The Systems Development and Life Cycle Manual, Version 2.0
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure the SDLC process is followed by all DOL and contractor personnel who are developing, acquiring, or managing systems or making enhancements to existing systems. The SDLC Manual includes requirements for developing and periodically updating user manuals, maintenance manuals, operational manuals, system administrators manuals, etc.***

Management's Response:

OCFO is in the process of developing a computer based training (CBT) product for DOLAR$. The first phase delivery is expected in July 2001. OCFO plans to expand the use and content of this tool to eventually provide full end user documentation and training for DOLAR$. OCFO has completed the basic system documentation for both DOLAR$ and IPS and continues to upgrade/update them (job controls, run books, scheduling, requirements and data dictionaries). Even though the IPS users' manual has not been upgraded since 1987, very little has changed from the end user point of view, and for those items that have been modified or enhanced, OCFO has communicated these modifications to the users and has issued user instructions. By the end of FY 2001 OCFO will evaluate the cost/benefit of updating the current IPS user manuals or waiting until the new payroll application, which will have substantial user documentation, is released in FY 2002 . Note: Easytrieve is not currently in production control.

OIG's Conclusion:

We concur with management's actions and plans to correct these weaknesses. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit to ensure compliance with the Department's SDLC.

Status of Prior Year Findings and Recommendations

Change Control Policies and Procedures

During our FY 1998 and FY 1999 audits (OIG Report No. 12-00-003-13-001 and 12-99-003-001), we found that DOLAR$ did not have up-to-date change control policies and procedures. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure the SDLC process is followed by all DOL and contractor personnel who are developing, acquiring, or managing systems or making enhancements to existing systems, and***
- ***ensure that the application change control policies and procedures are developed and implemented for all departmental systems, including procedures to implement an automated tool for application version control where applicable.***

During our FY 2000 audit, we found that OCFO management identified the need to update its SDLC practices, however, it was waiting for the CIO's Systems Development Life Cycle Manual. The CIO's SDLC manual was issued. Prior to the SDLC's issuance, the OCFO anticipated several changes through review of the draft CIO's SDLC manual and began to implement new procedures that included:

- formalizing approvals of changes,
- using flow charts to document the change cycle,
- using logs to track all changes, and
- looking at formalizing testing procedures for changes made to the system, etc.

These recommendations are **resolved and open**. Closure is dependent on our review of the OCFO updated SDLC practices.

Management's Response:

The finding correctly notes the status of the finding and the changes implemented.

- During FY 2001, OCFO has begun to document source code change information in the modules themselves, thus assisting in our configuration management. As time permits, OCFO is further codifying prior year changes where there might be inconsistencies in the migration materials for DOLAR$. The OCFO believes this finding can now be closed.
- The DOLAR$ SSP contains the policies and procedures for the change control process. The OCFO believes this finding can now be closed.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit to ensure compliance with the Department's SDLC.

3. DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

Current Year Finding and Recommendation

a. Disaster Recovery Plan

During our FY 2000 audit, we found that the OCFO's "Business Continuity Plan," dated December 1999 is too narrow in scope (addresses Y2K scenarios) and does not sufficiently address all critical objectives for a contingency plan as defined in the CIO's CSHB Attachment C-Contingency Planning Methodology Guide. By not having a comprehensive contingency plan that has been formally approved, documented in sufficient detail, and adequately tested, DOLAR$ may not be able to adequately recover from an extended service interruption. The inability to recover in the event of a disaster or extended service interruption may result in the loss of data.

The following criteria were used in reporting this finding:

- DOL Computer Security Handbook
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- FIPS Pub. No. 87, *Guidelines for ADP Contingency Planning*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agencies are in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility; plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training primary and back-up personnel, and frequency of updates, testing, etc.***

Management's Response:

The OCFO has been working to comply with all the requirements for appropriate documentation. Given the commitment to address security documentation first, the OCFO will address the updates of its business continuity and contingency planning during the later part of FY 2001. OCFO expects to have the appropriate documentation in place by the end of FY 2001.

OIG's Conclusion:

We concur with management's actions and plans to correct these weaknesses. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Status of Prior Year Findings and Recommendations

Disaster Recovery Plan

During our FY 1998 and FY 1995 audits (OIG Report No. 12-98-003-13-001 and 12-96-003-001), we found that the DOLAR$ Disaster Recovery/Business Continuity Plan did not have a complete inventory listing of items such as computer hardware, software, and telecommunications needed for operations. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure written disaster recovery plans are developed where needed, and***
- ***ensure each agency develops the required contingency plan. In addition, the CIO should ensure that appropriate test plans (full and partial) are conducted on a periodic basis.***

During our FY 2000 audit, we found that access to DOLAR$ is through the ECN and if the ECN becomes inoperable, DOLAR$ would rely on the mechanism used by the ECN in this case. The OCFO will include as part of its disaster plan, those portions of the ECN disaster recovery plan which DOLAR$ would rely on if the ECN became inoperable.

In addition, management stated the DOLAR$ application resides on a contracted mainframe system that was just recently accredited in February 2000 as meeting the security requirements of OMB Circular A-130. As confirmed by the contractor (SunGard), the disaster recovery services include user access. Based upon the information provided by management, the OCFO will include an inventory of items such as computer hardware, software, and telecommunications needed for operations as it continues its efforts to develop its disaster plan. Therefore, these recommendations are **resolved and open**. Closure is dependent on our review of the DOLAR$ revised disaster recovery plan.

Management's Response:

The OCFO is working with the CIO to establish the cross-referencing materials to conform their respective disaster recovery plans and manuals, and keep inventories up to date. In addition, the continuity plans will also be cross-referenced in the DOLAR$ systems documentation. All updates should be completed by the end of FY 2001.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions during the FY 2001 audit.

EMPLOYMENT STANDARDS ADMINISTRATION (ESA)

We tested general controls and security over EDP systems of the ESA as they pertain to the following critical financial applications:

- Federal Employees' Compensation System (FECS)
- Backwage Collection and Disbursement System (BCDS)
- Civil Monetary Penalties System (CMP)
- Longshore System (LS)
- Automated Support Package (ASP)

GAO's Federal Information System Controls Audit Manual (FISCAM) was used to guide testing. The scope of testing included two FISCAM general controls sections: (1) Entitywide Security Program Planning and Management (SP) and (2) Access Controls (AC). In addition, prior year issues reported by management as being closed during the period under review were also tested using the FISCAM. We followed up on prior year findings from two other FISCAM general controls sections: (1) Application Software Development and Change Control (CC) and (2) Service Continuity (SC).

The BCDS and CMP applications both reside on the same production server located in the ESA Data Center; thus, we tested the EDP controls over that server. The LS application resides on the different server also located in the ESA Data Center; thus, we tested the EDP controls over that server as well. Because the three financial applications reside on servers located in the ESA Data Center and access to these servers are the responsibility of ESA's Division of Information Technology Management and Services (DITMS), we tested the access control policies and procedures of DITMS, focusing on the three applications mentioned above.

The FECS application resides on a mainframe located at the SunGard Data Center ; thus, our scope was limited to the EDP controls that are the responsibility of ESA as they relate to the mainframe processing of FECS. The following outlines the controls deemed out of scope and were not tested:

- Controls that are the responsibility of DOL's contractor, SunGard. SunGard supports and maintains the mainframe operating system and physical environment used to process and store FECS application data. These controls are covered as part of the SunGard SAS 70 review.
- Controls associated with the Unix environments running the client server portion of FECS. Unix is the platform used as a Front End Processor (FEP) that initially processes and transmits FECS information from the 13 district offices to the SunGard mainframe.

The ASP application resides on a mainframe located at the Computer Science Corporation (CSC) Data Center; thus, our scope was limited to the EDP controls that are the responsibility of ESA as they relate to the mainframe processing of ASP. The following outlines the controls deemed out of scope and were not tested:

- Controls that are the responsibility of DOL's contractor, CSC. CSC supports and maintains the mainframe operating system and physical environment used to process and store ASP application data. These controls are covered as part of the CSC SAS 70 review.

- Controls associated with the Division of Coal Mine Workers' Compensation Data Center, which is run by CSC contractors, that contains telecommunications equipment used by the nine district offices and the National Office to connect to the mainframe.

1. DOL Needs to Strengthen Controls to Protect Its Information

Current Year Findings and Recommendations

a. File Permissions

During our FY 2000 audit, we found that file permissions were weak. Due to the sensitivity, specific conditions are not listed; however, they were provided to the appropriate offices at the completion of the audit.

The following are several risks that exist governing the inappropriate establishment of file permissions.

- Improperly setting the umask variable in the user's .profile, .login or .cshrc file increases the risk that unauthorized users will modify or delete files created by other users.
- Improper permissions on HOME directories or login scripts could potentially allow a user to obtain the level of access of another ID on the server. If the compromised ID is business-critical, then this vulnerability is high-risk and could be exploited to gain privileged access on the server.
- System configuration files and other files writeable by other users increase the risk that unauthorized users delete or modify these files.

The following criteria were used in reporting this finding:

- NISTIR 5153, *Minimum Security Requirements for Multi-user Operating Systems*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Management concurred with the finding and took immediate corrective action; therefore, this issue is considered **closed.**

b. Unix Path Variable

During our FY 2000 audit, we found that the user PATH variable on the production server was not adequately configured in a secure manner. Due to the sensitivity, specific conditions are not listed; however, they were provided to the appropriate offices at the completion of the audit.

Insecure PATH variables increase the risk that users will be "spoofed" by common system commands such as "ls," (list files) which is executed instead of the system ls. For example, an unauthorized user could write a program that performs certain functions and call the program ls. When an authorized user invokes the ls command the bogus ls program could be executed.

The following criteria were used in reporting this finding:

- NISTIR 5153, Minimum Security Requirements for Multi-user Operating Systems,
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Management concurred with the finding and took immediate corrective action; therefore, this issue is considered **closed**.

c. Generic Accounts

During our FY 2000 audit, we found that users are not required to supply an individual user ID and password before accessing a generic account, including the root account, on two production servers. In addition, auditing should be enabled on both servers. Anonymous accounts weaken accountability. If many users can use the same account without first logging in with an individual user ID and password, there is no way to distinguish which activities are performed by which users. Auditing is required to ensure that user accountability is maintained.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agency SSPs include specific technical standards (security settings, critical system configurations, etc.), for each general support system and major application.***

Management's Response:

ESA concurs with this finding. ESA is in the process of developing methods and procedures to implement controls and expects to put those methods/procedures in place during FY 2001.

OIG's Conclusion:

We concur with management's plans to correct these weaknesses. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

d. System Warning Banners

During our FY 2000 audit, we found that there was no system warning message in the /etc/motd file on two production servers.

It is important to inform users of the sensitive nature of the resources they are using. ESA's ability to prosecute criminals may be impacted by the lack of a warning message. It is also a good practice to proactively inform users that they are subject to audit.

The following criteria were used in reporting this finding:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*

Management concurred with the finding and took immediate corrective action; therefore, this issue is considered **closed**.

e. Password Aging

During our FY 2000 audit, we found that password aging parameters were weak on two production servers. Due to the sensitivity, specific conditions are not listed; however, they were provided to the appropriate offices at the completion of the audit.

Passwords unchanged over a long period of time give an intruder more time to try and crack passwords. In addition, password aging can also prevent users from rechanging their passwords before a minimum interval has elapsed. This will prevent users from quickly switching back to their old passwords.

The following criteria were used in reporting this finding:

- NISTIR 5153, Minimum Security Requirements for Multi-user Operating Systems
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Management concurred with the finding and took immediate corrective action; therefore, this issue is considered **closed**.

f. Password Length

During our FY 2000 audit, we found that the settings for the password length could be improved. Specifically, we noted that the minimum length for passwords on two production servers is six characters. Management stated that ESA's policies and procedures are in compliance with the CIO computer Security Handbook and believes the finding should be addressed by the CIO. Inadequate controls over the establishment of password parameters may lead to the risk of passwords being easily guessed allowing unauthorized users the ability to gain access to system resources.

The following criteria were used in reporting this finding:

- NISTIR 5153, *Minimum Security Requirements for Multi-user Operating Systems,* indicates that passwords shall meet a customer-specifiable minimum length requirement. The system-supplied default minimum length shall be eight characters.
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, established a minimum set of controls for agencies' automated information security programs, including assigning responsibility for security, security planning, periodic review of security controls, and management authorization of systems to process information. Agencies are required to establish controls to assure adequate security for all information processed, transmitted or stored in Federal automated information systems.

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agency SSPs include specific technical standards (security settings, critical system configurations, etc.), for each general support system and major application.***

Management's Response:

ESA concurs with this finding. While ESA agrees that a minimum length of six characters as a password could pose vulnerabilities, controls can be implemented to mitigate the vulnerabilities. It should be noted that ESA already has, in place, mitigating controls for password length. Closure of this finding will be dependent on OIG review of these controls.

OIG's Conclusion:

This recommendation is **resolved and open** pending our review of the compensating controls during the FY 2001 audit.

g. Unix Services

During our FY 2000 audit, we found that unnecessary services are running on two production servers. Due to the sensitivity, specific conditions are not listed; however, they were provided to the appropriate offices at the completion of the audit.

The r-services provide a large amount of risk to a system. They allow users to log in without authenticating. The rstat daemon gives an intruder information about the host, including when the machine was last booted, how much CPU it is using, how many disks it has, and how many packets have reached it, load average, network traffic, etc. Rusers provides information on users on the host. It provides information on how busy the machine is and on login accounts an intruder can use in an attack. Obtained account information can be used by a scanner or attacker in a brute-force attack. Telnet is one of the larger risks to a system because it allows user ID and password information to pass over the network in the clear. Any hacker on the network can sniff out this information and log in to the system as that user. Sessions can also be easily hijacked.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agency SSPs include specific technical standards (security settings, critical system configurations, etc.), for each general support system and major application.***

Management's Response:

ESA concurs with this finding. While ESA agrees the conditions noted by the OIG could pose vulnerabilities, controls can be implemented to mitigate the vulnerabilities. It should be noted that ESA already has, in place, mitigating controls for the conditions noted. Closure of this finding will be dependent on OIG review of these controls.

