

Office of Inspector General

U.S. Department of Labor
Office of Information Technology Audits

GISRA Evaluation and Security Test and Evaluation

Occupational Safety and Health Administration

FINAL REPORT

This review was performed by Pricewaterhouse Coopers LLP under contract to the Office of Inspector General, and, by acceptance, it becomes a report of the Office of Inspector General.

/s/

Assistant Inspector General for Audit

Report Number: 23-01-006-10-001

Date Issued: 9-24-01

TABLE OF CONTENTS

| | |
|--|-----------|
| EXECUTIVE SUMMARY..... | 1 |
| OVERVIEW OF SYSTEMS | 1 |
| DESCRIPTION OF EVALUATIONS..... | 2 |
| EVALUATION SUMMARY | 3 |
| MANAGEMENT COMMENTS | 4 |
| CONCLUSION..... | 5 |
| FINDINGS AND RECOMMENDATIONS..... | 6 |
| RISK MANAGEMENT | 6 |
| REVIEW OF SECURITY CONTROLS..... | 8 |
| LIFE CYCLE | 10 |
| AUTHORIZE PROCESSING-CERTIFICATION & ACCREDITATION | 12 |
| SYSTEM SECURITY PLAN | 14 |
| PERSONNEL SECURITY..... | 16 |
| PHYSICAL AND ENVIRONMENTAL PROTECTION..... | 18 |
| PRODUCTION, INPUT/OUTPUT CONTROLS..... | 21 |
| CONTINGENCY PLANNING | 23 |
| HARDWARE AND SYSTEM SOFTWARE MAINTENANCE..... | 26 |
| DATA INTEGRITY | 29 |
| DOCUMENTATION..... | 31 |
| SECURITY AWARENESS, TRAINING AND EDUCATION | 33 |
| INCIDENT RESPONSE CAPABILITY..... | 34 |
| IDENTIFICATION AND AUTHENTICATION..... | 36 |
| LOGICAL ACCESS CONTROLS..... | 39 |
| AUDIT TRAILS..... | 42 |
| ACRONYMS..... | 45 |
| APPENDIX A - Management Response to Draft Report..... | 46 |

EXECUTIVE SUMMARY

The Department of Labor (DOL) and Occupational Safety and Health Administration (OSHA) have developed and implemented many information security-related policies and procedures. However, OSHA needs to continue to strengthen its information security program. In particular, OSHA management needs to focus its attention and resources on implementing controls related to the following high priority areas: Risk Management; System Security Plan (SSP); Certification and Accreditation of Systems; Incident Response Capability; Identification and Authentication; Logical Access; and Audit Trails.

The FY 2001 Defense Authorization Act, Section X, Subtitle G, contains the Government Information Security Reform Act (GISRA), which requires the Inspector General (IG) or the independent evaluator, as determined by the IG, to evaluate the Department of Labor's (DOL) mission-critical systems. In addition to the above requirement, the Office of the Inspector General (OIG) is required to conduct cyber security testing and evaluation (ST&E) in support of *Presidential Decision Directive (PDD) 63* and in accordance with DOL's *Cyber Security Program Plan*. During the period of June through August 2001, PricewaterhouseCoopers (PwC) performed an evaluation of the implementation of the GISRA requirements by OSHA and an ST&E of OSHA's general support system to determine how well the system security access controls enforce the agency's policy.

Implementation of security requirements were verified and validated against the National Institute of Standards and Technology's (NIST) *Self-Assessment Guide for Information Technology Systems* (Self-Assessment Guide), which encompasses requirements of GISRA, Office of Management and Budget (OMB) Circular A-130, General Accounting Office (GAO) Federal Information Systems Controls Audit Manual (FISCAM), NIST Publications, and other Federal guidance.

An overview of the systems included in the GISRA evaluation and ST&E, our scope and methodology, and the summary results of our evaluations are described in the following sections of the report. The details of our findings are included in the "Findings and Recommendations" section of this report.

OVERVIEW OF SYSTEMS

The GISRA evaluation encompassed two OSHA mission-critical applications--Integrated Management Information System (IMIS) and Compliance Safety and Health Officer Health Information System (CHIS).

IMIS was created to satisfy the automated data processing requirements of OSHA. OSHA relies on the system to plan, manage, track and report on its enforcement, consultation and discrimination programs. The information is also used in rulemaking and compliance assistance programs. The system primarily collects and manages information on workplace safety and health inspections and also includes information on complaints, accident reports referrals, 11(c) discrimination cases, health sampling, and consultant visits. The IMIS includes more than 2.5 million records from 1972 to present.

CHIS is a small local area network (LAN) used to record, store, track, and make available, a limited amount of administrative, financial, and medical data pertinent to agency personnel who participate in OSHA's Medical Examination Program. OSHA uses this information in its assessment of available manpower to perform field duties. CHIS is limited to five authorized operators.

The ST&E was performed on OSHA's OSHANET general support system (GSS). OSHA's GSS, housed in Washington DC, is a LAN providing office automation capabilities for the OSHA's National Office. It also serves as a nationwide network supporting data communications and office automation capabilities for OSHA offices located throughout the U.S. Its data communications allow OSHA users to

maintain and use their e-mail and Internet/Intranet services. In addition, it allows OSHA users to access and use applications and other services (such as IMIS, Travel Manager, and home directories) on the GSS.

DESCRIPTION OF EVALUATIONS

Scope

The PwC team evaluated whether DOL and/or OSHA had promulgated policies and procedures that covered the GISRA requirements, as defined in the NIST Self-Assessment Guide. In addition, the team assessed the implementation of GISRA requirements for two OSHA major applications¹--IMIS and CHIS. The evaluation of the implementation of GISRA requirements was assessed against the 212 questions listed under the following 17 control objectives in the NIST Self-Assessment Guide:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification & Accreditation)
- System Security Plan
- Personnel Security
- Physical and Environment Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

The PwC team also conducted an ST&E of OSHA's GSS through penetration testing to determine how well the system security access controls enforce the agency's policy. The objective of the ST&E was to assess the technical implementation of the security design and to ascertain that security software, hardware, and firmware features affecting confidentiality, integrity, availability, and accountability have been implemented as required by the technical control objectives (i.e., Identification and Authentication, Logical Access Controls, and Audit Trails) in the NIST Self-Assessment Guide.

Methodology

Security requirements were reviewed and tested based on the NIST Self-Assessment Guide, as agreed to by DOL management, the OIG, and the PwC team. The PwC used an audit program, based on NIST Self-Assessment Guide, to complete the following three phases:

¹ OMB Circular A-130 defines a major information system (i.e., major application) as an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Phase I: Planning

- Conduct entrance meetings with OIG officials, the DOL Chief Information Officer (CIO), and selected OSHA management officials
- Develop request lists of information required to complete project
- Develop proforma data collection instruments for agency staff interviews and other data collection needs
- Develop detailed work program to identify specific steps to complete the GISRA review and evaluations

Phase II: Verification and Testing

- Review and analyze documentation
- Conduct interviews
- Perform internal and external penetration testing to:
 - Determine if security defenses sufficiently protected the network
 - Identify network topology/vulnerabilities
 - Use the topology and system vulnerabilities to determine if unauthorized access to internal network is possible
 - Demonstrate identified vulnerabilities
- Document GISRA evaluation and ST&E results
- Prepare work-papers and perform supervisory review

Phase III: Reporting

- Conduct meetings with appropriate staff regarding tentative findings
- Complete Tentative Findings Report--Combine GISRA evaluation and ST&E findings
- Perform supervisory review
- Respond to OIG review
- Hold meeting with agency management to discuss the results and recommendations for corrective action.
- Respond to agency review
- Revise Tentative Finding Report and issue Draft Report
- Hold closing meeting with OIG to deliver Final Report

EVALUATION SUMMARY

We found that overall the Department and OSHA have promulgated policies and some procedures covering all of the 17 control objectives. However, additional procedures are needed for the following 12 control objectives:

- Review of Security Controls
- System Security Plan
- Personnel Security
- Physical Security and Environmental Controls
- Production, Input/Output Controls
- Hardware/System Software Maintenance
- Data Integrity
- Documentation
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

We also reviewed OSHA's implementation of the 17 control objectives in the NIST Self-Assessment Guide. While OSHA has implemented many of the requirements under the control objectives, there are still requirements that have not been implemented for each of the 17 control objectives.

While all areas are considered important, the table below identifies the control objectives we considered high and medium priority based. For purposes of assessing priorities for each control objective, we used the following criteria:

High Priority: Control objectives that are characterized by the following: (1) inherently high risk; (2) DOL or agency procedures are limited; or (3) implementation of the procedures is limited.

Medium Priority: Control objectives that are still important, but do not meet any of the above criteria.

| Control Objective Category | High Priority | Medium Priority |
|--|---------------|-----------------|
| Management Controls | | |
| Risk Management | | X |
| Review of Security Controls | | X |
| Life Cycle | | X |
| Authorize Processing (Certification and Accreditation) | X | |
| System Security Plan | | X |
| Operational Controls | | |
| Personnel Security | | X |
| Physical and Environmental Protection | | X |
| Production, Input/Output Controls | | X |
| Contingency Planning | X | |
| Hardware and System Software Maintenance | | X |
| Data Integrity | | X |
| Documentation | X | |
| Security Awareness, Training and Education | | X |
| Incident Response Capability | X | |
| Technical Controls | | |
| Identification and Authentication | X | |
| Logical Access Controls | X | |
| Audit Trails | X | |
| Total | 7 | 10 |

MANAGEMENT COMMENTS

In response to our draft report, OSHA recommended changes to some of the wording in the report and posed a number of questions related to our assessment of the DOL policies and procedures. However, OSHA did not provide any additional comments. OSHA's comments are summarized under the "Management Comments" section for each finding. OSHA's complete response is included in its entirety as an appendix to this report.

CONCLUSION

We made the recommended changes and responded to the OSHA's questions. However, OSHA did not provide action plans or target dates to address the intent of the recommendations to any of the 17 findings. We provided comments and conclusions under the "Conclusion" section for each of the findings.

FINDINGS AND RECOMMENDATIONS

| | |
|---|---|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.1)</p> <p>Risk Management</p> | <p>Condition: The CIO’s Computer Security Handbook (CSH) provides the risk management policies and procedures to be followed by the DOL agencies.</p> <p>We confirmed that OSHA’s risk assessments for CHIS and IMIS substantially complied with the CSH. Both risk assessments were completed on November 28, 2000. IMIS does not process classified information but does handle what is considered agency sensitive information and contains Privacy Act data.</p> <p>However, OSHA has not fully implemented the risk management process as required by the CSH. In particular, OSHA has not:</p> <ul style="list-style-type: none"> • Conducted final risk determinations and related management approvals are not documented and maintained on file. • Conducted a mission/business impact analysis subsequent to the recent risk assessment process. <p>Cause: Prior to 2000, risk assessments were handled locally without a prescribed methodology, tool, or agency-required documentation requirements. While OSHA has taken significant actions to implement the risk management requirements, it has not prepared a detailed plan of action to identify and prioritize the specific steps of implementation of the selected safeguards which could reduce or eliminate the vulnerability of the systems to the threats.</p> <p>Criteria: The FY 2001 Defense Authorization Act, Section X, Subtitle G, <i>Government Information Security Reform Act (GISRA)</i> states that the head of each agency shall ensure that the agency’s security plan is practiced throughout the life cycle of each agency system.</p> <p>OMB Circular A-130 states that agencies shall establish information system management oversight mechanisms that ensure major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources.</p> <p>FISCAM CC-1: states that agencies should have a documented SDLC methodology that details the procedures that are to be followed when applications are being designed and developed, as well as when they are subsequently modified. It further states that policies and procedures should be in place that detail who can authorize a modifications and these authorizations are to be documented.</p> <p>NIST 800-18: <i>Guide for Developing Security Plans for Information Technology Systems</i>, states that an organization should be able to respond quickly when faced with an incident. Specifically, the publication states “Although a computer security plan can be developed for a system at any point in the life</p> |
|---|---|

| | |
|--|---|
| | <p>cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle.”</p> <p>NIST 800-27: <i>Engineering Principles for Information Technology Security</i> (A Baseline for Achieving Security), this recently released publication (June 2001) presents security principles and their relationship/applicability to each phase of life cycle development.</p> <p>NIST 800-30: <i>Risk Management Guide (Draft)</i> states that all security-related activities are a part of the risk management process and that risk management spans the entire system development life cycle (SDLC).</p> <p>The CSH requires OSHA to update the SSP as the system progresses throughout its life cycle.</p> <p>Effect: The absence of a current and clear understanding by program officials of the vulnerabilities of its systems limits the ability of OSHA to make timely decisions to mitigate risks to the OSHA mission and ability to carry on its normal business operations. Thus, effective security controls needed to ensure that the information in OSHA's systems is adequately protected and can be relied upon for decision-making may not be implemented</p> <p>Recommendation: We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet risk management requirements.</p> <p>Management Comments: OSHA recommended some minor changes to the Condition paragraph. No other comments were provided.</p> <p>Conclusion: We made the recommended changes. However, OSHA did not provide action plans or target dates to address the intent of the recommendation.</p> |
|--|---|

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.1.2)**

**Review of Security
Controls**

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) provides policy guidance to the DOL agencies regarding conducting periodic reviews of security controls. However, the following procedures are not specifically addressed in the DOL or OSHA guidance documents:

- Review the operating system periodically to ensure the configuration prevents circumvention of the security software and application controls.
- Routinely conduct tests and examinations of key controls (i.e., network scans, analyses of router and switch setting, penetration testing).

Independent reviews were recently conducted by external contractors Troy Systems and SeNet International. Self-assessments were conducted by OSHA. In addition, OSHA has analyzed security alerts/incidents and ensured that corrective actions have been effectively implemented. However, OSHA has not implemented the following requirements:

- Periodic reviews of its systems.
- Perform periodic reviews of its operating system to ensure the configuration prevents circumvention of the security software and application controls.
- Perform routine tests and exams of key controls (i.e., network scans, router and switch setting analysis, penetration testing).

Cause:

Until 2000, security reviews were handled locally, without a prescribed methodology, schedule, or agency-wide documentation requirements. However, OSHA has made progress in implementing the requirements related to this area. OSHA has been adhering to guidance as it published and recently updated its SSPs previously prepared under the NIST guidance in 1998. OSHA's Security Program Plan dated July 27, 2001, states that it will develop procedures for review of security controls process. However, OSHA has not developed an action plan, assigned resources, or established a schedule to develop and implement procedures to fully meet all security review control requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act (GISRA)*, requires that the head of each agency ensure periodic testing and evaluating of information security controls and techniques and implement appropriate remedial actions based on the evaluation. In addition, GISRA requires that each agency shall have an annual independent evaluation of the information security program and practices of that agency.

OMB Circular A-130 requires that agencies perform an independent review or audit of the security controls in each application at least every three years or sooner, if significant modification have occurred or where the risk and magnitude of harm are high.

FISCAM SP-5.1 states that "...Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan..."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that "...Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software "patches"), and penetration testing can assist in the ongoing review of system security measures. These tools, however, are no substitute for a formal management review at least every three years..."

The CSH states that "...An independent review of security controls for each Major Application System should be performed at least every three years ... the results of the review conducted should be analyzed. Include specifics on who conducted the review. If any recommendation or findings were made as a result of the review, the outcome should be addressed..."

Effect:

Without established written procedures, it is difficult to ensure that periodic reviews of OSHA's applications will be performed on a continuous basis, which may leave OSHA's sensitive applications vulnerable to misuse, unauthorized access, and unauthorized modifications.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet security review control requirements.

Management Comments:

OSHA recommended some minor changes to the Cause section. No other comments were provided.

Conclusion:

We made the recommended changes. However, OSHA did not provide action plans or target dates to address the intent of the recommendation.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.1.3)**

Life Cycle

Condition:

The U. S. Department of Labor (DOL) *Systems Development and Life Cycle Management Manual* (SDLCM) provides the life cycle policies and procedures to be followed by all DOL agencies.

We reviewed the implementation of life cycle requirements for IMIS and CHIS. However, IMIS was developed in the 1970's and CHIS was developed in the mid-1990's. As such system documentation is unavailable and we are unable to assess OSHA's compliance with life cycle requirements in the initiation, development, and implementation phases. Thus, for implementation the scope of our review was limited to the operations/maintenance phase. During this phase the following requirement was not met:

- Purging, overwriting, degaussing, or destroying of information or media when no longer needed.

Cause:

Since the implementation of the CHIS system, OSHA has experienced frequent personnel and contractor turnover. Original life cycle documents have been either lost or misplaced through the handling by multiple parties. During the redesign of IMIS over the next several years, OSHA plans to follow policies and procedures set forth by the SDLCM. The IMIS redesign is currently in the design phase of the SDLCM.

However, OSHA has not developed action plans or assigned the appropriate resources for the review and update of SSPs of IMIS and CHIS.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act* (GISRA) states that the head of each agency shall ensure that the agency's security plan is practiced throughout the life cycle of each agency system.

OMB Circular A-130 states that agencies shall establish information system management oversight mechanisms that ensure major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources.

NIST 800-27, *Engineering Principles for Information Technology Security*--this recently released publication (June 2001) presents security principles and their relationship/applicability to each phase of life cycle development.

NIST 800-30, *Risk Management Guide (Draft)*, states that all security-related activities are a part of the risk management process and that risk management spans the entire system development life cycle (SDLC).

The CSH requires all DOL agencies to update the SSP as the system progresses throughout its life cycle.

Effect:

Without adequate and proper life cycle documentation, OSHA is susceptible to inadequately funding security resources on a project or system. Without the

proper funding, projects may be more vulnerable to security threats because proper security objectives were never developed and implemented. In the absence of a life cycle procedural documentation, OSHA can not be assured that information security objectives are practiced throughout the final stages of the systems' life.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement actions plans to review and update SSPs for IMIS and CHIS and meet all appropriate life cycle phases requirements for those systems

Management Comments:

OSHA recommended some minor changes to the Condition and Cause sections. No other comments were provided.