OIG's Conclusion:

This recommendation is **resolved and open** pending our review of the compensating controls during the FY 2001 audit.

h. Trust Relationships

During our FY 2000 audit, we found that overly broad trust relationships are used. Due to the sensitivity, specific conditions are not listed; however, they were provided to the appropriate offices at the completion of the audit.

Using trust relationships could potentially expose the server. If a trusted computer or user is compromised, this could allow a user to gain remote access to the server without entering a password.

The following criteria were used in reporting this finding:

- NISTIR 5153
- OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agency SSPs include specific technical standards (security settings, critical system configurations, etc.), for each general support system and major application.***

Management's Response:

ESA concurs that there is a need to strengthen controls over its trust relationships and is currently reviewing and documenting specific trust relationships. Closure of this finding is dependent on the OIG reviewing the documented trust relationships.

OIG's Conclusion:

This recommendation is **resolved and open** pending our review of the documentation of the trust relationships during the FY 2001 audit.

i. Entitywide Security Program Plan

During our FY 2000 audit, we found that the Division of Coal Mine Workers' Compensation (DCMWC), a division within ESA that administers ASP, is not subject to follow ESA's policies and procedures resulting in security policies and procedures that:

- do not contain all of components required by the DOL CIO's Computer Security Handbook (CSHB) or ESA's plans; and
- duplicate the efforts of ESA, such as in the development of:
  - security awareness training programs
  - incident response capabilities

In addition, the DCMWC security management structure is not included in ESA's security management structure. Program Offices are not effectively utilizing ESA's centralized security office that has dedicated resources to provide policies and procedures that are consistent with ESA's security objectives and the CIO's CSHB; therefore, program offices may be duplicating efforts arising to inefficient use of resources and/or developing policies and procedures that are inconsistent with ESA's objectives.

The following criterion was used in reporting this finding:

- ESA GSS SSP

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agency entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, and access monitoring.***

Management's Response:

ESA does not concur with the finding that efforts to develop security awareness training programs nor incident response capabilities result in duplication of effort. ESA's IT Security Training and Awareness Program, as well as the policies and procedures which result from this Program, are being developed at a centralized level within ESA. Program-specific security awareness and training, e.g., that training which is applicable to specific applications, will be developed at the Program level. The same is true for incident reporting.

The DCMWC ASP system is not currently under ESA IT management. Because this system is completely separated from ESA IT systems, DCMWC is responsible for its management and oversight. This system is operated under contract by CSC on a CSC owned and operated mainframe. However, as noted in our January 3, 2001, response to the "Statement of Facts," DCMWC is in the process of migrating to a client server system modeled after the ESA IT architecture. Once this new system is implemented DCMWC will work with ESA IT staff to fully integrate it into the ESA IT environment. In fact, this conversion to the ESA IT model is part of DCMWC's long-standing plan to eliminate duplicate efforts, reduce costs and achieve economies of scale by placing DCMWC IT systems under ESA IT management. Upon integration, the ESA security plans will be updated to incorporate ASP security plans, and redundant programs will be eliminated.

With respect to the comment regarding the ASP security plan, DCMWC has a comprehensive security plan and extensive documentation regarding this plan. This plan, which covers both the GSS and MA, meets all of DOL's substantive requirements, but because this plan pre-dates the DOL guidelines the documentation does not conform to the format prescribed by the Department. As indicated in numerous discussions with DOL and the OIG, as part of the client server implementation process, DCMWC will update this security plan to cover the new system and will conform the plan to DOL guidelines.

OIG's Conclusion:

While ESA disagrees with the OIG assessment of duplicated effort caused by DCMWC independence, ESA is currently working to incorporate DCMWC into the ESA IT model and environment. This recommendation is **resolved and open**. Resolution will depend on the OIG review of the ESA IT environment after DCMWC has been fully incorporated into it.

j. Accreditation and Security Reviews

During our FY 2000 audit, we found that: (1) an application controls review has not been performed on the ESA MAs, specifically, BCDS/CMP, LS, and ASP; however, an application controls review is in progress for FECS, and (2) an accreditation statement does not exist for BCDS/CMP, LS, and ASP.

In the absence of independent reviews or audits of application controls, the integrity, reliability, and availability of data within the systems identified may be overlooked.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure that agencies are in compliance with the computer security handbook by verifying that all financially significant applications and support systems have been properly accredited and that independent functional reviews are conducted at least every 3 years.***

Management's Response:

ESA concurs with the findings related to the application controls reviews not being performed on BCDS/CMP, LS and ASP.

ESA also concurs that accreditation statements do not exist for BCDS/CMP or ASP. However, accreditation statements for Longshore were provided on December 20, 2000 and are documented in the Program's system security plans.

In order to abate these problems ESA has been in the process, over the past year, of restructuring its information security processes, including identification of an agency-wide computer security officer, and program-specific security officers. ESA plans, during FY 2001, to develop a schedule for the periodic for application reviews, risk assessments and system security plan revisions.

As noted above DCMWC is in the final stages of replacing the ASP system with a new client server system. The Office of the Inspector General recently completed an extensive "Security Testing and Evaluation Audit" of this system. Additional reviews will be conducted as required. An accreditation statement will be issued in conjunction with implementation of the new system.

OIG's Conclusion:

We concur with management's plans to correct these weaknesses. This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

However, ESA noted the OIG has completed a "Security and Testing Evaluation Audit" as a step in the certification process. This audit has not been issued and issues identified from the audit need to be addressed before certification.

k. Policies and Procedures for Clearing/Sanitizing Media Containing Sensitive Data

During our FY 2000 audit, we found that policies and procedures for clearing/sanitizing sensitive data and software from discarded and transferred equipment and media have not been developed and implemented. Without adequate controls for ensuring data and software are properly disposed and/or transferred, the risk exists that sensitive information may be disclosed to unauthorized individuals or parties. ESA is in the process of assessing the need for developing policies and procedures related to labeling, transmitting, securing, and disposing of sensitive data and media.

The following criterion was used in reporting this finding:

- NIST Special Publication 800-12, *An Introduction to Computer Security*

Recommendation:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agency SSPs are in compliance with the computer security handbook and that agency SSPs (for its GSS and MAs) include appropriate controls for the protection of physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside.***

Management's Response:

ESA concurs with this finding. It should be noted that ESA has developed a draft policy and procedures which will ensure that ESA has methodologies in place for the sanitation of all media prior to its being surplussed or transferred.

OIG's Conclusion:

This recommendation is **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

l. Logical Controls over the Authorizing and Periodic Monitoring of User Access

During our FY 2000 audit, we found that controls over the authorizing and periodic monitoring of users having logical access to ESA's ASP mainframe application require improvement.

- Standard Access Request Forms granting logical access to the ASP mainframe application were not adequately documented. Specifically, the following weaknesses were identified:

    - 3 of the 18 forms tested did not contain information justifying the users access as required on the form, and
    - 4 of the 18 forms tested did not contain the data security officer's signature approving the access being granted.

- Monitoring of TSO accounts having access to the ASP Mainframe application was not adequately performed resulting in obsolete and/or inappropriate access to the system. Specifically, we noted the following weaknesses:

    - 28 accounts were marked as canceled and deemed obsolete, however remain on the system,
    - 6 users had multiple active accounts,
    - 1 active account was labeled "unassigned" and deemed inappropriate, and
    - 32 accounts deemed active have not been accessed for at least 90 days ranging to 6 years.

Without clearly defined policies, procedures and assignment for security administration, security administrators may not fully be aware of management's security objectives and may not be consistently performing the necessary procedures required to provide effective control. Thus, inadequate controls over the monitoring and removal of obsolete, inactive, or IDS not assigned to a specific individual, from the system increases the risk of unauthorized access to system resources.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- OMB Circular A-130 Appendix III, *Security of Federal Automated Information Resources*
- ESA GSS SSP

Recommendations:

The following prior year recommendation to the Chief Information Officer and Assistant Secretaries pertains to this finding:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs contain sufficient policies and procedures governing the authorizing, modification, removal, monitoring of access based on the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the***

system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.

Management's Response:

As noted to the OIG auditors and staff, DCMWC is in the process of replacing the ASP mainframe with a new client server system. This system will be implemented in the current calendar quarter. Upon implementation the specific examples cited will be moot. In conjunction with system implementation, DCMWC will ensure that logical controls are clearly documented and understand. As noted previously, DCMWC will update its security plan documentation to include such controls and to conform to OCIO and NIST guidelines.

OIG's Conclusion:

This recommendation is **resolved and open** pending our review of the implementation of the policy and procedures for the new ASP system, and for the non-existence of the weaknesses identified.

Status of Prior Year Findings and Recommendations

Risk Assessment

During our FY 1998 audit (OIG Report No. 12-99-002-13-001), we found that ESA does not have a completed/approved risk assessment that considers data sensitivity and integrity, the range of risks to the entity's systems and data, and resource classifications over its GSS and MAs. We made the following recommendation to the Chief Information Officer and Assistant Secretaries:

- ***ensure entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessment, security management structure, and access monitoring.***

During our FY 2000 audit, we found that risk assessments have been performed and documented for the ESA GSS and the MAs; however, they are in the process of being reviewed and approved by the CIO. It should also be noted that resource classifications and criteria have been established for the GSS and MAs except for ASP. This recommendation is considered **resolved and open**. Closure of this recommendation depends upon our review of ESA's reviewed and approved risk assessment.

Management's Response:

ESA concurs with this response. All comments on ESA risk assessments have been received from the OCIO and all but one revised assessment has been returned to the OCIO. The remaining risk assessment is currently being completed.

(Black Lung ASP) Resource classifications and criteria will be established for the new ASP in conjunction with implementation.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed risk assessments and ASP's resource classifications during the FY 2001 audit.

Entitywide Security Program Plan

During our FYs 1997 and 1998 audits (OIG Report Nos. 12-99-002-13-001 and 12-98-002-13-001), we found that ESA does not have a formally approved entitywide security plan for its GSS and MAs. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessment, security management structure, and access monitoring, and***
- ***ensure computer security plans are developed and implemented for all departmental systems.***

During our FY 2000 audit, we found that security plans have been established and documented for ESA's GSS, and the following MAs: LS, BCDS and CMP are awaiting approval from the CIO. An MA security plan for FECS is currently under development. The documents that make up the ASP mainframe security plan do not meet the requirements outlined by the CIO for an MA System Security Plan (SSP). In addition, though policies and procedures have been established in the security plan for certain security activities (i.e., ongoing security awareness training, incident response capability, security management structure), funding to fully implement these are not expected until FY 2001. These recommendations remain **resolved and open**. Closure depends upon our review of ESA's completed security plans for all MA's.

Management's Response:

While ESA concurs with this finding, it should be noted that a system security plan for FECS was completed and delivered to the CIO for review on September 27, 2000 (as noted to the OIG on December 20), and the OCIO has already returned comments on that plan. ESA will continue to finalize other security plans as comments are received from the OCIO.

(Black Lung ASP) As noted above, DCMWC has an extensive security plan that predates the CIO guidelines. This plan meets the substantive requirements of these guidelines but does not conform to the CIO format. DCMWC will update its security plan to accommodate the client server system and conform it to the CIO requirements.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Security Management Structure and Security Responsibilities

During our FY 1998 audit (OIG Report No. 12-99-002-13-001), we found that ESA does not have a formally established security management structure with clearly assigned security responsibilities over ESA and its various programs. We made the following recommendation to the Chief Information Officer and Assistant Secretaries:

- ***ensure entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessment, security management structure, and access monitoring.***

During our FY 2000 audit, we found that the ESA GSS SSP establishes a security management structure with adequate independence, authority, and expertise; and an information systems security manager has been appointed at an overall level and at appropriate subordinate levels. However, the following should be noted:

- The security responsibilities of the DITMS Division Director are not clearly established and documented in the ESA GSS SSP.
- The security responsibilities of the MA System Owners are not addressed and are due to be completed with the MA SSPs in FY 2001.
- The MA Program Computer Security Officers have not been established and are due to be determined and documented with the MA SSPs due to be completed in FY 2001.
- The ESA GSS SSP does not include ASP; thus, the DCMWC security management structure for ASP is not documented within the ESA GSS SSP.

In addition, for ASP:

- Security roles and responsibilities have not been established and documented for the Security Officer and the DOL Security Backups.
- The DCMWC organization chart does not identify the security function/management.

This recommendation remains **resolved and open**. Closure is dependent on the verification of an independent security administration for all of ESA's financially significant systems and our review of the ESA's system security plan (SSP).

Management's Response:

ESA concurs that its General Support System Security Plan (SSP) does not contain security responsibilities for the Director of DITMS nor the major application System Owners. When ESA developed this Plan, these responsibilities were drafted, but were deleted from the document. ESA will incorporate these responsibilities into the next version of this Plan, which will be prepared as a result of OCIO comments once their review is completed.

ESA does not concur with the finding that Program Computer Security officers were not designated for each Program. They were established as part of the development of each major application's security plan. Copies of the memoranda designating these individuals have previously been provided to the OIG.

It should be noted that the DCMWC security management structure for ASP should be noted in that application's system security plan, and in the system security plan for the DCMWC general support system; the DCMWC infrastructure is separate from the ESA Enterprise Infrastructure.

(Black Lung ASP) As indicated above, upon integration with the ESA IT environment, the ASP system will be integrated into the ESA GSS SSP. Roles and responsibilities for the new ASP have been established and will be documented in conjunction with system implementation. The organization chart will be updated to reflect the security function.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions taken and the review of any documentation submitted during the FY 2001 audit.

Security-Related Personnel Policies

During our FYs 1997 and 1999 audits (OIG Report Nos. 12-00-003-13-001 and 12-98-002-13-001), we found that ESA has not implemented effective security controls related to personnel policies and procedures. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure that all applicable employees and contractors receive the required training and maintain appropriate documentation (e.g., list of all employees as of the training course date, attendance sheet of employees taking the course, topics, agendas, handouts, etc., provided during the program),***

- ***ensure computer security plans include procedures for proper termination of system access of former employees, and those procedures be implemented, and***
- ***ensure a background check is conducted for all government and contractor management personnel with high levels of system access.***

During our FY 2000 audit, we found that ESA has developed/approved an entitywide security plan, ESA GSS SSP that addresses security-related personnel policies. In addition, ESA plans to review the appropriateness of existing procedures regarding position sensitivity related issues and background screening and to consider the DOL Personnel Security Program for implementation. Funding permitting, ESA plans to implement a comprehensive personnel security-screening program in FY 2001. These recommendations remain **resolved and open**. Closure is dependent on ensuring that ESA's SSP, which addresses security clearances, has been developed and issued, and the correction of any deficiencies that have previously been identified or would exist as a result of the issuance of the new security policy have seen made.