Conclusion:

We made the recommended changes. However, OSHA did not provide action plans or target dates to address the intent of the recommendation.

| | |
|---|---|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.1.4)</p> | <p>Condition: The CSH and the DOL Management Series 9 (DLMS-9)--<i>Information Technology</i> provide policy and some procedural guidance to the DOL agencies regarding authorize processing--certification and accreditation requirements. The DLMS-9 was in the clearance process during this review.</p> <p>IMIS has an interim authority to operate and has met all requirements that serve as a basis for certification and accreditation, except for implementing signed Rules of Behavior. While OSHA developed Rules of Behavior, they have not been signed off by users.</p> <p>CHIS has not been certified or accredited and does not have an interim authority to operate. OSHA has developed a security plan and risk assessment (i.e., requirements for certification and accreditation) for CHIS. However, it has not implemented the following requirements that support the certification and accreditation process:</p> <ul style="list-style-type: none"> • Established Rules of Behavior that are signed by users. • Developed and tested a contingency plan. • Determined that in-place safeguards are operating as intended. • Initiated prompt action to correct deficiencies. <p>Cause: OSHA will be a full OSHA officials have held discussions with the DOL Office of the Chief Information Officer with respect to certification and accreditation of both IMIS and CHIS and have focused on the recent certification and accreditation of IMIS. OSHA expects to implement the required procedures and obtain certification and accreditation of CHIS in the near future. In addition, OSHA officials plan to incorporate employee sign-off in the security awareness training planned for September 2001. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement authorize processing--certification and accreditation requirements.</p> <p>Criteria: OMB Circular A-130 requires that "...A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk or magnitude of harm is high..."</p> <p>NIST Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology Systems</i>, states "...Management authorization must be based on an assessment of management, operational and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by technical evaluation and/or for security evaluation, risk assessment, contingency plan, and signed rules of behavior...Reauthorization should occur prior to a significant change in the system, but at least every three years..."</p> <p>The NIST FIPS PUB 102, <i>Guideline for Computer Security Certification and Accreditation</i>, explains that the certification process is a technical process that produces a judgment, statement of opinion, and complements the accreditation process. Accreditation [FIPS 39] is the authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment,</p> |
|---|---|

and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. Accreditation is the official management authorization for operation.

DLMS-9 states that agency heads "...are responsible for...issuing Interim Approval to Operate (IATO) under specified conditions to information systems that need to connect to an operational system(s) before full authorization is possible. This may be done in coordination with the CIO on a temporary basis as a facilitating measure to attain full authorization...The IATO may be granted for no more than a one-year period..."

The CSH requires that the Rules of Behavior (ROB) "...should clearly delineate responsibilities and expected behavior of all individuals with access to the General Support System or major application, and must define the consequences of behavior not consistent with the ROB...It is recommended that the rules contain a signature page for each user to acknowledge receipt..."

Effect:

Without proper certification and accreditation of OSHA's major applications, management cannot be assured that security controls have been designed into its systems as planned, which may leave sensitive data vulnerable to unauthorized access and use.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet authorize processing--certification and accreditation requirements for IMIS and CHIS.

Management Comments:

Currently, there is no formal DOL certification and accreditation process in place. However, a DOL security workgroup has been formed to address this control objective. OSHA will be a full participant on this workgroup.

Conclusion:

The actions planned by OSHA are partially responsive to the issues identified. However, OSHA did not provide action plans or target dates to address all of the requirements identified in the Condition section of this finding.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.1.5)**

System Security Plan

Condition:

The CSH and the CSPP provide policy and some procedural guidance to the DOL agencies regarding the development of SSPs. However, the following procedures are not addressed in the above DOL documents:

- SSPs should be approved by key affected parties and management.
- The summary of the plans should be incorporated into the strategic IRM plan.
- The plan should be reviewed periodically and adjusted to reflect current conditions and risks.

In addition OSHA has implemented all SSP requirements for IMIS and CHIS, except a summary of the security plan in the strategic IRM plan.

Cause:

OSHA has been following OCIO guidance regarding SSP development and recently issued a new OSHA SPP that states OSHA will develop procedures in this area as required. In addition, system re-design work is about to be conducted on both major applications, which will require amendments to their original security program plans to bring them into them into full compliance with SSP requirements. However, OSHA has not developed action plans or assigned the appropriate resources to fully implement SSP requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states "...Each agency shall develop and implement an agency-wide information security program to provide information security for the operations and assets of the agency, including operations and assets provided and managed by another agency..."

OMB Circular A-130 requires Federal agencies to "...Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include: Application Rules, Specialized Training, Personnel Security, Contingency Planning, Technical Controls, Information Sharing, and Public Access Controls..."

OMB Bulletin 90-08 states that "...The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system..."

FISCAM SP-2 states that (1) "...Entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities...", (2) to help ensure that the plan is complete and supported by the entity as a whole, senior management should obtain agreement from all affected parties in establishing policies for a security program, (3) "...To be effective, the policies and plan should be maintained to reflect current conditions...Outdated policies and plans not only

reflect a lack of top management concern, but also may not address current risks, and, therefore, may be ineffective...”

NIST 800-14, *Principles and Practices for Securing Information Technology (IT) Systems*, states that “...A security plan should be used to ensure that security is considered during all phases of the IT system life cycle...”

NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that all applications and systems must be covered by SSPs if they are categorized as a “major application” or “general support” system.

The CSH states that “...One aspect of managing an IT system is the development of a System Security Plan (SSP), which is documentation of the protection afforded the system by technical, managerial, and operational means. In addition, it states that, “...A SSP is a living, dynamic document reflecting the current security posture of the IT system. The SSP should be developed during the initial phases of system development and acquisition...The SSP should also be updated on the basis of the subsequent mitigation activity or plan, after a significant system configuration change, or every three years. When the system is decommissioned, the SSP should be updated and stored with system records...”

The CSPP states that all Federal IT systems have some degree of sensitivity and are required to have a SSP and that all DOL systems will have current and effective SSP.

Effect:

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. Also, by not incorporating the summary of SSP into the strategic IRM plan, increases the risk that information management activities may not be carried out in the most efficient, effective, and economical manner.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet SSP requirements for IMIS and CHIS.

Management Comments:

OSHA pointed out an inconsistency with a previous finding. No other comments were provided.

Conclusion:

We made the correction to the previous finding. However, OSHA did not provide action plans or target dates to address the intent of the recommendation.

| | |
|--|---|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.1)</p> <p>Personnel Security</p> | <p>Condition: The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) provides policy and some procedural guidance to the DOL agencies regarding personnel security. However, the CSH and OSHA procedures do not specifically require:</p> <ul style="list-style-type: none"> • Documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties. • Distinct systems support functions performed by different individuals. • Regularly scheduled vacations and periodic job/shift rotations. • Specific personnel security procedures for hiring and transfer of personnel. <p>Furthermore, for IMIS and CHIS, OSHA does not:</p> <ul style="list-style-type: none"> • Segregate duties based on job descriptions and responsibilities. • Regularly schedule vacations or periodic job/shift rotations. • Complete appropriate background screening for assigned positions prior to granting access. <p>Cause: While OSHA has performed screening of individuals based on the sensitivity of the position (especially those individuals involved with CHIS), it had in the past decided not to do so where the risk involved did not justify screening costs of trusted employees. OSHA is currently committed to complying with recent OCIO requirements to meet OPM policies regarding personnel security and is in the process of implementing procedures in this area. However, OSHA has not developed action plans or assigned the appropriate resources to fully implement personnel security requirements.</p> <p>Criteria: OMB Circular A-130 requires screening of personnel who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.</p> <p>FISCAM SD-1 states that management should document job descriptions that clearly describe employee duties and prohibited activities.</p> <p>FISCAM SD-1.1 requires that incompatible duties be identified and policies implemented to segregate these duties.</p> <p>FISCAM SD-4.1 states "...The security plan should include policies related to the security aspects of hiring, terminating, and transferring employees and assessing their job performance..."</p> <p>FISCAM SP-1.2 states that "...Documented job descriptions should exist that clearly describe employee duties and prohibited activities..."</p> <p>FISCAM SP-4 states that management should include policies related to the security aspects of hiring, terminating and transferring employees and assessing their job performance.</p> |
|--|---|

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that (1) all positions should be reviewed for sensitivity level, and (2) user access be restricted (least privilege) to data files, to processing capability, or to peripherals and type of access to the minimum necessary to perform the job.

Effect:

Without development and implementation of adequate personnel screening requirements, OSHA is exposed to the risk of improper and unauthorized access to its sensitive applications. Improper system access could compromise the efficient working of the systems by misuse, unauthorized modification, viewing of sensitive information, and system disruption.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet personnel security requirements.

Management Comments:

No comments were provided.

Conclusion:

OSHA did not provide action plans or target dates to address the intent of the recommendation.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.2.2)**

**Physical and
Environmental
Protection**

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) provides policy and some procedural guidance to the DOL agencies regarding physical and environment protection. However, the CSH and OSHA procedures do not include the following requirements:

- Secure unused keys.
- Authenticate visitors, contractors and maintenance personnel through the use of preplanned appointments and identification checks.
- Emergency exit and re-entry of personnel after fire drills.
- Change computer room entry codes periodically.
- Sign-in and escort visitors into sensitive areas.
- Investigate and take remedial action for suspicious access activity.
- Review fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson periodically
- Install redundant air-cooling system.
- Periodically review electronic power distribution, heating plants, water, sewage, and other utilities for risk of failure.
- Provide an uninterruptible power supply or back up generator.
- Encrypt data files on laptops.
- Store laptops and other portable systems securely.
- Protect system from plumbing lines.
- Limit viewing of computer monitors by unauthorized personnel.
- Control physical access to data transmission lines.

Despite the limited procedures, OSHA has implemented many physical and environment protection controls, such as physical access controls and fire safety measures. However, based on our interviews, review of documentation, and our observations at the OSHA Headquarters Network (GSS) Operations Center, we found the following deficiencies.

- The possibility exists for unauthorized physical access to data transmission lines through phone/data line closets through access to keys to other DOL agency closets, which can also open the phone closets.
- While contractor maintenance is monitored, the contractors are not escorted to the closets.
- Unauthorized persons can gain access to view computer monitors and potentially sensitive information.
- An unprotected door to the IMIS network operations center was identified.

In addition, OSHA has recently undergone contractor transition with respect to CHIS and the physical protection of daily operations of this system could be compromised.

Cause:

OSHA operates in facilities that are controlled by DOL and is limited in its ability to develop and implement procedures over the physical environment. OSHA will continue to try to obtain more detailed information from DOL and the General Services Administration about the physical environment and planned and in place controls.

Criteria:

FISCAM AC-3 requires agencies to establish physical and logical access controls to prevent or detect unauthorized access.

FISCAM AC-3.1 requires "...Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment..."

FISCAM SC-2.2 details the policies and procedures that should be in place to prevent potential damage to facilities and interruptions in service and states that "...Environmental controls prevent or mitigate potential damage to facilities and interruptions in service.... Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages..."

FISCAM AC-4 requires agencies to monitor access, investigate apparent security violations, and take appropriate remedial action details the policies and procedures that should be in place in order to maintain critical audit trails and report unauthorized or unusual activity.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, discusses the physical and environmental security controls that "...are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical environmental security program should address the following seven topics--Physical Access Controls, Fire Safety Factors, Failure of Supporting Utilities, Structural Collapse, Plumbing Leaks, Interception of Data, Mobile and Portable Systems. In doing so, it can help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft..."

DOL Management Series 9, *Information Technology*, requires agencies to develop procedures ensuring adequate physical security of network assets.

Department of Labor *Security Program Plan Instructions* state that "...Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation..."

The CSH requires physical and environmental security controls to be implemented to protect the facility housing system resources, the system resources themselves and the facilities used to support the operation.

Effect:

The lack of clearly defined policy and procedures in place for physical and environment protection controls exposes OSHA to interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

Recommendation:

We recommend that OSHA, working in concert with DOL, assign appropriate resources and develop and implement action plans to fully meet physical and environmental control requirements.

Management Comments:

OSHA recommended some minor changes to the Cause section. No other comments were provided.

Conclusion:

We made the recommended changes. However, OSHA did not provide action plans or target dates to address the intent of the recommendation.

| | |
|---|--|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.3)</p> | <p>Condition: DOL and OSHA have policies and most procedures covering production, input/output control requirements. However, there are no procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.</p> |
| <p>Production, Input/Output Controls</p> | <p>In addition, we found that OSHA has implemented some production, input/output controls. However, it has not implemented the following controls:</p> <ul style="list-style-type: none"> • Ensuring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information. • Ensuring that only authorized users pick up, receive, or deliver input and output information and media. • Transporting or mailing media or printing. • Internal/external labeling for sensitivity. • External labeling with special handling instructions. • Audit trails for inventory management. • Physical protection of media storage vault/library. • Sanitizing media for reuse. <p>Cause: In the past, OSHA did not implement more stringent input/output controls, because most data was not considered to be sensitive. More recently, OSHA has developed procedures for input/output controls and is in the process of implementing these procedures. While OSHA is making progress, it has not assigned resources or developed action plans to issue procedures and fully implement requirements related to production, input/output controls.</p> <p>Criteria: NIST Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology System</i>, specifically require agencies to develop and implement the following procedures:</p> <ul style="list-style-type: none"> • Ensuring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information. • Ensuring that only authorized users pick up, receive, or deliver input and output information and media. • Transporting or mailing media or printing. • Internal/external labeling for sensitivity. • External labeling with special handling instructions. • Audit trails for inventory management. • Physical protection of media storage vault/library. • Sanitizing media for reuse. <p>The CSH requires that production, input/output controls include measures used to protect information that is input into the system (such as raw data), information that is processed by the system, and the information that is result of processing by the system, such as a report. Examples of controls would be marking, storing, and transmitting sensitive documents; procedures for sanitizing electronic media for reuse or prior to maintenance or repair; and Installing and updating software to preclude unintentionally degrading system operation or corruption of data.</p> |

| | |
|--|--|
| | <p>Effect: Without the development and implementation of clearly defined policy and procedures related to production, input/output controls, OSHA runs the risk of loss of input/output information and media and possibly exposing sensitive information to unauthorized users.</p> <p>Recommendation: We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet production, input/output control requirements.</p> <p>Management Comments: OSHA recommended one minor editorial change. No other comments were provided.</p> <p>Conclusion: We made the recommended change. However, OSHA did not provide action plans or target dates to address the intent of the recommendation.</p> |
|--|--|

| | |
|---|--|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.4)</p> | <p>Condition: The CSH and the CSPP provide policy and procedural guidance to the DOL agencies regarding contingency planning.</p> <p>However, CHIS has no contingency plan and no contingency planning procedures have been implemented for CHIS. In addition, OSHA has not periodically tested and readjusted the IMIS contingency plan, as appropriate.</p> <p>Cause: OSHA has not assigned resources or developed action plans to fully implement contingency planning requirements for IMIS or CHIS.</p> <p>Criteria: OMB Circular A-130 states that with regards to contingency planning, agencies should "...establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support...Experience has demonstrated that testing a contingency plan significantly improves its viability..."</p> <p>NIST Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology Systems</i>, "...requires that the agency have procedures the will permit a continuation of essential functions if information technology support is interrupted...The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated...General support systems require appropriate emergency, backup and contingency plans...These plans should be tested regularly to assure the continuity of support...Also, these plans should be known to users and coordinated with their plans for applications..."</p> <p>NIST 800-14, <i>Generally Accepted Principles and Practices for Securing Information Technology Systems</i>, states that "...an organization should test and revise the contingency plan. A contingency plan should be tested periodically..." It also indicates the functional steps that an organization should employ when preparing for contingencies and disasters. These steps are (1) develop a business plan, (2) identify resources (3) develop scenarios, (4) develop strategies, and (5) test and revise the plan.</p> <p>FISCAM, SC-1.3 states that "...In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed..."</p> <p>FISCAM, SC-2.1 states that "...Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions..."</p> <p>FISCAM, SC-3.1 states that "...Contingency plans should be documented, agreed on by both user and data processing departments, and communicated to affected staff...Staff should be trained in and aware of their responsibilities in preventing mitigating and responding to emergency situations...Training sessions should be held at least once a year and whenever changes to emergency plans are made...[The plan] should identify and provide information on:</p> <ul style="list-style-type: none"> • Supporting resources that will be needed, |
| <p>Contingency Planning</p> | |

- Roles and responsibilities of those who will be involved in recovery activities,
- Arrangements for off-site disaster recovery location and travel and lodging for necessary personnel, if needed,
- Off-site storage location for backup files, and
- Procedures for restoring critical applications and their order in the restoration process.” “Multiple copies of the contingency plan should be available with some stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable...”

Department of Labor Management Series 9, *Information Technology*, requires that a contingency plan/disaster recovery plan for all information systems within a DOL agency must be completed prior to approval of SSPs.

Effect:

Without adequate contingency planning, OSHA is susceptible to operational difficulties related to unexpected IT disasters. In the event of such a disaster, OSHA may not be able to restore their system applications and data in a timely or efficient manner. Without taking the necessary steps to fully implement and test contingency plans, OSHA may not fully and adequately support management’s overall business and security objectives.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet contingency planning requirements for IMIS and CHIS.

Management Comments:

OSHA responded that in the opening sentence in the Condition section that the word “some” should be inserted before “policy and procedural guidance.” Also, it needs to be noted that there is no firm, formal DOL policy and procedures for comprehensive contingency plans. Recently, DOL formed a security workgroup to address this control objective DOL-wide. OSHA will be a full participant in this effort.

Conclusion:

We disagree with the comment about no firm, formal DOL policy and procedures for comprehensive contingency plans. Based on our review DOL does provide policy and procedures for comprehensive contingency plans. The DOL CSPP (October 22, 1999) and the CSH provide high level policy guidance regarding contingency planning which meet the intent of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.4). These DOL policy documents clearly require that all major applications (i.e., mission-critical systems) to have a contingency plan. (See Section 9, pages 10-11 of the CSPP and Chapter 4 of the CSH). In addition, Attachment C-*Contingency Planning Methodology Guide* of the CSH, provides the detailed procedures for contingency planning, which also meets the intent of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.4).

Furthermore, on June 21, 2001, the DOL Deputy Chief Information Officer, certified in the Department’s *Framework Self-Assessment Requirements to Comply with GISRA*, that the Department met the Contingency Planning policy

and procedures requirements of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.4).