Management's Response:

ESA concurs with this finding. As stated, ESA has begun, in FY 2001, to develop a more comprehensive personnel-security program.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the ESA's personnel-security program during the FY 2001 audit.

Logical Controls to Prevent or Detect Unauthorized Access

During our FYs 1998 and 1999 audits (OIG Report Nos. 12-99-002-13-001 and 12-00-003-13-001), we found that controls over the authorizing and periodic monitoring of users having logical access to ESA's FECS mainframe application require improvement. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs contain sufficient policies and procedures governing the authorizing, modification, removal, monitoring of access based on the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access, and***
- ***ensure all departmental Computer Security Plans have policies and procedures for user access, physical access, and monitoring of sensitive and critical resource access***

During our FY 2000 audit, we found that FECS management is the process of improving the controls over authorizing and monitoring logical access to the mainframe by developing an MA SSP for FECS that will cover the entire security and operating environment that includes both the mainframe and client server platforms. These recommendations remain **resolved and open**. Closure depends upon our review of ESA's improved controls over the authorizing and periodic monitoring of users having logical access to ESA's FECS mainframe application.

Management's Response:

{blank per agency request}

Access Monitoring and Security Violations

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that ESA security monitoring controls over the mainframe environment needs improvement. We made the following recommendation to the Chief Information Officer and Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate policies and procedures for the monitoring of inappropriate or unusual activity occurring on the system. Policies and procedures should include, but are not limited to management's determination of what should be recorded on logs and what constitutes a violation of the policy, frequency of reviews, reporting and escalation processes, and maintenance of documentation (manual or automated) for audit trail purposes, etc.***

During our FY 2000 audit, we found that FECS management is currently improving the controls over authorizing and monitoring logical access to the mainframe by developing an MA SSP for FECS that will cover the entire security and operating environment that includes both the mainframe and client server platforms. This recommendation is **resolved and open**. Closure of this recommendation is dependent on our review of ESA's SSPs containing inappropriate or unusual activity response procedures for the financially significant applications and support systems.

Management's Response:

{blank per agency request}

Logical Controls to Prevent or Detect Unauthorized Access

During our FYs 1998 and 1999 audits (OIG Report No. 12-99-002-13-001 and 12-00-003-13-001), we found that controls over the authorizing and periodic security monitoring of users having logical access to ESA's UNIX environment require improvement. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs contain sufficient policies and procedures governing the authorizing, modification, removal, monitoring of access based on the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access, and***
- ***ensure all departmental Computer Security Plans have policies and procedures for user access, physical access, and monitoring of sensitive and critical resource access.***

During our FY 2000 audit, we found that DITMS management is in the process of improving the controls over authorizing and monitoring logical access to the UNIX environment. Testing performed as part of the FY 2000 audit noted the following:

- 2 of the 20 ESA Access Authorization Forms were not available for review,
- 3 of the 20 ESA Access Authorization Forms were missing the user privacy understanding section, and
- 14 program specific forms were not provided.

However, it should be noted:

- ESA's Office of Management, Administration and Planning Division of Automated Systems Management Procedures Manual, Request for Government Issued User Accounts and Services, requires the use of Authorization Documentation.
- ESA's Security Officer is in the process of completing a recertification of users on the FECS, LS, BCDS and CMP systems.

These recommendations remain **resolved and open**. Closure depends on our review of the ESA's improved controls over the authorizing and periodic security monitoring of users having logical access to ESA's UNIX environment.

Management's Response:

ESA concurs with this finding. ESA is currently in the process of performing its scheduled yearly audit to ensure validity of system users. It should be noted, however, that this audit is not being conducted by the ESA Security Officer alone. This audit is being conducted by the Chief of the Branch of Operations and Support, ESA Systems Managers, and the ESA Security Officer. In the case of the three forms where the privacy information was not completed, it should be noted that those forms were completed after ESA modified procedures removing this section from its form. The modification was made in response to concerns by local unions. ESA will investigate the requirements for privacy notification/understanding and, based on that review, will re-insert the privacy language if the investigation warrants it.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

Physical Controls to Prevent or Detect Unauthorized Access

During our FYs 1998 and 1999 audits (OIG Report Nos. 12-99-002-13-001 and 12-00-003-13-001), we found that physical controls to prevent or detect unauthorized or inappropriate access to the DITMS data center need improvement. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate controls for the protection of the physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside. In addition, we recommend agency SSPs include specific technical standards (security settings, critical system configurations, etc.) for each general support system and major application, and***
- ***ensure all departmental Computer Security Plans have policies and procedures for user access, physical access, and monitoring of sensitive and critical resource access.***

During our FY 2000 audit, we found that DITMS management is in the process of implementing the new ESA Computer Room access policies and procedures. ESA has implemented new physical access request forms that appear sufficient to document the critical information needed when granting access to the DITMS data center and policies for handling defective or unused cards. In addition, ESA implemented a card-key system in June of 2000 providing additional security features and monitoring tools over the DITMS data center. These recommendations are **resolved and open**. Closure is dependent on our review of the physical access controls to DITMS data center during the FY 2001 financial statement audit.

Management's Response:

ESA concurs with this finding. However, it should be noted that the ESA Computer Room Access Policy and Procedures was finalized in August 2000.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

2. DOL Needs to Fully Implement a Systems Development Life Cycle Methodology

Status of Prior Year Findings and Recommendations

Documentation

During our FY 1998 and FY 1999 audits (OIG Report Nos. 12-98-002-13-001 and 12-00-003-13-001), we found that:

- The System Development methodology and the Configuration Change Management procedures have not been formally documented and implemented for FECA.
- Documentation of FECS technical programming and user operations is inadequate.

We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure the "Department of Labor Computer System Development Life Cycle (SDLC) Manual" that addresses policies and procedures for documenting various aspects of the system (including user manuals) and under what conditions documentation should be updated. The manual should be reviewed and approved by all agency heads, issued, and followed, and***
- ***ensure that the SDLC process is followed by all DOL and contractor personnel who are developing, acquiring, or managing new systems or making enhancements to existing systems.***

During our FY 2000 audit, we found that revised mainframe application change control procedures were scheduled to be incorporated into the ESA General Support System in FY 2001. These recommendations are **resolved and open**. Closure is dependent upon our review of the SDLC policies and procedures.

Management's Response:

{Blank per agency request}

Library Management Software

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that the Library management software installed on the mainframe used to process the FECA application is not being used to manage or control the FECA source code. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure that its system development life cycle methodology, that is to be followed by the agencies, includes policies and procedures for emergency changes, the separation of***

duties of development and support staff from the production environment, and the usage of automated library management tools, and

- ***ensure agency compliance with the SDLC manual and institute emergency change control procedures, thus allowing access to the system when unexpected events arise.***

During our FY 2000 audit, we found that the version control software CA-Librarian has been installed and procedures for moving source code under control of this software are being developed. In the interim, manual procedures for implementing version control and for a change control process have been developed and recently implemented. These recommendations are **resolved and open**. Closure is dependent on our review of ESA's revised SDLC guidance on emergency changes, the separation of duties, and the usage of automated library management tools.

Management's Response:

{Blank per agency request}

Controlling Libraries

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that FECA program development staff has access to production and test environments; mainframe programmers may move changes to the production environment. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure that the SDLC manual provide for the establishment of control points for formally requesting, approving, and testing system software changes, and that these controls are implemented and followed, and***
- ***ensure that its computer security handbook include, in the separation of duties and least privilege sections of the SSP Guide, that agency heads identify and document incompatible duties for general support systems and major applications.***

During our FY 2000 audit, we found that FECS management is currently working with SunGard to ensure that developers cannot access production libraries by reviewing all access control lists for production data sets. These recommendations are **unresolved**. Resolution is dependent upon the OIG review of the ESA's computer security handbook with guidance on granting and monitoring of access and documentation that reviews have been scheduled of ESA's financially significant systems for implemented policies on governing access.

Management's Response:

{Blank per agency request}

3. DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

Status of Prior Year Findings and Recommendations

Disaster Recovery Plan

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that a complete inventory of items such as computer hardware, software, and telecommunications needed for operations is not included in the ESA disaster recovery/business continuity plan. We made the following recommendations to the Chief Information Officer and Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility; plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training for primary and backup personnel, and frequency of updates, etc., and***
- ***ensure that written disaster recovery plans are developed where needed.***

During our FY 2000 audit, we found that ESA will continue to work with the Department as it refines its approach to contingency and disaster planning. Once final guidance is issued, ESA will begin an agency-wide effort to reassess its contingency and disaster planning efforts and will take actions, if necessary, to correct any problems or deficiencies noted. These recommendations are **resolved and open**. Closure is dependent on our review of ESA's completed contingency plans, which include a complete inventory of items such as computer hardware, software, and telecommunications needed for operations, for ESA's financially significant systems and their support systems.

Management's Response:

ESA concurs with this finding. ESA has already begun a reassessment of its contingency and disaster planning efforts in lieu of Departmental guidance. The completed contingency and disaster planning documents will contain all information noted, such as a complete inventory of hardware and software.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the corrective actions taken during the FY 2001 audit.

MINE SAFETY AND HEALTH ADMINISTRATION (MSHA)

We tested general controls and security over EDP systems of the MSHA as they pertain to the following critical financial application:

- Assessments Database Management System (ADBMS)

GAO's Federal Information System Controls Audit Manual (FISCAM) was used to guide testing. The scope of testing included the six FISCAM general controls sections: (1) Entitywide Security Program Planning and Management (SP), (2) Access Controls (AC), (3), Application Software Development and Change Control (CC), (4) System Software (SS), (5) Segregation of Duties (SD), and (6) Service Continuity (SC).

The ADBMS application resides on the Honeywell Bull mainframe DPS-9000 computer system located at the Defense Enterprise Computing Center (DECC) in San Antonio, Texas. In addition, the Directorate of Program Evaluation and Information Resources (PEIR), Information Resource Center, Division of Systems Operations and Communications, located in Lakewood, Colorado, contains telecommunications equipment used by MSHA to connect to the DECC Bull Mainframe, DPS-9000. ADBMS consists of an online telecommunications network linking the Wilkes-Barre Assessment Center, the Arlington Assessment Office and the Civil Penalty Compliance Office (CPCO) to the Honeywell Bull mainframe DPS-9000 computer system.

The PEIR group is responsible for application development and maintenance. Our scope was limited to the EDP controls that are the responsibility of MSHA and the MSHA controls as they relate to the Bull mainframe processing of ADBMS. Limited testing was performed at the DECC that supports and maintains the mainframe operating system and physical environment used to process and store ADBMS application data.

1. DOL Needs to Strengthen Controls to Protect Its Information

Current Year Findings and Recommendations

a. Risk Assessment

During our FY 2000 audit, we found that the MSHA Risk Analysis Report is dated February 17, 1989. The analysis is outdated and MSHA Management is currently in the process of performing a risk assessment. In the absence of an up-to-date risk assessment, identification of current threats and vulnerabilities, appropriate decisions for mitigation and subsequent adjustments to the security controls and policies may not be performed on a timely basis for critical system resources. Therefore, effective security controls may not be implemented to prevent or detect unauthorized or inappropriate access to MSHA's systems and information.

The following criteria were used in reporting this finding:

- The DOL Computer Security Handbook (CSHB)
- The Federal Managers' Financial Integrity Act of 1982
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, access monitoring, etc.***

Management's Response:

MSHA completed a risk assessment of the Agency's major applications, including the Assessments Database Management System (ADBMS), in November 2000. This Risk Assessment was conducted using Risk Watch, the model adopted by the Department. The draft *Vulnerability Report* was submitted to the Office of the Chief Information Officer on December 12, 2000. The identification of MSHA's current risks and threats in the *Vulnerability Report* will be used to establish more effective information security policies during the implementation of MSHA's integrated security program beginning in January 2001.

OIG's Conclusion:

This recommendation is **resolved and open** pending our review of the MSHA policy and procedures for performing risk assessments and our review of the completed risk assessment for ADBMS during the FY 2001 audit.

b. Entitywide Security Program Plan

During our FY 2000 audit, we found that the Department of Labor's Mine Safety and Health Administration's (MSHA) GSS Security Plan has not been fully completed to be in compliance with the CIO's Computer Security Handbook. In addition, the MA for ADBMS is under development and due to be finalized in FY 2001. Without a formal documented security plan, employees may perform inadequate or improper procedures that could, in turn, compromise the security control structure of the organization or sensitive data residing within MSHA's systems. In addition, policies, procedures, and guidelines presented within the security plan should be

updated periodically or they may not adequately reflect recent modifications within the current working environment of an organization or may not fully support management's overall business and security objectives.

The following criteria were used in reporting this finding:

- The DOL Computer Security Handbook (CSHB)
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- OMB Bulletin 90-08

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, access monitoring, etc.***

Management's Response:

MSHA completed a General Support System Security Plan and a Major Application System Security Plan, which includes an ADBMS System Security Plan, on November 15, 2000. The plans were submitted to the Office of the Chief Information Officer. These plans are in compliance with the CIO's Computer Security Handbook.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the MSHA General Support System Security Plan and ADBMS System Security Plan during the FY 2001 audit.

c. Security Management Structure and Security Responsibilities

During our FY 2000 audit, we found the Department of Labor's Mine Safety and Health Administration (MSHA) does not have an Information Security organization identified in its security plans and the information security structure has not been defined in the organization chart dated June 1, 2000.

In addition, there is no central system security office that could:

- facilitate risk assessments,
- coordinate the development and distribution of security policies and procedures,
- routinely monitor compliance with these policies,
- provide security awareness training among system users, and
- provide reports to senior management concerning policy and control evaluation results.

Without a well designed entitywide security program plan, security controls may be inadequate; responsibilities may be unclear, misunderstood; and controls may be inconsistently applied. The effectiveness of a security program is affected by the way in which responsibilities for overseeing its implementation are assigned. Generally, such responsibility is assigned to a central system security program office that reports directly to the Chief Information Officer.