While we commend and encourage OSHA's involvement in the DOL-wide security workgroup to address contingency planning, OSHA still needs to develop action plans and target dates to address the intent of the recommendation.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.2.5)**

**Hardware and
System Software
Maintenance**

Condition:

The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding hardware and system software maintenance. In addition, OSHA has promulgated additional procedures that provide additional guidance in this area. However, there are no written procedures for setting default settings of security features in the most restrictive mode.

We also found that OSHA has not implemented procedures to:

- Place restrictions on who performs maintenance and repair activities.
- Restrict access to all program libraries.
- Develop on-site and off-site maintenance procedures.
- Implement an impact analysis to determine the effect of proposed changes on the existing security controls, including the required training needed to implement the control.
- Use software change request forms to document request and related approvals.
- Specify the type of test data to be used.
- Document and obtain management approval for emergency change procedures.
- Set default settings of security features to the most restrictive mode.
- Update contingency plans and other associated documentation to reflect system changes.
- Document the use of copyrighted software or shareware and personally owned software/equipment.

Cause:

OSHA has not developed action plans and assigned the appropriate resources to fully implement hardware/system software maintenance requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states that, "...The head of each agency [should]...(A) adequately ensure the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets..."

FISCAM CC-1.2 states that "...Allowing employees to use their own software, or ever use diskettes for data storage that have been used elsewhere, increases the risk of introducing viruses. It also increases the risk of violating copyright laws and making bad decisions based on incorrect information produced by erroneous software..."

FISCAM CC-2.1 states that "...Once a change has been authorized, it should be written into the program code and tested in a disciplined manner. Because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of procedures or standards for prioritizing, scheduling, testing, and approving changes..."

FISCAM CC-2.3 states that "...Many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised

| | |
|--|---|
| | <p>software...Once a modified software has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. To accomplish these objectives, an entity should have and follow established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who need to begin using it...”</p> <p>FISCAM CC-3.2 states that "...Access to software libraries should be protected by the use of access control software or operating system features and physical access controls. Separate libraries should be established for (1) program development and maintenance, (2) user testing, and (3) production. Also, controlled copies of the source versions of all programs (the code created by programmers) should be separately maintained and protected from unauthorized access. If unauthorized modifications are suspected of a production program, the source code can be recompiled to determine what has been changed...”</p> <p>FISCAM CC-3.3 states that "...The movement of programs and data among libraries should be controlled by an organization segment that is independent of both the user and the programming staff...”</p> <p>FISCAM SC-2.1 states that "...Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions...”</p> <p>FISCAM SS-3.1 states that system software changes are authorized, tested, and approved before implementation.</p> <p>FISCAM SS-3.2 states that "...When possible, the installation of system software changes and new versions or products should be scheduled to minimize the impact on data processing operations, and an advance notice should be provided to system software users...”</p> <p>DLMS-9 establishes policy and procedure governing the authorized acquisition, reproduction and distribution or transmission of licensed and copyrighted computer software in the Department of Labor (DOL).</p> <p>The CSH requires that SSPs address hardware and system software maintenance controls over (1) servicing equipment on-site and off-site (2) documenting changes and approvals, (3) version control process, (4) distribution and implementation of new or revised software.</p> <p>Effect: The results of failing to ensure more complete and implemented hardware and system software procedures, especially in the areas of default settings that could easily be compromised and a lack of emergency change procedures could lead to unauthorized access or unanticipated changes to system applications and hardware.</p> <p>Recommendation: We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet hardware/system software requirements.</p> |
|--|---|

Management Comments:

No comments were provided.

Conclusion:

OSHA did not provide action plans or target dates to address the intent of the recommendation.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.2.6)**

Data Integrity

Condition:

The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding data integrity. The OSHANET SSP also provides OSHA with additional guidance in this area. However, the following procedures are not covered by DOL or OSHA:

- Update virus signature files routinely.
- Use integrity verification programs for applications to look for evidence of data tampering, errors, and omissions.
- Investigate inappropriate or unusual activity and take appropriate actions.
- Execute procedures to determine compliance with password policies.
- Install intrusion detection tools on the system.
- Review intrusion detection reports routinely and handle suspected incidents accordingly.
- Perform penetration testing on the system.

OSHA has implemented some data integrity requirements. However, the following procedures have not been implemented.

- Update virus signature files routinely.
- Use reconciliation routines for applications (i.e., checksums, hash totals, record counts)
- Execute procedures to determine compliance with password policies.
- Use integrity verification programs for applications to look for evidence of data tampering, errors, and omissions.

Cause:

OSHA has not developed action plans and assigned the appropriate resources to fully implement data integrity requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act (GISRA)*, states that, "...The head of each agency ... (A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets; (B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency..."

OMB Circular No A-130 states "...'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, availability, through the use of cost-effective management, personnel, operational and technical controls..."

FISCAM SS-2.2 states that inappropriate or unusual activity should be investigated and appropriate actions taken details the policies and procedures that should be taken when inappropriate or unusual activity occur which may contribute to data integrity issues.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, is a comprehensive document that details the policies that should be enforced in regards to securing information technology systems and promoting data integrity.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, advises that the determination of adequate controls over data integrity requires answers to whether "...Integrity verification programs [are] used by applications to look for evidence of data tampering, errors, and omissions? (Techniques include consistency and reasonableness checks and validation during data entry and processing) ...whether the "...access control mechanisms support individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual)...”and whether “...system performance monitoring [is] used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?...”

Effect:

The lack of effective data integrity controls could pose security vulnerability through:

- Inaccurate or missing data resulting from unauthorized destruction or tampering of electronic files and records.
- Access to proprietary or sensitive data by unauthorized personnel.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet data integrity requirements.

Management Comments:

The OSHA response disagreed with one of the bullets in the Condition section. In addition, the response questioned whether the CSH, DLMS-9, and the SDCLM provide policy guidance regarding data integrity. No other comments were provided.

Conclusion:

We removed bullet statement in the Condition. However, OSHA still needs to provide action plans and target dates to address the intent of the recommendation.

Based on our review, the CSH (Section 9c(1)(f)) and the DLMS-9 (Section 407), and the SDLCM (throughout the manual) do provide formal DOL policy guidance for data integrity that meets the intent of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.6).

| | |
|---|--|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.7)</p> | <p>Condition: The CSH and DLMS-9 provide policy and some procedural guidance to the DOL agencies regarding documentation requirements. SSPs for OSHANET, IMIS, and CHIS also provide OSHA with additional guidance in this area. However, there are no DOL or OSHA procedures requiring the following:</p> <ul style="list-style-type: none"> • Standard operating procedures exist for all the topic areas covered in the NIST Self-Assessment Guide. • Network diagrams and documentation on setups of routers and switched. • Software and hardware testing procedures and results. <p>OSHA has implemented some of the documentation requirements. However, OSHA has not completed the following documentation:</p> <ul style="list-style-type: none"> • Standard operating procedures exist for all the topic areas covered in the NIST Self-Assessment Guide. • Emergency procedures. • Contingency plans. • Certification and accreditation documents and statements authorizing the systems to process. <p>Cause: Information security personnel are in the process of enhancing current security policy, procedures and other applicable security documentation. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement data integrity requirements.</p> <p>Criteria: OMB Circular A-130, regarding how agencies will ensure security in information systems, states that agencies must "...incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning..."</p> <p>NIST Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology Systems</i>, states that "...Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures..."</p> <p>NIST Special Publication 800-12, <i>An Introduction to Computer Security: The NIST Handbook</i>, states that "...Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently..."</p> <p>Effect: Lack of documentation can lead to difficulty in supporting and enhancing OSHA's systems in the future. The lack of complete documentation could also lead to incomplete security policy and procedure functionality being followed,</p> |
|---|--|

thus, leaving the system vulnerable to threats. In addition, if updated and consistent security documentation is not available for access, users may involuntarily compromise OSHA's security practices, thus leaving its systems unsecured and susceptible to various vulnerabilities and threats, both internal and external.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet documentation requirements.

Management Comments:

OSHA response questioned whether the DLMS-9 and the CSH provide policy and procedural guidance to DOL agencies regarding documentation requirements. The response also questioned the authority of DLMS-9, since it was in draft during this review.

No other comments were provided.

Conclusion:

Based on our review, the CSH (Attachments A, B, and C)) and DLMS-9 (Sections 407A and 407B) do provide formal DOL policy and some procedural guidance related to documentation requirements that meet the intent of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.7).

Even though DLMS-9 was in draft, we gave credit to DOL and OSHA for having policy and procedures to the extent that DLMS-9 addressed the requirements identified in the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.2.7).