The following criteria were used in reporting this finding:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST 800-12: *An Introduction to Computer Security*
- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, and access monitoring, etc.***

Management's Response:

MSHA has assigned entity-wide security officer duties to a position that reports directly to the Deputy Director, Program Evaluation and Information Resources. In consultation with contract security specialists, the Agency completed a security program implementation work plan on December 11, 2000. Work on security program implementation commences on January 2, 2000. One of the first steps in the work plan is the development of a formal security management structure within MSHA. This structure will identify reporting relationships and authorities at the functional, program, and individual levels.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the MSHA security structure and security plan during the FY 2001 audit.

d. Security Procedures

During our FY 2000 audit, we found that procedures for adding, modifying and removing user access privileges from the MSHA Assessment Data Base Management System (ADBMS) are not clearly defined and documented in the MSHA draft security Plan, dated April 14, 2000. Employees are deleted from production by Database/LAN Administrator without proper management authorization.

If ownership responsibilities are not clearly assigned, access/removal authorizations may be left to personnel who are not in the best position to determine users' access needs. Such personnel are likely to authorize overly broad access in an attempt to ensure that all users can access the resources they need. This defeats the purpose of access controls and, depending on the sensitivity of the resources involved, can unnecessarily provide opportunities for fraud, sabotage, and inappropriate disclosures. The effectiveness of a security program is affected by the way in which responsibilities for overseeing its implementation are assigned.

The following criteria were used in reporting this finding:

- NIST 800-12: *An Introduction to Computer Security*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient policies and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A re-certification should be conducted of all IDS on the system and the business need documented.***

In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.

Management's Response:

User access privileges are being established through use of a Unified Access Authorization (UAA) form scheduled to be finalized and fully implemented by the end of January. User access levels and system-related information will be incorporated for MSHA's server-based platforms including the MSHA Standardized Information System (MSIS), Teradata, Exchange and Citrix. Information from the existing Defense Enterprise Computing Center (DECC) System Access Authorization Request (SAAR) forms, along with information from the UAA form, will be utilized to populate and update an Intranet application designed to provide this data to system managers and security personnel. A valid user list that contains only authorized employees will be available and periodically reviewed by program managers and supervisors. The procedure will identify those with access rights to the ADBMS as well as all other user groups throughout MSHA.

The overall responsibility for the UAA form and procedures will be lodged with the Arlington IT security office being established in PEIR headquarters as described in c. Security Management Structure and Security Responsibilities. In addition, oversight and compliance guidelines for the process of authorizing system users will be included in a new IT Security chapter being drafted for inclusion in the Agency's Accountability Program. This is scheduled to be completed in FY 2001.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA procedures and policies for security during the FY 2001 audit.

e. Security-Related Personnel Policies

During our FY 2000 audit, we found that effective security related personnel policies were not implemented for MSHA. The following examples illustrate:

- Initial security training for new hires is not being conducted.
- There is no documentation (sign-in sheet, date of last security awareness training, etc.) from the last MSHA periodic security awareness training program.
- Employee background checks were not performed in a timely manner on employees hired in sensitive positions. In addition, periodic reinvestigation were not performed for these employees.
- Contractors given access to "high risk public trust" data such as MSHA programming production data are not required to have background investigations.
- Employees and contractors with access to "high risk public trust" information were not required to complete confidentiality agreements. Confidentiality agreements were not required for the users of ADBMS critical system. ADBMS contains "Privacy Act" information.
- Employee training was not tracked and monitored to help ensure that employee expertise

was maintained at the appropriate level.

- Procedures were not established to guide MSHA members completing exit tasks for departing employees. For example, there were no procedures stating when or how to notify the Network Administrator to remove a user ID for a departed MSHA employee.
- Checklists for departing employees from MSHA, includes Form DL 1-107 (Separation Clearance), were not always completed. In addition, the forms did not cover the removal of user IDS from all sensitive applications.
- Position descriptions/job descriptions are out dated or missing from employee files.

In the absence of adequate security-related personnel policies in place, an entity may risk the following: hiring unqualified individuals, leaving terminated personnel access to create unauthorized transactions, perform intentional errors, create a denial of service, and potentially disclose sensitive data, allowing staff expertise to decline and inappropriate segregation of duties. Overall, the lack of security-related personnel policies could lead to adverse personnel activities that could compromise the security over ADBMS.

The following criterion was used in reporting this finding:

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

Recommendation:

The following prior year recommendations to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that computer security plans include procedures for proper termination of systems access of former employees, and those procedures are implemented,***
- ***ensure that all applicable employees and contractors receive the required training and maintain the appropriate documentation (e.g., lists of employees as of the training course date, attendance sheet of employees taking the course, topics, agendas, handouts, etc., provided during the program), and***
- ***a background check should be conducted for all Government employees and contractor management personnel with high levels of system access.***

Management's Response:

Various personnel and contractor management practices have been implemented to address the conditions identified in this item.

With regard to security training, significant improvements have been made in the implementation and enforcement of MSHA's policies. Program managers have been instructed to ensure that new employees receive security training prior to receiving network or system access. Annual refresher

training is required for all other MSHA employees. This training is being given and documented at all locations, with lists of persons taking the training provided to the MSHA Security Officer in Arlington.

The Office of Assessments has created a tracking system for all ADBMS employee training, both informal hands-on training and formal training. The Office of Assessments is developing a policy to ensure compliance with documenting and tracking ADBMS training.

The security requirements for contractors working on MSHA systems have been reviewed and appropriate personnel security requirements have been included in each statement of work. In addition, confidentiality agreements are being developed for signature by MSHA employees as well as contractor staff. This will require employee union notification prior to implementation.

Since the ADBMS is considered a "high risk public trust" system, the Human Resource Division (HRD) in Arlington will determine which employees are required to have background investigations in order to use and access ADBMS data. HRD will determine which positions require periodic re-investigations as well as the frequency of the re-investigations.

MSHA's Human Resources Division is developing a policy and procedures for exiting MSHA employees. This policy will mandate the use of the Separation Clearance form (DOL Form 1-107 - Rev. April 1997). This revision includes a section (1-t) to list system names from which to remove the employee. The previous revision dated 1987 did not have the 1-t section. MSHA exiting procedures will include instructions for each employee's supervisor to provide a copy of the completed DOL1-107 to the appropriate LAN Administrator.

(Note: The auditors may not have a copy of the most recent revision to DOL1-107. See copy of the DOL1-107 (Rev. April 1997) Separation Clearance form.)

The Office of Assessments is in the process of reviewing and, where appropriate, revising the position descriptions for their staff.

OIG's Conclusion:

These recommendations are **resolved and open**. Closure is dependent upon our review of the new MSHA procedures and policies for personnel security and the corrective action identified during the FY 2001 audit.

f. Authorization of Access

During our FY 2000 audit, we found that procedures for authorizing access to systems resources within MSHA were weak. Specifically:

- Access to the ADBMS Application is not always authorized and documented. Though

policies and procedures exist, we found that they were not part of the MSHA security plan. In a test of 25 employees with access to the ADBMS application, we found only 12 had System Authorization Access Request (SAAR) forms on file.

- The design and use of the SAAR form can be enhanced. Specifically, the form does not indicate the authorized access privileges of the user.

Without clearly defined policies, procedures and assignment for security administration, security administrators may not fully be aware of management's security objectives and may not be consistently performing the necessary procedures required to provide effective control. Specifically,

- Undocumented or out-of-date access request forms may compromise the integrity of the system by granting access that is not consistent with management's security objectives, authorized intent, or user job responsibilities.
- Inadequate controls over the monitoring and removal of obsolete or inactive IDS from the system increases the risk of unauthorized access to system resources.
- Ineffective controls surrounding the granting and periodic monitoring of user access privileges increases the risk of unauthorized modification (intentional or accidental) to information stored and/or processed by the entity.

User accountability within the system is diminished without adequate controls over the maintenance of access request forms.

The following criteria were used in reporting this finding:

- System Authorization Access Request (SAAR) Memorandum from the Director of Program Evaluation and Information Resources
- NIST 800-12: *An Introduction to Computer Security*
- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient policies and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.***

Management's Response:

A review of the ADBMS user group was conducted. SAAR forms were prepared and authorized for all system users to ensure that only valid, authorized users have access to the system. Users without the requisite authorizations no longer have access to the system.

Additional information related to the Unified Access Authorization form and SAAR form is outlined under e. Security-Related Personnel Policies.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA procedures and policies for security-related personnel policies and additional testing of the implementation of the authorization forms during the FY 2001 audit.

g. Access Monitoring

During our FY 2000 audit of MSHA, we found that owners do not periodically review access authorization listings to determine whether access remains appropriate for the GSS and MA. In addition, changes to security profiles on both the Bull and NT systems are not periodically reviewed by management. As a result, some users access to the system is inappropriate. Specifically:

- We found 4 of 16 users tested, had access that did not appear appropriate based upon their job functions (e.g., mail clerks, file clerks, etc.).
- We found 3 of 6 application programmers had production level access.
- We found 1 of the 16 selected users in Wilkes-Barre Assessment Center had been assigned two Logical ID's.

Access that is not based upon a business need, using the concept of "least privilege," increases the risk of users performing functions that are inappropriate based upon their job responsibilities.

The following criteria were used in reporting this finding:

- System Authorization Access Request (SAAR) Memorandum from the Director of Program Evaluation and Information Resources
- NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient policies and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.***

Management's Response:

The Assessments program office recently issued new, secure IDS and passwords for all the ADBMS users.

MSHA is in the process of developing and implementing a Unified Access Authorization form and process, as previously discussed under d. Security Procedures. Once this system is in place, it will be possible to produce reports listing active, authorized users for each system and the levels of access authorized for those users. These reports will be provided on a periodic basis to the system managers for their review and certification. This process will be a component of an overall IT security program and will be managed through the Arlington IT security office.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the corrective actions taken and the new MSHA procedures and policies for security during the FY 2001 audit.

h. Remote Access

During our FY 2000 audit, we found that dial-in access of remote users to the MSHA's LAN located in Denver is not documented or monitored. Specifically, we found all 25 users tested were part of the "remote" group. This access allows users to dial-in remotely via Point-to-Point Protocol (PPP). In addition, controls were not in place to monitor remote dial-in**.** Inadequate monitoring of dial-in accounts increases the risk that unauthorized individuals or malicious intruders may not be detected and could gain access to systems resources.

The following criteria were used in reporting this finding:

- System Authorization Access Request (SAAR) Memorandum from the Director of Program Evaluation and Information Resources
- NIST 800-12: *An Introduction to Computer Security*

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient policies and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.***

Management's Response:

Dial-in authorization and monitoring procedures are being reviewed. It is not MSHA's policy to install dial-in software on any machine, desktop or laptop, without proper authorization. Authorization will be granted and periodically reviewed through the Unified Access Authorization form and procedures as discussed in response to d. Security Procedures and e. Security-Related Personnel Policies .

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA procedures and policies for security during the FY 2001 audit.

i. Physical Access

During our FY 2000 audit, we found access to the IRC is not adequately controlled. Specifically, we found that the doors leading to the LAN Servers that connect to the ADBMS application residing in San Antonio, as well as the printing area are not locked. Without effective physical controls over sensitive areas, the risk exists that unauthorized individuals may do physical harm or install devices that may impact the integrity, availability, or confidentiality of information stored and/or processed by the entity.

The following criteria were used in reporting this finding:

- NIST 800-12: *An Introduction to Computer Security*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with the computer security handbook and that agency SSPs (for its GSS and MAs) include appropriate controls for the protection of physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside.***

Management's Response:

The issue of insufficient physical controls on the IRC computer room has been addressed. A memorandum from the center chief to the chief of the IRC Systems Operation and Communication Division was issued on November 9, 2000, with instructions to ensure that the computer room is secured at all times, and to document and report any breaches of the security controls.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA procedures and policies for physical access and our review of the physical controls surrounding MSHA's environment during the FY 2001 audit.

j. Logical Controls to Prevent or Detect Unauthorized Access

During our FY 2000 audit, we found that logical access to the LAN and Bull operating system are inadequate. Specifically we found that:

- LAN system security settings do not require passwords to be:
  - controlled by the assigned user and not subject to disclosure (users are sharing passwords in order to check other users' mail);
  - changed periodically;
  - at least six alphanumeric characters in length; and
  - prohibited from reuse (e.g., maintaining a password history).
- Bull system security settings do not require passwords to be:
  - unique for specific individuals – Group user IDs'IDSd passwords are established (e.g., shared);
  - controlled by the assigned user and not subject to disclosure - through the use of group user ID's and passwords;
  - changed periodically;

    - at least six alphanumeric characters in length; and
    - prohibited from reuse (e.g., maintaining a password history).
- Security parameters over the LAN and the Bull do not prohibit the use of generic user IDS and passwords.
- Logical IDS used to gain access to Transaction Processing (TP) can be improved. Specifically:
    - TP does not require a password; and
    - Logical IDs are arranged in sequence (i.e., AR01, AR02, AR03, etc.).
- Computer terminals are not automatically logged off after a period of inactivity on the LAN.
- The use of screen saver passwords are not required.

Inadequate controls over the establishment of password parameters may lead to the risk of passwords being easily guessed allowing an unauthorized user the ability to gain access to systems resources. Lack of controls to automatically logged off sessions after a period of inactivity increases the risk that unauthorized users could gain access to the LAN via users who are legitimately logged into the LAN.

The following criteria were used in reporting this finding:

- NIST 800-12: *An Introduction to Computer Security*
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the Agency SSPs include specific technical standards (security settings, critical system configuration, etc.) for each general support system and major application.***

Management's Response:

Effective December18, 2000, MSHA LAN security settings were modified to enforce the following:

- Passwords must be 8 to 14 characters long;
- Passwords must contain at least one item from 3 of the following:
    - Uppercase Letters
    - Lowercase letters
    - Numbers

    - Special characters
- Passwords expire every 90 days;
- Passwords must be unique 5 times before the same password can be used again;
- Passwords cannot be changed for at least 30 days after the last change; and,
- User accounts are locked out for 60 minutes after 5 unsuccessful logon attempts (wrong password).

Honeywell mainframe based systems are scheduled for migration to a new platform through the MSHA Standardized Information System. The new system will adhere to the following standards:

- Individual user identifications;
- Passwords will be changed every 90 days;
- Passwords will be at least 8 characters in length in a combination of upper and lower case characters and numbers;
- Prohibited password reuse for 6 generations; and
- User access limited to the minimum level needed in performance of duties.

In order to improve security access requirements at DECC related to the transaction processing (TP) system, testing and implementation has been completed requiring the entry of an individual password accompanying the LID, adding an increased level of security to the on-line system. This effectively disrupts the sequential pattern of the lids. Further changes to existing applications for unique LIDS are not feasible at this time.

Whereas the use of generic user IDS and passwords is permitted on the Bull system, it is not permitted on MSHA's LAN. It is not the policy on the LAN to automatically log off a user after a period of inactivity, nor does MSHA plan to institute such a policy. However, on machines using the desktop core load, a screen saver is initiated after 15 minutes of inactivity on the LAN. Users must re-enter their passwords to resume the network session. Nonetheless, LAN users have been instructed to log off and shut down their computers when they leave for the day. On the Bull system, users are logged off of the system after a relatively short period of inactivity.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA procedures and policies for logical access and our testing of the new security settings during the FY 2001 audit.

k. Encryption

During our FY 2000 audit, we found that encryption tools have not been implemented to adequately protect the transmission of information between the MSHA LAN and the Bull mainframe. Lack of strict controls governing logical controls over telecommunications access

increases the risk of unauthorized persons jeopardizing the confidentiality, integrity, and availability of information. By not encrypting information as it travels over the network, MSHA faces the risk that information (including information required to be protected under the privacy act) could be obtained and/or reviewed by unauthorized users through the use of sniffers or other technologies.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

Recommendation:

The following prior year recommendations to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency are in compliance with the computer security handbook and that agency SSPs (for its GSS and MAs) include appropriate controls for the protection of physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside, and***
- ***ensure that the SSPs include specific technical standards (security settings, critical system configuration, etc.) for each general support system and major application.***

Management's Response:

MSHA is in the process of investigating the software and hardware upgrades necessary to implement router-to-router encryption throughout MSHA. This would provide for data transfer security but would not provide origin to destination encryption necessary to ensure complete data transfer security. As part of the initiative to upgrade network infrastructure security, including the requirement to fully encrypt Privacy Act data, various technologies, including Virtual Private Network (VPN), are being evaluated for implementation in MSHA within the context of the new MSIS environment.

OIG's Conclusion:

These recommendations are **resolved and open**. Closure is dependent upon our review of the security measures being implemented in the new MSIS environment during the FY 2001 audit.

l. Monitoring Policies

During our FY 2000 audit, we found that management does not have a process in place to

adequately address security monitoring for both the Bull and LAN systems. Specifically:

- Policies do not define what constitutes violation and escalation procedures.
- Security managers do not investigate security violations.
- Violations are not requested from the DECC, summarized and reported to senior management.
- Management does not review activities involving access to and modifications of sensitive or critical files on the Bull.
- Access control policies and techniques are not modified when violations and related risk assessments indicate that such changes are appropriate.

Without adequate monitoring controls, unauthorized attempts at gaining access to system resources may remain undetected and may eventually lead to an unauthorized user gaining access to the system. Without auditing access sensitive resources, management may not be aware of unauthorized attempts or modifications. This may expose the entity to the risk of an individual gaining unauthorized access to sensitive files that significantly impact the integrity and availability of the system.

The following criteria were used in reporting this finding:

- System Authorization Access Request (SAAR) Memorandum from the Director of Program Evaluation and Information Resources
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with the computer security handbook and that agency SSPs (for its GSS and MAs) include appropriate policies and procedures for the monitoring of inappropriate or unusual activity occurring on the system. Policies and procedures should include, but are not limited to management's determination of what constitutes a violation of the policy, the frequency of reviews, reporting and escalation processes, and maintenance of documentation (manual or automated) for audit trail purposes, etc.***

Management's Response:

With the availability of the TP log file and associated reports previously described in j. Logical Controls to Prevent or Detect Unauthorized Access, management once again has the ability to review update types, frequency, transaction initiator and transaction success/failure for

the most sensitive and critical of MSHA's files. However, there are additional violation reports that are currently not available to MSHA from the Bull system. DECC has been notified of this security deficiency and is exploring the possibility of providing these reports for MSHA's critical and supporting files.

MSHA is planning the evaluation and selection of network monitor/security software. It is MSHA's intention to implement a product that is capable of identifying and logging unauthorized access from either a LAN connection or dial-in source.

As part of the MSHA security program implementation plan, MSHA will develop policy and procedures for incident handling and response. A section of the policy will include the creation of a Computer Security Incident Response Team (CSIRT) within MSHA. The MSHA CSIRT will be part of an overall Department of Labor CSIRT directed by the OCIO. The policies and procedures will be in place by September 2001.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the implementation of the MSHA security program during the FY 2001 audit.

m. Accreditation Policies

During our FY 2000 audit, we found that ADBMS, a critical application, and the GSS used to support the application, does not have written authorization or accreditation statements from the program or function managers whose missions are supported by MSHA. Systems or applications that have not proceeded through proper accreditation run the risk of not having completed mandatory security tests, evaluations, or risk analyses. This may lead to the oversight of critical processing or security controls that could, in turn, compromise important production data files or programs within the system.

The following criteria were used in reporting this finding:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- The Federal Managers' Financial Integrity Act of 1982
- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with the security handbook by verifying that all financially significant applications support systems have been properly accredited and that independent functional reviews are conducted at least every 3 years.***

Management's Response:

MSHA submitted security plans to the OCIO in December 2000 for the General Support System and 6 Major Applications including the Assessments ADBMS. MSHA completed a risk assessment of the Agency's major applications, including the Assessments Database Management System (ADBMS), in November 2000. This Risk Assessment was conducted using Risk Watch, the model adopted by the Department. The draft *Vulnerability Report* was submitted to the Office of the Chief Information Officer on December 12, 2000. The identification of MSHA's current risks and threats in the *Vulnerability Report* will be used to produce an Authorization to Process document for the ABDMS. However, as the Major Applications are moved to the Common Platform as part of the MSHA Standardized Information System (MSIS) project, a certification and accreditation process for the GSS and the MSIS is scheduled to begin in October of 2001.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon the certification and accreditation of MSHA's MAs and our review of the MSIS process for certification and accreditation during the FY 2002 audit.

2. DOL Needs to Fully Implement a Systems Development Life Cycle Methodology

Current Year Findings and Recommendations

a. Application Change Procedures

During our FY 2000 audit, we found that application changes to the database are logged; however, the information is generated in an unreadable format and, therefore, is not reviewed. The Database Manager does not have an effective utility to translate the before and after images in a readable format. Updates to transactions cannot be traced to the original change.

The following criterion was used in reporting this finding:

- NIST 800-12: *An Introduction to Computer Security*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant

Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with DOL's SDLC Manual and the process is followed by all DOL and contractor personnel who are developing, acquiring, or managing systems or making enhancements to existing systems.***

Management's Response:

The transaction processing log file and related programs that run on the Bull system were temporarily unusable following the migration from DMIV TP to TP8. The log files have been modified and are now fully functional. The reports generated from the programs log transaction activities as they occur thereby providing a method for tracking database changes. The DBA reviews the reports in order to identify any unusual activity. The DBA notifies the SDM division chief of any unusual activity.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the logs and the procedures for reviewing the activity logs during the FY 2001 audit.

b. Change Control Policies And Procedures

During our FY 2000 audit, we found several weaknesses in MSHA's change control process. Specifically:

- Change request forms are not appropriately documented or authorized. Of the 17 change request forms tested, only 12 could be obtained. In addition, 1 of the 12 did not appear to be appropriately authorized.
- Software changes are logged by fiscal year but information associated with the various stages of a change history (i.e., request, development, test, user acceptance, final approval, migration, etc.) is not being tracked or captured in an effective manner.
- Test plan standards are not documented that include a comprehensive set of test transactions and data used in testing new changes.
- System and/or user documentation is not always updated for software, hardware, operating personnel, and system users when a new or modified system is implemented.
- Library management software is not used to:

    - produce audit trails of program changes;
    - maintain program version numbers;
    - record and report program changes;
    - maintain creation/date information for production modules; and
    - maintain copies of previous versions, and control concurrent updates.

Without strong controls over the application change management process, changes to the system may:

- not meet user requirements
- not be adequately tested
- not be appropriately authorized
- be associated with higher costs
- not adequately address security concerns

Controls over the modification of application software programs and the movement of programs and data among libraries decreases the risk of unauthorized program and data changes. Without the appropriate controls, improper changes could be incorporated in the program, causing processing irregularities, hampering further system development at a future time or causing security features to become inoperable.

The following criterion was used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with DOL's SDLC Manual and the process is followed by all DOL and contractor personnel who are developing, acquiring, or managing systems or making enhancements to existing systems.***

Management's Response:

MSHA developed and implemented *System Change Management Guidelines* in June. These guidelines covered change request review, development standards, testing standards, version control, release control, user acceptance, documentation update, user training, and implementation management.

At this time we do not plan to implement library management software to control the existing legacy systems. However, a *Configuration Management Plan* is being developed that will expand upon the change management procedures and will apply to all applications and systems within the Agency's Information Resource Center. For the legacy applications, a work order system has been developed that contains, among other things, a description of the requested change, the name of the approving official, and the SDM branch and programmer responsible for the change. The status of each change request is tracked from the start of the work through testing, user

approval, and final implementation. Reports from this system provide audit trails of each requested change on each application. Version control numbering, where appropriate, is instituted and a version description document (VDD) will be prepared for each version release.

Change control of system and user documentation will be managed through use of the Rational Clear Case tool. The Rational software tools were selected for use on the MSHA Standardized Information System (MSIS) and will document source code changes and version control, as well as track previous versions and concurrent updates.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSIS policies and procedures for change control during the FY 2001 audit.

3. DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

Current Year Findings and Recommendations

a. Service Continuity

During our FY 2000 audit, we found that MSHA does not have current contracts and agreements established for alternate data processing and telecommunications facilities (hotsite, coldsite or mobile vendors, agreements with other agencies to utilize their excess capacity). Lack of alternate processing agreements increase the likelihood of management not being able to recover or timely recover its operations in the event of an extended service interruption**.**

The following criteria were used in reporting this finding:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
- FIPS Pub. No. 87, *Guidelines for ADP Contingency Planning*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility;***

plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training primary and back-up personnel, and frequency of updates, periodic tests, etc.

Management's Response:

MSHA completed a risk analysis of the General Support System (LAN/WAN) and the Major MSHA Applications in November. The Vulnerability Reports have been submitted to the DOL OCIO for review.

As part of the MSHA Security Program Plan, MSHA will develop a contingency plan for the MSHA LAN/WAN and all major applications beginning the second quarter of FY 2001. MSHA developed a Security Program Work Plan that includes the purpose, objectives and deliverables for a Contingency Plan. One of the deliverables is a plan to test the contingency plan.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA Security Program Plan and the implementation of the Contingency Plan during the FY 2001 audit.

b. Business Continuity Plan

During our FY 2000 audit, two weaknesses were identified in MSHA's ability to provide uninterrupted service in support of its mission. Specifically:

- The Defense Enterprise Computing Center (DECC) has a contingency plan, however, the plan has never been tested.
- The Mine Safety and Health Administration "Business Continuity and Contingency Plan (BCCP)," dated September 1999 is too narrow in scope (addresses Y2K scenarios) and does not sufficiently address all critical requirements for a disaster recovery plan.

Without a tested contingency plan, management may not be aware of the plans' effectiveness or weaknesses that may negatively impact an entity's ability to recover in the event of an extended service interruption.

The following criteria were used in reporting this finding:

- OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*
- NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems
- FIPS Pub. No. 87, *Guidelines for ADP Contingency Planning*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that the agency is in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility; plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training primary and back-up personnel, and frequency of updates, periodic tests, etc***.

Management's Response:

MSHA completed a risk analysis of the General Support System (LAN/WAN) and the Major MSHA Applications in November. The Vulnerability Reports have been submitted to the DOL OCIO for review.

As part of the MSHA Security Program Plan, MSHA will develop a contingency plan for the MSHA LAN/WAN and all major applications beginning the second quarter of FY 2001. MSHA developed a Security Program Work Plan that includes the purpose, objectives and deliverables for a Contingency Plan. One of the deliverables is a plan to test the Contingency plan.

OIG's Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA Security Program Plan and the implementation of the Contingency Plan during the FY 2001 audit.

Current Year Management Letter Comments

a. Segregation of Duties

During our FY 2000 audit we found the duties currently performed by computer operations and application programming are not appropriately segregated. Specifically, MSHA's Production Control function responsible for running production jobs reports directly to the Manager of System Design and Management Division and not to the Systems Operation and Communication Division. Duties that are inappropriately separated lead to the risk that a single individual may adversely impact the availability, confidentiality and integrity of the system by being in a position to override/by-pass key controls established by management.

The following criteria were used in reporting this finding:

- NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*
- NIST 800-12: *An Introduction to Computer Security*

Recommendation:

The following prior year recommendation to the Chief Information Officer and the Assistant Secretaries pertains to this finding:

- ***ensure that MSHA's SSP is in compliance with the CIO's Computer Security Handbook and clearly define roles and responsibilities of its staff members in accordance with the least privileged concept and that duties performed by its employees do not allow the circumvention of management's intended controls.***

Management's Response:

The Production Control staff has been placed under the Systems Operations and Communications Division and report to the Manager of that division. See PEIR organization chart below.

MSHA Organization Chart

In file “FINAL 2000 CIO Report Graphic3.wpd

OIG’s Conclusion:

This recommendation is **resolved and open**. Closure is dependent upon our review of the new MSHA Security Program Plan and structure during the FY 2001 audit.

OFFICE OF THE ASSISTANT SECRETARY FOR ADMINISTRATION AND MANAGEMENT (OASAM)

We tested general controls and security over EDP systems of the OASAM as they pertain to the following critical financial application.

- Purchase Request Information System (PRISM)

Issues reported by management as being closed during the period under review were re-tested using GAO's Federal Information System Controls Audit Manual (FISCAM). The OIG's IT Audit Rotation schedule did not include any new testing to be performed as part of the FY 2000 Financial Statement Audit.