OSHA still needs to provide action plans and target dates to address the intent of the recommendation.

| | |
|--|---|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.8)</p> <p>Security Awareness, Training and Education</p> | <p>Condition: The CSH provides policy and procedural guidance to the DOL agencies regarding security awareness, training, and education. The CSH is available to all DOL employees through the LaborNet intranet. While OSHA has implemented most of the security awareness, training, and education requirements, rules of behavior were not available for CHIS.</p> <p>Cause: Until 2000, computer security awareness, training, and education was addressed locally. There was no agency-wide, formalized effort, with clear policy and procedural guidance.</p> <p>Criteria: OMB Circular A130 states that training should be provided to “ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system. In addition, this circular requires that agencies “...Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system...Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system...”</p> <p>NIST Special Publication 800-18, <i>Guide for Developing Security Plans for Information Technology Systems</i>, states that “...A set of rules of behavior must be established for each system. ... The rules of behavior should be made available to every user prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt...”</p> <p>The CSH requires rules of behavior for all systems. The CSH states that the rules of behavior should clearly delineate responsibilities and expected behavior of all individual with access to each agency system and must define the consequences of behavior not consistent with the rules of behavior.</p> <p>Effect: Without enforcing the requirements for rules of behavior, OSHA employees may not be fully aware of their responsibilities relative to the security of OSHA’s sensitive systems.</p> <p>Recommendation: We recommend that OSHA implement the rules of behavior for CHIS.</p> <p>Management Comments: No comments were provided.</p> <p>Conclusion: OSHA did not provide action plans or target dates to address the intent of the recommendation.</p> |
|--|---|

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.2.9)**

**Incident Response
Capability**

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) and OSHA’s OSHANET SSP provide policy and some procedural guidance to the DOL agencies regarding incident response capability. However, the CSH and OSHA procedures do not specifically require:

- Training personnel to recognize and handle incidents.
- Modifying incident responsibility capability procedures and control techniques after an incident takes place.
- Sharing incident information and common vulnerabilities or threats with other organizations with interconnected systems.
- Reporting incidents, vulnerabilities, and threats to Federal Computer Incident Response Capability (FedCIRC) and other Federal and local law authorities.

Despite the limited procedures, OSHA has established and maintained a formal incident response capability and process and does monitor and track incidents until resolution. In addition, management recently developed procedures to expedite helpdesk calls deemed to be potential computer security incidents and has recently hired a contractor to evaluate and update the helpdesk Escalation Procedures for Computer Security Incidents. However, OSHA has not:

- Provided training to recognize and handle incidents.
- Established a process to modify incident handling procedures and control techniques after an incident occurs.

Cause:

While OSHA has taken many actions to implement the incident response capabilities, it has not developed action plans and assigned the appropriate resources to fully implement incident response capability requirements.

Criteria:

The FY 2001 Defense Authorization Act, *Government Information Security Reform Act (GISRA)* states agencies must have “...procedures for detecting, reporting, and responding to security incidents, including...notifying and consulting with law enforcement officials and other offices and authorities...”

OMB Circular A-130 requires that agencies establish formal incident response mechanisms and make system users aware of these mechanisms and how to use them. The circular further states that “...To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide...”

FISCAM SP-3.4 requires “...agencies to establish formal incident response mechanisms and to make system users aware of these mechanisms and how to use them...”

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, indicates that “...when faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident...”

DLMS-9 and CSPP require all DOL agencies to train users on incident reporting, establish and maintain an ad hoc CSIRT and report all incidents appropriately.

Effect:

Without properly written, distributed, and executed incident reporting procedures, the risk that computer viruses can cause costly resource intensive resolution increases. In addition, without adequate and proper training, OSHA is susceptible to incorrectly responding to and/or mishandling reported incidents. Improperly handling of a reported incident could compromise the information systems security to additional threats or result in not resolving the threat in the most cost-effective method and/or in a timely manner.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet incident response capability requirements.

Management Comments:

No comments were provided.

Conclusion:

OSHA did not provide action plans or target dates to address the intent of the recommendation.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.3.1)**

**Identification and
Authentication**

Condition:

The CSH and DLMS-9 provide policy and some procedural guidance to the DOL agencies regarding identification and authentication requirements. OSHA also provides additional guidance in this area. However, there are no procedures regarding the following requirements:

- Maintain a current list of approved and authorized users, and their access.
- Prohibit access scripts with embedded passwords.
- Disable inactive user identifications disabled after a specified period of time.
- Do not display password when entered.
- Replace vendor-supplied passwords immediately.
- Terminals, workstations, and networked personal computers are not left unattended when the user ID and password are logged in.
- System owners periodically review access authorization listings to determine whether they remain appropriate.
- User IDs and passwords are immediately removed when users no longer need access to the system.

In addition, OSHA has implemented many of the identification and authentication requirements. However, the following requirements have not been implemented:

- Maintain a current list of approved and authorized users, and their access.
- Change passwords at least every 90 days or earlier, if needed.
- Prohibit access scripts with embedded passwords.
- Data owners periodically review access authorization listings to determine whether they remain appropriate.

Cause:

The geographic dispersion of OSHANET is a major contributing factor to the inconsistent implementation of procedures. Since OSHANET is not centrally managed, it has led to difficulty in monitoring the system. Each region has varying levels of resource expertise and sensitivity to security issues, which has led to inconsistencies in the implementation of policies and procedures. While OSHA intends to resolve these problems, it has not has not developed action plans and assigned the appropriate resources to fully implement identification and authentication requirements.

Criteria:

OMB Circular A-130 states that "...individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job..."

FISCAM AC-2.1 states that "...the computer resource owner should identify the specific user or class users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties...The owner should also identify the nature and extent of access to each

resource that is available to each user...” In general, users may be assigned one or more of the following types of access to specific computer resources: read, update, delete, merge, and/or execute.

FISCAM AC-2.2 states that “...Emergency and temporary access authorization is controlled...” Emergency and temporary access authorizations should be “...documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period...” The audit techniques include “...review of pertinent policies and procedures, compare a selection of both expired and active temporary and emergency authorizations with a system-generated list of authorized users, and determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed...”

FISCAM AC-3.2 states that “...Identification is the process of distinguishing one user from all others, usually through the use of user IDs. User IDs are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of user IDs is typically not protected. Typical controls for protecting the confidentiality of passwords include the following: password selection is controlled by the assigned user, passwords are changed periodically, about every 30 to 90 days, passwords are not displayed when they are entered, minimum character length, at least 6 characters, is set for the passwords so that they cannot be easily guessed, use of names, words, or old passwords within six generations is prohibited, while use of alphanumeric passwords should be encouraged, vendor-supplied passwords are replaced immediately upon implementation of a new system, and individual users are uniquely identified rather than having users within a group share that same ID or password...”

FISCAM AC-3.2 also states that “...to help ensure that passwords cannot be guessed, attempted to log on the systems with invalid passwords should be limited. Typically, potential users are allowed three or four attempts to log on...” Lastly, another technique for reducing the risk of password disclosure is encrypting the password file. Encryption further reduces the risk that the password file could be accessed and read by unauthorized individuals. NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that “...identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system...”

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that “...Passwords should be changed periodically...If passwords are used for authentication, organizations should specify Required Attributes. Secure password attributes such as a minimum length of six, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID should be specified and required...”

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that “...Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability...” NIST 800-12 provides ways of improving password security: password generators, limits on log-in attempts, password attributes (e.g., passwords with a certain minimum length, use of special characters, picking passwords that are

not in an on-line dictionary), periodic changing of passwords, and technical protection of the password file (e.g., one-way encryption).

Federal Information Processing Standards Publication 186-1 lays out a standard in the encryption algorithm.

The CSH requires the analysis of identification and authentication controls in the development of SSPs.

Effect:

Password management involves techniques, procedures and mechanisms that adequately protect the system from unauthorized, unlimited access and usage, and enhances the system's security. Poor or inadequate password management leaves the system vulnerable to such access from both internal and external sources. OSHA will need to develop and implement proper password procedures in order to mitigate against such risks.

Recommendations:

We recommend that OSHA take the following actions as soon as possible:

- Set and enforce strong password policy--both in writing and by computer configuration
- Require users to change passwords every 90 days
- Regularly download passwords from the servers and use password cracking software to test the strength of the passwords.

We also recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet identification and authentication requirements.

Management Comments:

OSHA response questioned whether the DLMS-9 and the CSH provide policy and procedural guidance to DOL agencies regarding identification and authentication requirements. The response also questioned the authority of DLMS-9, since it was in draft during this review.

No other comments were provided.

Conclusion:

Based on our review, Attachment A of the CSH and DLMS-9 (Sections 407A, B, E, F, and G) do provide formal DOL policy and some procedural guidance related to identification and authentication requirements that meet the intent of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.1). However, as noted in the Condition section, many of the required procedures are not addressed in the DOL documents.

Even though DLMS-9 was in draft, we gave credit to DOL and OSHA for having policy and procedures to the extent that DLMS-9 addressed the requirements identified in the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.1).