1. DOL Needs to Strengthen Controls to Protect Its Information

Status of Prior Year Findings and Recommendations

Risk Assessments

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that the Office of Business System Services (OBSS) did not have a completed/approved risk assessments that considers data sensitivity and integrity, the range of risks to the entity's systems and data, and resource classifications for the PRISM application. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessment, security management structure, and access monitoring.***

During our FY 2000 audit, we found that a risk assessment for PRISM is in progress. Management stated that 60 percent of questionnaires fielded for vulnerability assessing have been received and answers imported in Risk Watch. This recommendation is **resolved and open**. Closure is dependent on our review of the completed risk assessment.

Management's Response:

The PRISM risk assessment, through use of Risk Watch software, was formulated during August-September, 2000. A draft report was submitted to the OCIO October 3, 2000. Resulting comments made by the OCIO were considered, and appropriately incorporated into the risk assessment. A second draft report was submitted to the OCIO on December 11, 2000, for final review and management approval.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed risk assessments during the FY 2001 audit.

Entitywide Security Program Plan

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that OASAM's security plan can be enhanced to further meet federally established criteria. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that computer security plans are developed and implemented for all departmental systems.***

During our FY 2000 audit, we found that management is currently updating all of the System Security Plans in accordance with the Department of Labor's revised Computer Security Handbook. This recommendation is **resolved and open**. Closure is dependent on our review of the completed security plan.

Management's Response:

The PRISM System Security Plan, using a newly revised template provided by OCIO, was submitted to the OCIO December 6, 2000. OCIO comments, received December 28, 2000, will be incorporated into the plan.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed PRISM System Security Plan during the FY 2001 audit.

Incident Response Capabilities

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that OASAM's reporting of incident responses could be improved. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that departmental and agency policies exist and are implemented to address computer security incident response.***

During our FY 2000 audit, we found that OASAM incident response procedures have been revised and addressed in the Computer Security Handbook. This recommendation is **resolved and open**. Closure is dependent on our review of the agency's implementation of incident response procedures during FY 2001.

Management's Response:

No additional comments are provided by OASAM. PRISM follows the operating guidelines contained in Appendix D, "Detailed Technical Incident Response Procedures," of the DOL Computer Security Handbook.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the agency's implementation of incident response procedures during the FY 2001 audit.

Personnel Security Controls

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that OBSS has not implemented effective security controls related to personnel policies and procedures. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***a background check to be conducted for all Government and contractor management personnel with high levels of system access.***

During our FY 2000 audit, management stated the following after our field work was completed:

- The physical, operation and system security controls are in progress along with OBSS Major Application and General System Support Plans.
- All OBSS job descriptions and related duties have been reviewed and updated. A training form was developed to document and track all employee training and professional development. Training forms have been distributed to personnel for any updates.
- In accordance with DOL Computer Security Handbook, a security awareness and education program must be included in all system security plans. All OBSS personnel will receive awareness training biannually.

This recommendation is **resolved and open**. Closure is dependent on our review of the agency's completed system security plan, and management's submission of the document as part of the FY 2001 audit.

Management's Response:

OBSS position descriptions address assignment of computer security and other related system administration duties to senior computer specialist staff within OBSS.

Nearly 75 percent of OASAM's information technology staff, including the three (3) computer specialists within OBSS, participated in the all-day DOL Computer Security Awareness Day held

on October 25, 2000. Attendance records for the various programs and keynote speaker sessions are available from the OCIO.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the agency's completed system security plan addressing personnel security and management's submission of the documentation of the security training during the FY 2001 audit.

Independent Review of Critical Systems

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that the general support system of PRISM has not undergone an independent review or audit within the last 3 years. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that agencies are in compliance with the computer security handbook by verifying that all financially significant applications and support systems have been properly accredited and that independent functional reviews are conducted at least every 3 years.***

During our FY 2000 audit, we found that a security review of the GSS is scheduled. This recommendation remains **resolved and open.** Closure is dependent upon our review of the accreditation and independent functional review of PRISM.

Management's Response:

The Employee Computer Network (ECN) underwent an OIG penetration test during September 2000. A report covering the PRISM penetration test, which generally covers the access controls within PRISM, is in draft; the final report has not yet been completed by OIG.

OIG's Conclusion:

This recommendation remains **resolved and open** pending the submission of the accreditation and independent functional review of PRISM to the OIG during the FY 2001 audit.

Authorizations and Monitoring of Logical Access

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that policies and procedures over the authorization, modification, and periodic monitoring of users (end users, contractors, production support, etc.), having logical access to the PRISM environment (application, operating system, databases, utilities, etc.) require improvement. Specifically, the

PRISM users selected for testing did not have the appropriate access authorization forms on file. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs contain sufficient policies and procedures governing the authorizing, modification, removal, monitoring of access based on the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.***

During our FY 2000 audit, we found that policies governing authorizing, modification, and monitoring of PRISM users will be included in the PRISM system security plan. All PRISM users, production and test, will have appropriate access forms on file.

This recommendation is **resolved and open**. Closure is dependent on our review of the PRISM SSP and the retesting of authorization forms.

Management's Response:

OBSS maintains a file of PRISM access authorization forms in the director's office, and are available for OIG review. On December 7, 2000, OBSS submitted a request for recertification, in the form of a "Procurement Software Registration Form," to the supervisor/manager of every production system PRISM user. Approximately 90 percent of the 68 forms have been completed and returned. Outstanding forms are expected in OBSS in the near future.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the PRISM SSP and the retesting of authorization forms during the FY 2001 audit.

Physical Controls

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that physical controls to prevent or detect unauthorized or inappropriate access to the ITC data center need improvement. We made the following recommendation:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate controls for the protection of the physical environment in which system hardware, backups, telecommunication equipment, and***

other sensitive components reside. In addition, we recommend agency SSPs include specific technical standards (security settings, critical system configurations, etc.) for each general support system and major application.

During FY 2000 we noted that access to the data center can be further restricted. Specifically, we found that:

- 4 of the 20 individuals reviewed no longer have a business need to the data center and their access should be revoked
- 6 of 20 individuals were from the CFO's office and were deemed to have inappropriate access to the data center based upon their job function
- 3 of 20 access request forms could not be found documenting access
- 9 of the 20 forms did not contain sufficient information to adequately identify the access being granted.
- 16 of the 20 forms did not contain adequate approvals.

This recommendation is **resolved and open**. Closure is dependent on our review of the completed corrective actions that prevent or detect unauthorized or inappropriate access to the ITC data center during FY 2001 audit.

Management's Response:

Fire extinguishers are periodically serviced, with the most recent service during December 2000. Surveillance equipment will be considered during the computer room renovation scheduled for FY 2002, although no regulation requiring such equipment has been discovered. The changes that have been made to date regarding computer room access control are considered adequate for the current configuration.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed corrective actions that prevent or detect unauthorized or inappropriate access to the ITC data center during FY 2001 audit.

Password Parameters

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that logical access controls over the PRISM application server could be improved. We made the following recommendation:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate controls for the protection of the physical environment in which system hardware, backups, telecommunication equipment, and***

other sensitive components reside. In addition, we recommend agency SSPs include specific technical standards (security settings, critical system configurations, etc.) for each general support system and major application.

During our FY 2000 audit, we found that corrective actions are in progress. This recommendation is **resolved and open**. Closure is dependent on our review of the completed corrective actions.

Management's Response:

All corrective actions have been completed. Accounts no longer are locked out for 30 minutes; such lockout now requires intervention by the help desk managed by ITC's Computer Technology Center. Privileged user passwords are now distributed to individual local system administrators. Password aging on any server is now set to an ITC standard.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed corrective actions during the FY 2001 audit.

NT Security Settings

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that security settings for the PRISM NT server are not optimally configured to (1) restrict users from having more access rights to system and application files then are required, and (2) to reduce the risk of unauthorized access to the server. In addition, the administrator account is permitted to log on to the server from the network and null session access is allowed to the PRISM NT server. We made the following recommendation:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate controls for the protection of the physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside. In addition, we recommend agency SSPs include specific technical standards (security settings, critical system configurations, etc.) for each general support system and major application.***

During our FY 2000 audit, we found that corrective actions are in progress. This recommendation is **resolved and open**. Closure is dependent on our review of the completed corrective actions.

Management's Response:

NT and advanced user rights are now appropriately assigned to each server. Permissions for directories on the PRISM production server are now adequately restricted. User connection to the PRISM server is satisfied through the use of Oracle software, and is activated only upon required database access requests. The period of inactivity has been reviewed, and users are now logged off after expiration of the inactivity time. A screen saver with password has been enabled on the PRISM server. PRISM operates in a 24/7 mode, except for late weekends to accommodate database unload; forced logoff is not appropriate.

The local administrator account is not permitted to logon to the server from the network; PRISM system administrators may use their network accounts to log onto the server to enable access to other network tools. Null sessions have been eliminated for all server access.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed corrective actions during the FY 2001 audit.

2. DOL Needs to Fully Implement a Systems Development Life Cycle Methodology

Status of Prior Year Finding and Recommendation

System Software

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that system software policies and procedures governing technical, monitoring, and configuration management controls can be improved. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that the SDLC manual provides adequate guidance for the monitoring of access and use of system software utilities.***

During FY 2000, we found that a Configuration Control Board has been created by ITC/OCIO to review all Change Requests. A comprehensive and complete System Development Life Cycle (SDLC) and Change Management process exist to ensure all changes to hardware and software are formally requested, approved and adequately tested to minimize the risk of errors and irregularities in the production environment. This recommendation is **resolved and open**. Closure is dependent on our review of the agency's policies and procedures during FY 2001.

Management's Response:

ITC manages the system change process throughout the ECN through the use of System Change Requests.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the agency's policies and procedures during the FY 2001 audit.

3. DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

Status of Prior Year Findings and Recommendations

Emergency Response Capabilities

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that emergency response policies and procedures are inadequate to ensure staff is trained in and is aware of their responsibilities in preventing, mitigating, and responding to emergency situations. We made the following recommendations to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that agencies are in compliance with the computer security handbook and that agency SSPs include appropriate policies and procedures for:***
  - ***properly creating, securing, maintaining, and rotating backups;***
  - ***emergency responses and ensure training is provided to appropriate personnel;***
- ***ensure that adequate environmental controls are in place at DOL data center facilities; and***
- ***ensure agencies are in compliance with its SDLC manual that includes guidelines for: (1) using and monitoring use of system software utilities, (2) identifying, selecting, installing, and modifying system software, and (3) effective hardware maintenance, problem management, and change management to assist in preventing unexpected interruptions.***

During our FY 2000 audit, we found that contingency planning in accordance with the DOL computer security handbook does address response policies/procedures for all situations, and mandates these procedures to be part of the system security plans. In order to standardize all Agency response procedures, the Critical Infrastructure Protection Work Group is tasked with developing a contingency plan template. Upon completion of this template, OBSS will update its current contingency plan. Therefore, until the agency updates its contingency plan based on the new template, these recommendations are **resolved and open**. Closure is dependent on our review of the agency's completed emergency response procedures.

Management's Response:

Appendix C, "Contingency Planning and Methodology Guide," of the DOL Computer Security Handbook provides contingency planning policies. Development of procedures for preventing, mitigating and responding to emergency situations within PRISM are underway as part of OASAM's effort to formalize standard operating procedures.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the agency's completed emergency response procedures during the FY 2001 audit.

Alternate Data Processing Facilities

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that OASAM does not have arrangements for an alternate data processing and telecommunication facility (e.g., Hotsite). We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility; plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training for primary and backup personnel, and frequency of updates, etc.***

During our FY 2000 audit, we found that a hotsite has been designated and Frame Relay circuits have been ordered and installation has begun. This recommendation is **resolved and open**. Closure is dependent on our review of the completed corrective action plan.

Management's Response:

OASAM is near completion of testing its hot-site facility in Kansas City. It is anticipated that the site will be completed in the near future.

OASAM has in place and functioning an ATM/Frame Relay. The next phase of the plan is to install and setup an Internet connection and mirrored servers to ensure adequate backup of information resources and continuity of operations.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the agency's completed emergency response procedures during the FY 2001 audit.

Periodically Test the Contingency Plan and Adjust it as Appropriate

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that OASAM's Business Continuity and Contingency Plan (BCCP) was not tested during the period under review. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, the CIO should ensure that appropriate test plans (full and partial) are conducted on a periodic basis.***

During our FY 2000 audit, we found that due to the level of effort and extensive preparations required for Y2K readiness, the BCCP was not tested until after the audit period. This recommendation is **resolved and open**. Closure is dependent on our review of the agency's completed BCCP test plan.

Management's Response:

The BCCP, the Department's Continuity of Operations Plan (COOP) and the evaluation performed by FEMA during September 2000, and the Critical Infrastructure Protection Plan (CIPP) have been submitted to OIG in November 2000 for review. An update to the COOP is scheduled for submission to FEMA by September 1, 2001.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the agency's completed BCCP test plan during the FY 2001 audit.

OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION (OSHA)

We tested general controls and security over EDP systems of the OSHA as they pertain to the following critical financial application:

- Integrated Management Information System (IMIS)

Issues reported by management as being closed during the period under review were retested using GAO's Federal Information System Controls Audit Manual (FISCAM). The OIG's IT Audit Rotation schedule did not include any new testing to be performed as part of the FY 2000 Financial Statement Audit. The scope in the prior year was limited to the EDP controls that are the responsibility of OSHA as they relate to the mainframe processing of IMIS. Therefore, the following outlines the controls deemed out of scope and were not tested:

- Controls that are the responsibility of DOL's contractor, SunGard. SunGard supports and maintains the mainframe operating system and physical environment used to process and store IMIS application data.

- Controls associated with the UNIX environments running the client server portion of IMIS. UNIX is the platform used to host/NCR or Front End Processor (FEP) that initially processes and transmits information from the field offices tot he SunGard mainframe. However, physical control weaknesses noted with the Washington D.C., UNIX environment were documented and reported in this summary.