OSHA still needs to provide action plans and target dates to address the intent of the recommendations.

| | |
|---|--|
| <p>NIST Self-Assessment Guide for Information Technology Systems (Section 4.3.2)</p> <p>Logical Access Controls</p> | <p>Condition: The CSH and DLMS-9 provide policy and some procedural guidance to the DOL agencies regarding logical access control requirements. In addition, OSHA has established various policies and procedures through the OSHANET SSP regarding logical access controls over agency data. However, the following procedures are not covered by any of the above documents:</p> <ul style="list-style-type: none"> • Restrict access to files at the logical view or field. • Implement communication software to restrict access through specific terminals. • Disable insecure protocols (e.g., UDP, ftp). • Reinitialize all vendor-supplied default security parameters to more secure settings. • Maintain and review network activity logs. • Automatically disconnect the network connection at the end of a session. • Restrict trust relationships among hosts and external entities appropriately. • Monitor dial-in access. <p>OSHA has implemented many of the logical access controls requirements. However, the following requirements have not been implemented:</p> <ul style="list-style-type: none"> • Encryption meets Federal standards. • Key generation, distribution, storage, use, destruction, and archiving process for encryption. • Restrict access to files at the logical view or field. • Implement communication software to restrict access through specific terminals. • Disable insecure protocols (e.g., UDP, ftp). • Reinitialize all vendor-supplied default security parameters to more secure settings. • Maintain and review network activity logs. • Automatically disconnect the network connection at the end of a session. <p>Cause: In the past, OSHA did not have regular technical reviews of their security posture to examine existing and emerging threats to its general support system and associated major applications. Improvements have been made through the development of the OSHANET SSP, which analyze their security needs and provide implementation procedures of various security controls. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement logical requirements.</p> <p>Criteria: OMB Circular A-130 states that "...individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job..."</p> |
|---|--|

NIST SP 800-18 states that "...Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users..."

FISCAM AC-3.2 states that "...to ensure that access controls are uniformly administered, the security management function should implement and maintain logical access controls based upon authorizations from appropriate levels within the entity. ..."

FISCAM SD-2.1 indicates that physical and logical controls should be established. It further states that "...both physical and logical access controls can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities..."

The CSH defines logical access controls as "...system-based mechanisms that provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make...". The CSH states that logical controls should authorize or restrict the activities of users and system personnel within the general support system, permit only authorized access to or within the GSS, restrict users to authorized transactions and functions, and detect unauthorized activities.

Effect:

Results of the penetration test showed that complete compromise of the network is possible when passwords are weak, systems lack current patches, and security controls are inconsistently maintained. The penetration test team was able to remotely command the web server over the internet using a well-known vulnerability with Microsoft's web servers.

Recommendations:

We recommend that OSHA take the following actions as soon as possible:

- Regularly scan network for vulnerabilities using automated security scanners.
- Review the system's password strength by periodically pulling the encrypted passwords from the systems and running a password cracker against the passwords.
- Install third party password restrictive software that will force users to choose good passwords.
- Keep systems updated on current security patches and security fixes.

We also recommend that OSHA develop action plans and assign resources to fully implement all remaining logical access control requirements.

Management Comments:

OSHA response questioned whether the DLMS-9 and the CSH provide policy and procedural guidance to DOL agencies regarding logical access controls. The response also questioned the authority of DLMS-9, since it was in draft during this review.

No other comments were provided.

Conclusion:

Based on our review, Attachment A of the CSH and DLMS-9 (Sections 407A, B, E, F, and G) do provide formal DOL policy and some procedural guidance related to logical access controls that meet the intent of the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.2). However, as noted in the Condition section, many of the required procedures are not addressed in the DOL documents.

Even though DLMS-9 was in draft, we gave credit to DOL and OSHA for having policy and procedures to the extent that DLMS-9 addressed the requirements identified in the NIST *Self-Assessment Guide for Information Technology Systems* (Section 4.3.2).

OSHA still needs to provide action plans and target dates to address the intent of the recommendations.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.3.3)**

Audit Trails

Condition:

Within the last two years, the Department of Labor (DOL) has issued policies and procedures addressing Audit Trails. For example, the CIO's Computer Security Handbook (CSH) provides audit trail policies and procedures to be followed by the DOL agencies. In addition, OSHA also provides policies and procedures covering this area. However, the following procedures are not covered by DOL or OSHA:

- Ensure separation of duties between security personnel who administer the access control function and personnel who administer the audit trail.
- Review the audit trail logs on a regular and continuous basis.
- Utilize keystroke monitoring.

OSHA has implemented many of the audit trail requirements. However, the following procedures have not been implemented:

- Strictly control access to online audit logs.
- Retain off-line storage of audit logs for a period of time and strictly control access to the audit logs.
- Ensure separation of duties exist between security personnel who administer the access control function and those who administer the audit trail.
- Review audit trails frequently.
- Use automated tools to review audit records in real time or near real time.

Cause:

In the past, OSHA took a reactive rather than a proactive approach to this area. The agency did not have a formal, documented, prevention and detection program, or agency-wide regular technical reviews of its security posture to examine existing and emerging threats to its general support system and associated major applications. Improvements have been made through the development of the OSHANET SSP, which analyze their security needs and provide implementation procedures of various security controls. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement logical requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states that the head of each agency shall develop and implement an agency-wide information security program to include "procedures for **detecting**, reporting, and responding to security incidents..." (emphasis added).

FISCAM AC-4 states that "...security software generally provides a means of determining the source of a transaction of an attempted transaction and of monitoring users' activities (the audit trail). However, to be effective (1) this feature should be activated to maintain critical audit trails and report unauthorized or unusual activity and (2) managers should review and take action on these reports..."

NIST Special Publication 800-18: *Guide for Developing Security Plans for Information Technology Systems*, states that agencies should have "...Audit trails maintain a record of system activity by system or application processes and by user activity...[and should consider whether]...(1) the audit trail support[s] after-the-fact investigations of how, when, and why normal

operations ceased ... (2) the audit trail provide[s] accountability by providing a trace of user actions... (3) access to online audit logs [is] strictly controlled... (4) ... separation of duties between security personnel who administer the access control function and those who administer the audit trail [exists] and (5) how frequently audit trails are reviewed and whether there are review guidelines...”

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that “...audit trails maintain a record of system activity by system or application processes by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification...”

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that “...an audit trail should include sufficient information to establish what events occurred and who (or what) caused them...” An event record should specify what event occurred, the User ID associated with the event, the program or command used to initiate the event, and the result.

The CSH states that “...audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. Audit trails provide a means to accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis...” Audit trails should provide accountability to users for their actions such as type of event, when the event occurred, the user ID associated with the event, and the program and command used to initiate the event.

Effect:

The penetration test team was able to remotely command the web server over the internet using a well-known vulnerability with Microsoft's web servers. Once administrative control is gained on the servers log files can be modified and deleted. With no intrusion detection system an organization's network can be compromised without ever knowing (i.e., no audit trails).

Without appropriate audit trail procedures, OSHA security is susceptible to unauthorized access to sensitive audit information and unauthorized modification or deletion of audit log information. If audit logs are not reviewed on a regular and continuous basis, system administrator will be unable to detect or recognize incidents or vulnerabilities in a timely manner. Because of its minimal compliance with the audit trail control requirements, OSHA's systems are vulnerable to user misuse and other security compromises.

Recommendations:

We recommend that OSHA independently test and implement an intrusion detection system as soon as possible.

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet audit trail requirements.

Management Comments:
No comments were provided.

Conclusion:
OSHA did not provide action plans or target dates to address the intent of the recommendations.

ACRONYMS

| | |
|---------|--|
| CHIS | Compliance Safety and Health Officer Health Information System |
| CIO | Chief Information Officer |
| COBOL | Common Business Oriented Language |
| CSPP | Cyber Security Program Plan |
| CSH | Computer Security Handbook |
| CSIRT | Computer Security Incident Response Team |
| DLMS | DOL Management Series |
| DNS | Domain Name Server |
| DOL | Department of Labor |
| FedCIRC | Federal Computer Incident Response Capability |
| FIPS | Federal Information Processing Standards |
| FISCAM | Federal Information Systems Controls Audit Manual |
| FY | Fiscal Year |
| GAO | General Accounting Office |
| GISRA | Government Information Security Reform Act |
| GSS | General Support System |
| HVAC | Heating, Ventilation and Air Conditioning |
| IATO | Interim Approval to Operate |
| IDS | Intrusion Detection System |
| IG | Inspector General |
| IMIS | Integrated Management Information System |
| INFOSEC | Information Security |
| IRM | Investment Resource Management |
| ISO | Information Security Office |
| IT | Information Technology |
| LAN | Local Area Network |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OSHA | Occupational Safety and Health Administration |
| PDD | Presidential Decision Directive |
| PwC | PricewaterhouseCoopers, LLP |
| SDLC | Systems Development Life Cycle |
| SDLCM | Systems Development and Life Cycle Management Manual |
| SSP | System Security Plan |
| ST&E | Security Testing and Evaluation |
| TFAR | Tentative Finding and Recommendations |
| WAN | Wide Area Network |

**MANAGEMENT RESPONSE TO THE
DRAFT REPORT**



SEP -7 2001

MEMORANDUM FOR:

JOHN J. GETEK
Assistant Inspector General
For Audit

FROM:

JOHN L. HENSHAW
Assistant Secretary

SUBJECT:

Response to GISRA Evaluation and
Security Test and Evaluation Draft Report
No. 23-01-006-10-001

This memorandum transmits OSHA's response to your August 29, 2001 request for written comments addressing GISRA Evaluation and Security Test and Evaluation Draft Report No. 23-01-006-10-001. Our detailed comments concerning the draft report's findings and recommendations are provided in the body of the attached draft report, primarily in the Management Comments sections. All changes and comments are highlighted and tracked throughout the draft report.