1. DOL Needs to Strengthen Controls to Protect Its Information

Status of Prior Year Findings and Recommendations

System Accreditation

During our FYs 1999 and 1998 audits (OIG Report No. 12-99-002-13-001 and 12-00-002-13-001), we found that IMIS did not have a written authorization or accreditation statement from the program or function managers whose missions are supported by OSHA. We made the following recommendations to the Chief Information Officer and the Assistant Secretaries:

- ***agencies are in compliance with the security handbook by verifying that all financially significant applications support systems have been properly accredited, and that independent functional reviews are conducted at least every 3 years, and***
- ***all departmental systems are accredited by the program management.***

During our FY 2000 audit, we found that OSHA management was working with the OCIO to reexamine the security of the IMIS to verify proper accreditation. These recommendations are **resolved and open**. Closure is dependent on our review of the completed accreditation of the IMIS system.

Management's Response:

OSHA has adopted the DOL Systems Development and Life Cycle Management Manual (SDLCM) methodology. The DOL SDLCM has been distributed to Federal and Contractor staff for immediate use on the IMIS Re-Write task.

However, from a closer examination of Federal and DOL requirements documents, including OMB Circular A-130, the DOL Systems Development and Life Cycle Management Manual (Version 2.0), and FIPS Pub 102, OSHA has determined that establishing a program for certification and accreditation is a major effort that will require policies and procedures, allocation of a variety of roles and responsibilities, a prioritized listing, based on mission needs, of those applications that require certification and accreditation, development of an organization structure to handle certifications and accreditations, staffing, training, and support. These activities will take a significant amount of time, human resources, and funding to complete.

OSHA plans to begin work with the OCIO in early January 2001, to address:

- Whether the OCIO plans to establish a DOL program for certification and accreditation, or if individual agencies are expected to establish their own programs.
- What time frame is projected? What resources will be available to assist agencies?
- What interim processes and procedures agencies can use for legacy systems, such as the IMIS, to satisfy certification and accreditation requirements while a certification and accreditation program is being built?

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of OSHA's corrective actions during the FY 2001 audit.

Entitywide Security Program Plan

During our FY 1997 and FY 1999 audits (OIG Report No. 12-98-002-13-001 and 12-00-002-13-001), we found that OSHA does not have a formally approved entitywide security plan. We made the following recommendations to the Chief Information Officer and the Assistant Secretaries:

- ***ensure computer security plans are developed and implemented for all departmental systems, and***

- ***entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, and access monitoring.***

During our FY 2000 audit, we found that OSHA had received feedback and comments on the IMIS Draft 1998 Security Plan from the OCIO. OSHA is reviewing these comments. OSHA will work with the OCIO to update the IMIS security plan in accordance with the DOL Computer Security Handbook, version 1.0. These recommendations are **resolved and open**. Closure is dependent upon our review of the completed IMIS security plan.

Management's Response:

Independent risk assessments of the IMIS were completed in November 2000. In compliance with OMB Circular A-130 and DOL Computer Security Handbook requirements, OSHA is updating the IMIS System Security Plan (SSP) to reflect not only the risk assessments findings, but also to address SOF2 issues. The target completion date for the IMIS SSP is January 5, 2001.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the updated IMIS System Security Plan during the FY 2001 audit.

Personnel Policies and Procedures

During our FY 1997 and FY 1999 audits (OIG Report No. 12-98-002-13-001 and 12-00-002-13-001), we found that OSHA management information security controls related to personnel policies and procedures are inadequate. We made the following recommendations to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that a background check should be conducted for all Government employees and contractor management personnel with high levels of system access,***
- ***ensure computer security plans include procedures for proper termination of systems access of former employees, and those procedures are implemented, and***
- ***ensure that all applicable employees and contractors receive the required training and maintain the appropriate documentation (e.g., lists of employees as of the training course date, attendance sheet of employees taking the course, topics, agendas, handouts, etc., provided during the program).***

During our FY 2000 audit, we found that OSHA was working with the OCIO to update the IMIS security plan to include personnel policies and procedures to correct OSHA's deficiencies in

accordance with the DOL Computer Security Handbook, version 1.0. These recommendations are **resolved and open**. Closure is dependent upon our review of the completed IMIS security plan.

Management's Response:

Security, confidentiality and non-disclosure requirements were written into the recent Task Order for the IMIS Security Plan Update. This practice is expected to be expanded to other IMIS-related Task Orders.

OSHA has begun exploring, in concert with other DOL agencies, the development and use of confidentiality/security agreements for employees and contractors. Efforts in this area are expected to continue throughout FY 2001. Closure may require consultation with the unions.

A Separation Clearance form and process has been developed and implemented for contract personnel to address ID badges, hardware and software, keys, and deletion of user IDs. A Separation Clearance process exists for Federal staff. During the 2nd Quarter of 2001, OSHA will evaluate this process for possible improvements to ensure timely notification and deletion of user IDs.

The Directorate of Information Technology (DIT) initiated dialog with OCIO staff, OSHA's Office of Personnel Management, and OASAM to obtain guidance and documentation on implementing a background screening program for Federal and contract personnel. By the end of the 3rd Quarter of 2001, OSHA expects to have identified staff requiring background screening and the level of screening required, and to begin scheduling the screening.

OSHA was a full participant on the committee to plan the annual DOL Computer Security Awareness Day, including user and technical training sessions. Sign-in logs provided a mechanism to record the participation of OSHA federal and contract staff.

A computer security awareness and training plan will be developed and included in the Agency's Cyber Security Program Plan scheduled for submission to the OCIO by December 29, 2000. Awareness and training are expected to be ongoing. Documentation and monitoring of training will be addressed in the Plan.

Informal dialog on the need to have position descriptions revised to reflect IMIS security responsibilities has been initiated with OSHA's Office of Personnel Management. Closure is expected to depend on OSHA working with OASAM and the OCIO.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of IMIS documentation and corrective actions during the FY 2001 audit.

Risk Assessments

During our FYs 1998 and 1999 audits (OIG Report No. 12-99-002-13-001 and 12-00-002-13-001), we found that OSHA does not have a completed/approved risk assessment that considers data sensitivity and integrity, the range of risks to the entity's systems and data, and resource classifications. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that entitywide security programs are developed, documented and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessments, security management structure, and access monitoring.***

During our FY 2000 audit, we found that OSHA purchased the Risk Watch Automated Risk Analysis software tool in FY 1999 and staff attended training. OSHA staff has been a part of the Critical Infrastructure Protection workgroup that has contributed to the Vulnerability Assessment guide and the DOL Computer Security Handbook. This recommendation is **resolved and open**. Closure is dependent upon our review of the completed risk assessment.

Management's Response:

OSHA procured the services of Troy Systems to conduct an independent RiskWatch quantitative risk assessment and a qualitative risk assessment of the IMIS. Troy submitted final reports to OSHA on November 28, 2000. Copies of the reports have been submitted to the OCIO for review.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the completed risk assessment during the FY 2001 audit.

Authorization and Monitoring of User Logical Access

During our FYs 1998 and 1999 audits (OIG Report No. 12-99-002-13-001 and 12-00-002-13-001), we found that controls over the authorizing and periodic monitoring of users having logical access (including dial-in) to OSHA's Integrated Management Information System (IMIS Host/Micro Systems) are inadequate. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient polices and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A recertification should be conducted of all IDS on the system and the business need documented. In addition,***

IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.

During our FY 2000 audit, we found that OSHA was in the process of reexamining IMIS user IDS for accuracy and completeness and we will make the appropriate changes. OSHA's final resolution will be in compliance with the DOL Computer Security handbook, version 1.0. OSHA will work very closely with the OCIO to set up procedures, guidelines, and oversight for providing the list of authorized users and their authorized access level. Management is reviewing its procedures on authorizing access and should have a corrective action plan to correct the deficiencies during the 1st quarter of FY 2001. This recommendation is **resolved and open**. Closure is dependent upon our review of the completed corrective action plan.

Management's Response:

Federal and contract staffs working on the IMIS Re-Write have been tasked to address the SOF 6 weaknesses. In the interim, OSHA plans to develop and/or update formal IMIS Host/Micro Systems' policies and procedures to cover the authorization, modification, deletion/termination, and periodic re-certification of user access and assignment of access, by the 3rd Quarter of FY 2001.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions during the FY 2001 audit.

Authorization and Monitoring of User Physical Access

During our FY 1999 audit (OIG Report No. 12-00-002-13-001), we found that controls over the authorizing and periodic monitoring of users having physical access to OSHA Communication Center can be improved. We made the following recommendation:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs (for its GSS and MAs) include appropriate controls for the protection of physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside. In addition, we recommend agency SSPs include specific technical standards (security settings, critical system configuration, etc.) for each general support system and major application.***

During our FY 2000 audit, we found that OSHA was in the processes of establishing and implementing a standard key access form for requesting card key access and developing and maintaining an OSHA Communication Center visitor log. In addition, OSHA will document and implement formal physical security policies and procedures for the OSHA Communication Center by the end of 1st quarter FY 2001. This recommendation is **resolved and open**. Closure is

dependent on our review of OSHA's physical security policies and procedure for the OSHA Communication Center.

Management's Response:

OSHA has established, published, and implemented access policy and procedures for the Communications Room (FPB-S6212) to provide a standard format and process for requesting key cards and replacement key cards, to establish appropriate and inappropriate use policy, and to provide a Log of visitors (anyone without a key card).

OSHA has developed a Separation Clearance form and process for contract personnel to include sign-off to verify that a departing employee has returned his/her key card.

OSHA has initiated dialog with the Office of Administrative Services about the need to work with the Department to establish processes and procedures to ensure that OSHA has: 1) a feedback mechanism that provides a record of authorizations; 2) periodic, but regular, reports on who has what access, and to verify that action has been taken on requests for deletion/deactivation of cards. Work to make additional process improvements is expected to continue in the 2nd Quarter of FY 2001.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions during the FY 2001 audit.

2. DOL Needs to Fully Implement a Systems Development Life Cycle Methodology

Status of Prior Year Findings and Recommendations

Systems Development Life Cycle Methodology

During our FY 1999 audit (OIG Report No. 12-00-002-13-001), we found that OSHA has not established a system development life cycle (SDLC) methodology meeting Federal standards and guidelines. We made the following recommendation:

- ***ensure the SDLC process is followed by all DOL and contractor personnel who are developing, acquiring, or managing systems or making enhancements to existing systems.***

During our FY 2000 audit, we found that OSHA stated it has been a full participant in the OCIO SDLC workshops held during May 2000. OSHA is currently reviewing the results of these workshops and will be providing comments to the OCIO. Upon review and approval by all Agencies and the distribution of the DOL SDLC by the OCIO, OSHA will work with the OCIO

and the Assistant Secretary to ensure this SDLC process is followed by all OSHA and contractor personnel. This recommendation is **resolved and open**. Closure is dependent on our review of OSHA's completed SDLC policies and procedures.

Management's Response:

OSHA has adopted the DOL Systems Development and Life Cycle Management Manual methodology. Federal and Contractor staff, working on the IMIS Re-Write, is using the document to integrate security requirements into the life cycle process. Specifically, OSHA has a team working on a recommendation for change control and configuration management, including evaluation of configuration management products. The primary focus of the team is on software that will be used to implement changes on mainframe applications (both application and system software), desktop applications, production file servers, Oracle applications (both application and system software), Unix applications, and network applications, including Hub and gateway protocols.

In the interim, OSHA has been working to develop a more formalized approach to IMIS project management that encompasses Application Development and Change Management. Specifically, Microsoft Project, Formal Test Plan documentation and electronic mail are being used to document the change control process. However, by the end of the 2nd quarter, FY 2001, OSHA expects to implement a more formal approach to sign-off and information gathering that will serve to document the process end-to-end.

By the end of 3rd quarter FY 2001 the Change Control and Configuration Management Team is expected to present its findings and recommendations for software products that can be used to implement applications software change control on the various platforms.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions during the FY 2001 audit.

3. DOL Needs to Complete and Fully Test Its Plan(s) for Maintaining Continuity of Operations

Status of Prior Year Findings and Recommendations

Service Continuity Plan

During our FY 1999 audit (OIG Report No. 12-00-002-13-001), we found that an OSHA disaster recovery/business continuity plan for the national office to recover local area network, NCR

microcomputers and telecommunications in the event of an extended outage of information system processing does not exist. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility; plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training primary and back-up personnel, and frequency of updates, etc.***

During FY 2000, we found that OSHA was working with the OCIO to revise and update the IMIS Contingency Plan in accordance with the DOL Computer Security Handbook, version 1.0. This recommendation is **resolved and open**. Closure is dependent on our review of the completed IMIS Contingency Plan.

Management's Response:

OSHA has been a full participant in the DOL Critical Infrastructure Protection Work Group's (CIPWG) effort to develop a template for contingency plans for DOL-wide use, and to search for COTS products that may aid the contingency planning effort. In addition, a white paper has been developed to address contingency plans for the IMIS NCR's. The due date for contingency plans has not yet been determined by the OCIO. However, OSHA expects to initiate plans to update the existing IMIS contingency plan during the 2nd Quarter of FY 2001. The plan is expected to be a living document to be updated in compliance with Federal and DOL requirements.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the approved contingency plan during the FY 2001 audit.

EMPLOYMENT AND TRAINING ADMINISTRATION (ETA)

We tested general controls and security over EDP systems of the ETA as they pertain to the following critical financial application.

- Unemployment Insurance System (UIS)

Issues reported by management as being closed during the period under review were retested using GAO's Federal Information System Controls Audit Manual (FISCAM). The OIG's IT Audit Rotation schedule did not include any new testing to be performed as part of the FY 2000 Financial Statement Audit.

1. DOL Needs to Strengthen Controls to Protect Its Information

Status of Prior Year Findings and Recommendations

Independence of Security Administration

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found the independence of the security administration function can be strengthened. In addition, the duties currently performed by the security administrator are not appropriately segregated. Specifically, the ETA Information Security Officer reports directly to the ETA Chief of Operations and not to the ETA Chief Information Officer. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that entitywide security programs are developed, documented, and implemented for all departmental systems. The programs should include an up-to-date security plan, risk assessment, security management structure, and access monitoring.***

During our FY 2000 audit, we found management is currently updating its security reporting procedures. In addition, management stated that starting immediately, UIS will report all security issues pertaining to the UIS network directly to the ETA Information Security Officer, ETA Chief of Operation, and the ETA Chief Information Officer. This recommendation is **resolved and open**. Closure of this issue is dependent on our review of the security reporting procedure as a part of our FY 2001 audit.

Management's Response:

1. Updated System Security Plan - *Provided to the OIG with Response to Draft Report.*
2. Updated Risk Assessment - *Provided to the OIG with Response to Draft Report.*
3. Security Management Structure - ETA will be adding additional security staff to the team, which will allow ETA to implement a totally integrated security management structure and

will include access monitoring. New Security Management Structure will be included in the updated SSP due April, 2001.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the documentation provided in response to the draft report and the other corrective actions taken during our FY 2001 audit.

Security Awareness

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found an ongoing security awareness program does not exist. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***all applicable employees and contractors receive the required training and maintain appropriate documentation (e.g., list of all employees as of the training course date, attendance sheet of employees taking the course, topics, agendas, handouts, etc., provided during the program).***

During our FY 2000 audit, we found management is currently working with the Office of the Chief Information Officer (OCIO) to develop a security awareness training program. According to management, a draft security awareness program is scheduled to be ready for review by the OCIO in the first quarter of FY 2001. This recommendation is **resolved and open**. Closure is dependent upon our review of the security awareness training program as a part of the FY 2001 audit.

Management's Response:

1. ETA is currently developing a policy that states that all employees associated with ETA security efforts must attend security training every year to upgrade their skills and security awareness.

2. In October, 2000, ETA coordinated with the Department and presented an annual security awareness training program for National office employees. This awareness training program was presented on October 25, 2000.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions taken and security awareness training program during our FY 2001 audit.

Incident Response Capabilities

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found that ETA's reporting of incident responses could be improved. We found the following does not exist:

- Written procedures for communicating and reviewing security incident reporting violations for UIS system.
- A centralized e-mail address that forwards mail to UIS, ETA and CIO security staff members and permit users to conveniently exchange information with the security administration.

We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate policies and procedures for the monitoring of inappropriate or unusual activity occurring on the system. Policies and procedures should include, but are not limited to management's determination of what should be recorded on logs and what constitutes a violation of the policy, frequency of reviews, reporting and escalation processes, and maintenance of documentation (manual or automated) for audit trail purposes, etc.***

During our FY 2000 review, we found ETA has updated its security reporting procedures to include:

- All security incidents shall be immediately reported to the following Federal staff:
  - UI - Chief, Division of Data Systems and Support
  - UI - Task Team Leader
  - UI - Task Order Project Officer (Will keep records on file and copies in our fire-proof safe.)
- Detail information concerning the incident shall be reported to the Office of Technology and Information Services (OTIS). Documented information will be given to the OTIS-Senior Security Officer, OTIS-Chief, Information Officer (CIO). The CIO reports all network security issues to senior level management of ETA. Both hard and electronic copies of indents shall be kept on file for review. Electronic files are backed up nightly.

As of September 30, 2000, management did not provide evidence that the procedures outlined in the status were added to ETA's security plan. This recommendation is **resolved and open**. Closure of this issue is pending the submission of the revised plan that includes the new procedures and the FY 2001 audit to test the operating effectiveness of the new controls.

Management's Response:

1. ETA's revised security plan due in April, 2001 will include the document detailed incident reporting policy and procedures.

2. OWS has updated the incident response section in the security plan since the OIG report. However, the entire plan is undergoing further revisions as a result of a review from the Department CIO's office (report prepared by Troy Systems). A copy of the plan will be available for OIG review by December, 2000. For details on the ETA incident reporting policies, refer to Appendix 1 of the System Security Plan from the Office of Technology and Information Services.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the corrective actions taken during our FY 2001 audit.

Physical Controls

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found physical controls to prevent or detect unauthorized or inappropriate access to the Office of Technology and Information Services (OTIS) data center need improvement. Specifically, the following conditions were found:

- Controls over the authorizing and periodic monitoring of users having physical access to OTIS data center (rm. S6222 and S6228) can be improved. Our review noted that policy and procedures do not exist for the authorization, modification/reissuance, deletion, and periodic recertification of electronic card keys and standard keys. Specifically, the following weaknesses were identified:

    - Access request forms for card keys (allowing access to the data center doors) are not used.
    - Three of 23 individuals tested for having access to the data center were deemed to have inappropriate access.

- Visitors are not controlled.
    - Operations personnel are not aware of routinely scheduled cleaning maintenance shifts.

We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that agency SSPs include appropriate controls for the protection of the physical environment in which system hardware, backups, telecommunication equipment, and other sensitive components reside. In addition, we recommend agency SSPs include specific technical standards (security settings, critical system configurations, etc.) for each general support system and major application.***

During our FY 2000 audit (OIG Report No. 12-00-003-13-001), we found ETA's Office of Technology and Information Services management are updating the policies and procedures for the authorization, modification/reissuance, deletion and periodic recertification of electronic card keys and standard keys. This recommendation is **resolved and open**. Closure is dependent on our review of the updated policies and procedures.

Management's Response:

1. Access Request Forms - Request Forms are now required to have access granted to the Data Center. *Provided to the OIG with Response to Draft Report.*
2. Access to the Data Center - ETA has reduced the number of employees with access to the Data Center and removed access from non-essential staff.
3. Visitors - ETA has implemented and posted a sign-in procedure for all visitors entering the Data Center.
4. The updated SSP due in April, 2001 will include ETA Data Center policy.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the updated policies and procedures during the FY 2001 audit.

Application Documentation

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found the application manual for the UIS Subsystem, FMRS (Financial Management Report System) is inadequate. The instructions did not provide sufficient information to be used as a user manual. Specifically, the document provided to users did not explain how to perform data processing or adequately document the application's functions. We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***the Chief Information Officer complete the "Department of Labor Computer System Development Life Cycle (SDLC) Manual" that addresses policies and procedures for documenting various aspects of the system (including user manuals) and under what conditions documentation should be updated. The manual should be reviewed and approved by all agency heads, issued, and followed.***

During our FY 2000 audit, we found that the CIO has issued the SDLC manual. We also found subsystems within OWS (UIS) follow the SDLC. Program documentation for the FMRS has been done, however, program staff did not feel the need for a user's manual due to a small number of users having access to the FMRS application. In addition, user turnover is low; therefore, training of new users is infrequent. Thus, development of a user manual was not a program office priority and not cost effective considering the time and effort in terms of dollars. OWS stated it assumes the risk of not closing this issue. This recommendation is now **unresolved**. Resolution depends on the OWS developing the FMRS application user manual.

Management's Response:

The Division of Fiscal and Actuarial Services (DFAS) is the program area within OWS which is responsible for the FMRS system. At this time, due its small number of users and turnover being relatively low, the development of a user's manual was not considered cost effective by the program area.

OIG's Conclusion:

This recommendation remains **unresolved**, resolution is dependent on the OWS developing alternative measures for a FMRS application user manual.

Authorization of Application Changes

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found software modifications were not consistently approved by the Project Manager. Specifically, in four of the six changes tested we found that the Project Manager had not signed-off.

We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure this SDLC process is followed by all DOL and contractor personnel who are developing, acquiring, or managing new systems or making enhancements to existing systems.***

During our FY 2000 audit, we found procedures have been updated. All signatures are required before any changes are accepted. The Project Manager has been informed of this procedural change. However, the OIG has not received the ETA Office of Work Force Security updated procedures that indicate all signatures are required before any changes. In addition, no change requests were received showing compliance with the new procedures. This recommendation is **resolved and open**. Closure is dependent on our FY 2001 audit to review procedures and to test the operating effectiveness of the new controls.

Management's Response:

OWS procedures for this finding have been completed. *Provided to the OIG with Response to Draft Report.*

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review and testing of the OWS procedures submitted during the FY 2001 audit.

Documenting Application Changes

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found controls over the inventory of program changes could be improved. The documentation log kept by configuration management does not provide adequate information on change requests. Specifically, we noted the following conditions:

- The log does not detail the current status of change requests and software modifications.
- There is no correlation between the system-generated report and the document control log. The application version number cannot be determined from the title/description in the documentation logs.
- Neither operations nor configuration management could identify the specific operator who implemented the change.

We recommended that:

- ***the Chief Information Officer complete the "Department of Labor Computer System Development Life Cycle (SDLC) Manual" that addresses policies and procedures for documenting various aspects of the system (including user manuals) and under what conditions documentation should be updated. The manual should be reviewed and approved by all agency heads, issued, and followed.***

During our FY 2000 audit, we found the CIO has issued the SDLC manual and OWS is working on further enhancing this process by configuring a third party package for software configuration management and improving its software inventory and tracking capabilities. In addition, management is in the process of reviewing the Configuration Management procedures, and will determine whether the process of creating and packaging software changes can be better controlled. Updates to the current procedures will change as required. This recommendation is **resolved and open**. Closure is dependent on the OIG review of the corrective actions in our FY 2001 audit.

Management's Response:

OWS has enhanced the configuration management process by configuring and installing a third party product : CCC- Harvest. Further, updates to its existing procedures have been completed to address these findings. *Provided to the OIG with Response to Draft Report.*

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the documentation provided and corrective actions taken during the FY 2001 audit.

Storage of Critical Information Off-Site

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found controls surrounding the storage of UIS's back-up tapes and the Disaster Recover Plan can be improved. The following weaknesses were noted:

- Policies and procedures for the safeguarding, monitoring and maintenance of backup tapes do not exist. Specifically, the following weaknesses were noted:
    - ETA does not maintain inventory records of magnetic tapes stored off-site.
    - The UIS backup tapes (stored in containers) and the keys to the containers are not adequately secured. For approximately one week, the UIS backup tapes were not adequately safeguarded while awaiting pickup from courier. UIS backup tapes are stored in locked off-site storage containers in the Network Administrator's cubicle, however the keys for the containers are located on a shelf in an opened, unlocked overhead cabinet.
    - UIS does not store the annual and quarterly backup tapes off-site.
- A copy of the UIS Disaster Recovery Plan (1/99) is not stored at the off-site facility.

We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook by ensuring each agency develops the required contingency plan. In addition, agencies should ensure that: arrangements have been made for an alternate processing facility; plans are stored at the off-site storage facility; plans include sufficient guidelines for developing roles, responsibilities and recovery instructions, training primary and back-up personnel, and frequency of updates, etc.***

During our FY 2000 audit, we found ETA management has started corrective actions. UIS backup procedures have been updated. The inventory records and safeguarding the UIS backup

tapes are still in progress. In addition, management represented that a copy of the UIS "Disaster Recovery Plan" and the "UIS Security Plan" has been sent to the off-site storage facility. This recommendation is **resolved and open**. Closure is dependent on the OIG review of the corrective actions in our FY 2001 audit.

Management's Response:

ETA has completed the corrective action to address the findings. These policies and procedures will be added to the updated SSP to be completed in April, 2001.

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the updated SSP and the corrective actions taken during our FY 2001 audit.

Personnel Controls

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found ETA management information security controls related to personnel policies and procedures are inadequate. We found the following security-related personnel policies have not been adequately implemented:

- Background checks and references have not been made on new hires for the period covering October 1, 1998 to September 30, 1999.
- There is no formal policy for reinvestigating "Non-critical Sensitive" positions.
- Current information on employee training and professional development is not adequately documented and monitored.

We made the following recommendations to the Chief Information Officer and the Assistant Secretaries:

- ***ensure that a background check should be conducted for all Government employees and contractor management personnel with high levels of system access, and***
- ***ensure that employees are required to attend training and maintain the appropriate documentation (e.g., lists of employees as of the training course date, attendance sheet of employees taking the course, topics, agendas, handouts, etc., provided during the program).***

During our FY 2000 audit, we found ETA/OTIS management in the process of discussing audit issues with Human Resource to determine the appropriate course of action. These recommendations are **resolved and open**. Closure is dependent upon the OIG review of the updated procedures in our FY 2001 audit.

Management's Response:

ETA is currently working with OHR on developing a proper personnel background check and reinvestigation policy and procedure. These policies and procedures will be included in the updated SSP due in April, 2001.

OIG's Conclusion:

These recommendations remain **resolved and open** pending our review of the updated SSP and the corrective actions taken during our FY 2001 audit.

Authorization and Monitoring of Logical Access

During our FY 1999 audit (OIG Report No. 12-00-003-13-001), we found controls over the authorizing and periodic monitoring of users having logical access to ETA's Unemployment Insurance Service systems are inadequate. We found that formal policies exist and procedures do exist for the authorization, modification, deletion/termination, periodic recertification of user access and assignment of access via dial in methods. However, the following weaknesses were identified:

- The National office on a monthly basis monitors UIS system access, however, the user management is not involved in the recertification of access approval process. Authorized users are identified on a user access list. But it is not distributed to the appropriate regional managers for recertification approval. Three National Office management personnel review the access control listing and approves removal of a UIS account. However, the deleted account is not documented.

- *User Account Request Form (ETA PC LAN & UI UNIX Network)* tested had the following weaknesses:
  - There is no authorization date and creation date of access.
  - The Requestor is recorded but not the authorizing agent's approval/signature.
  - Instructions for filling out the form do not exist.
  - New division names are not recorded on form.
  - Information that is inappropriate to fill out, did not indicate "inapplicable."
  - Required information was missing or incomplete on 9 of 21 forms examined.

We made the following recommendation to the Chief Information Officer and the Assistant Secretaries:

- ***ensure agencies are in compliance with the computer security handbook and that the agency SSPs (for its GSS and MAs) contain sufficient policies and procedures governing the authorization, modification, removal, monitoring of access based upon the concept of "least privileged," and the emergency access. A recertification should***

be conducted of all IDS on the system and the business need documented. In addition, IDS that have been granted access to production programs and data (outside of the application) should be restricted from this level of access.

During our FY 2000 review, we found UIS was updating procedures to include all Regional Managers in the creation, deletions, and recertification of regional user Unix accounts. The Regional manager will be notified (via e-mail) whenever a change to a regional account is requested. Hard copies will be kept on file. A new User Account Request Form is being created. This recommendation is **resolved and open**. Closure is dependent upon the OIG review of the updated procedures in our FY 2001 audit.

Management's Response:

1. Procedures have been updated to communicate changes to the status of UNIX accounts of Regional users to Management. *Provided to the OIG with Response to Draft Report.*

2. OWS has created a new user account request form which has been in use since November, 2000. *Provided to the OIG with Response to Draft Report.*

OIG's Conclusion:

This recommendation remains **resolved and open** pending our review of the documentation provided during our FY 2001 audit.