In addition, we are providing the following additional comments:

1. We agreed to provide an expeditious review and submission of comments concerning the tentative findings report with the understanding that we would have a further opportunity to comment on and/or make changes to the draft report. We, however, were not aware that:
 - Our written comments on your draft report are incorporated into the appropriate sections of the final report, along with your evaluation of our comments.
 - Our comments are included in their entirety as an attachment to the final report.
 - The final report, including our written comments, is subject to disclosure under the Freedom of Information Act and may be subject to discovery proceedings in the event of litigation.

In the future please inform us more thoroughly regarding the relevant details of the comment process.

2. The draft report does not make clear that some referenced DOL policy documents, particularly the Department of Labor Manual Series -9, Chapter 400, "Security," were still in the clearance process during the GISRA review.
3. The draft report does not make clear that OSHA has not yet addressed some of the control objectives, including Certification and Accreditation and Contingency Planning because complete and final DOL processes, procedures, and schedules for delivery have not yet been developed, cleared, and published. Department of Labor Security Workgroups have, however, been formed to address the objectives in the near-term. OSHA expects to be a full participant in these workgroups.
4. A point made early in the audit process by OSHA, but not captured in the tentative and draft reports is that the Compliance Safety and Health Officer (CSHO) Health Information System (CHIS) is a mis-classified system. Currently, CHIS is not a Major Application. It is primarily a management tool used to record, store, track, and make available a limited amount of administrative, financial, and medical data related to OSHA's Medical Examination Program.
5. An underlying assumption throughout the draft report seems to be that all requirements apply equally to all systems. This is not the case. We, therefore, recommend that the recommendation statements for each of the control objectives be changed to have OSHA implement only applicable requirements.

If you have any questions regarding our comments, please contact Cheryle A. Greenaugh, Director of the Directorate of Information Technology at (202) 693-1818, or Maria A. Jones, OSHA's Computer Security Point-of-Contact, at (202) 693-1729.

Office of Inspector General

U.S. Department of Labor
Office of Information Technology Audits

GISRA Evaluation and Security Test and Evaluation

Department of Labor
Occupational Safety and
Health Administration

**NOTICE - THIS DRAFT REPORT IS RESTRICTED TO
OFFICIAL USE ONLY**

This review was performed by PricewaterhouseCoopers LLP under contract to the Office of Inspector General. This is a draft report and is subject to revision before it is released in final form. This draft is provided to officials solely for their review and comment on the subjects reported. Recipients of this draft are not authorized to distribute or release this information except for official review and comment.

Report Number: 23-01-006-10-001

Date Issued:

TABLE OF CONTENTS

| | |
|---|-------------------------|
| EXECUTIVE SUMMARY | 1 |
| OVERVIEW OF SYSTEMS | 1 |
| DESCRIPTION OF EVALUATIONS | 2 |
| EVALUATION SUMMARY | 3 |
| FINDINGS AND RECOMMENDATIONS..... | 5 |
| RISK MANAGEMENT | 5 |
| REVIEW OF SECURITY CONTROLS..... | 7 |
| LIFE CYCLE | 9 |
| AUTHORIZE PROCESSING-CERTIFICATION & ACCREDITATION..... | 11 |
| SYSTEM SECURITY PLAN..... | 13 |
| PERSONNEL SECURITY..... | 15 |
| PHYSICAL AND ENVIRONMENTAL PROTECTION..... | 17 |
| PRODUCTION, INPUT/OUTPUT CONTROLS | 20 |
| CONTINGENCY PLANNING | 22 |
| HARDWARE AND SYSTEM SOFTWARE MAINTENANCE..... | 24 |
| DATA INTEGRITY..... | 27 |
| DOCUMENTATION..... | <u>30</u> 29 |
| SECURITY AWARENESS, TRAINING AND EDUCATION | <u>32</u> 31 |
| INCIDENT RESPONSE CAPABILITY | <u>33</u> 32 |
| IDENTIFICATION AND AUTHENTICATION | <u>35</u> 34 |
| LOGICAL ACCESS CONTROLS | <u>38</u> 37 |
| AUDIT TRAILS | <u>40</u> 39 |

The Department of Labor (DOL) and Occupational Safety and Health Administration (OSHA) have developed and implemented many information security-related policies and procedures. However, OSHA needs to continue to strengthen its information security program. In particular, OSHA management needs to focus its attention and resources on implementing controls related to the following high priority areas: Risk Management; System Security Plan (SSP); Certification and Accreditation of Systems; Incident Response Capability; Identification and Authentication; Logical Access; and Audit Trails.

The FY 2001 Defense Authorization Act, Section X, Subtitle G, contains the Government Information Security Reform Act (GISRA), which requires the Inspector General (IG) or the independent evaluator, as determined by the IG, to evaluate the Department of Labor's (DOL) mission-critical systems. In addition to the above requirement, the Office of the Inspector General (OIG) is required to conduct cyber security testing and evaluation (ST&E) in support of *Presidential Decision Directive (PDD) 63* and in accordance with DOL's *Cyber Security Program Plan*. During the period of June through August 2001, PricewaterhouseCoopers (PwC) performed an evaluation of the implementation of the GISRA requirements by OSHA and an ST&E of OSHA's general support system to determine how well the system security access controls enforce the agency's policy.

Implementation of security requirements were verified and validated against the National Institute of Standards and Technology's (NIST) *Self-Assessment Guide for Information Technology Systems (Self-Assessment Guide)*, which encompasses requirements of GISRA, Office of Management and Budget (OMB) Circular A-130, General Accounting Office (GAO) Federal Information Systems Controls Audit Manual (FISCAM), NIST Publications, and other Federal guidance.

An overview of the systems included in the GISRA evaluation and ST&E, our scope and methodology, and the summary results of our evaluations are described in the following sections of the report. The details of our findings are included in the "Findings and Recommendations" section of this report.

OVERVIEW OF SYSTEMS

The GISRA evaluation encompassed ~~two~~ one OSHA major applications—The Integrated Management Information System (IMIS) ~~--and the~~ Compliance Safety and Health Officer Health Information System (CHIS).

IMIS was created to satisfy the automated data processing requirements of OSHA. OSHA relies on the system to plan, manage, track and report on its enforcement, consultation and discrimination programs. The information is also used in rulemaking and compliance assistance programs. The system primarily collects and manages information on workplace safety and health ~~and contains~~ inspections, and also includes information on complaints, accident reports, referrals, 11(c) discrimination cases, health sampling, and consultation visits. The IMIS includes data for more than 2.5 million inspections records from 1972 to present., information on complaints, accident reports, referrals, 11(c) discrimination cases, health sampling, and consultation visits. ~~OSHA uses this information in rulemaking and compliance assistance programs.~~

CHIS is a small Local Area Network (limited to 5 authorized operators) used to record, ~~store~~ rack, track, and make available, a limited amount of , monitor, store, and make available medical, financial and administrative, financial and medical data pertinent to agency personnel performing its medical who participate in OSHA's Medical Examination Program. OSHA uses this information in its assessment of available manpower to perform field duties. ~~examination program, primarily as to the fitness for duty of OSHA's medical officers.~~

The ST&E was performed on OSHA's OSHANET general support system (GSS). OSHA's GSS, housed in Washington DC, is a local area network (LAN) providing office automation capabilities for the OSHA's National Office. It also serves as a nationwide network supporting data communications and office automation capabilities for OSHA offices located throughout the U.S. Its data communications allow OSHA users to maintain and use their e-mail and Internet/Intranet services. In addition, it allows OSHA users to access and ~~use~~ manipulate major applications and other services, (such as IMIS, ATA, Travel Manager, and home directories) on the GSS.

DESCRIPTION OF EVALUATIONS

Scope

The PwC team evaluated whether DOL and/or OSHA had promulgated policies and procedures that covered the GISRA requirements, as defined in the NIST Self-Assessment Guide. In addition, the team assessed the implementation of GISRA requirements for two OSHA major applications--IMIS and CHIS. The evaluation of the implementation of GISRA requirements was assessed against the 212 questions listed under the following 17 control objectives in the NIST Self-Assessment Guide:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification & Accreditation)
- System Security Plan
- Personnel Security
- Physical and Environment Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

The PwC team also conducted an ST&E of OSHA's GSS through penetration testing to determine how well the system security access controls enforce the agency's policy. The objective of the ST&E was to assess the technical implementation of the security design and to ascertain that security software, hardware, and firmware features affecting confidentiality, integrity, availability, and accountability have been implemented as required by the technical control objectives (i.e., Identification and Authentication, Logical Access Controls, and Audit Trails) in the NIST Self-Assessment Guide.

Methodology

Security requirements were reviewed and tested based on the NIST Self-Assessment Guide, as agreed to by DOL management, the OIG, and the PwC team. The PwC used an audit program, based on NIST Self-Assessment Guide, to complete the following three phases:

Phase I: Planning

- Conduct entrance meetings with OIG officials, the DOL Chief Information Officer (CIO), and selected OSHA management officials
- Develop request lists of information required to complete project
- Develop proforma data collection instruments for agency staff interviews and other data collection needs
- Develop detailed work program to identify specific steps to complete the GISRA review and evaluations

Phase II: Verification and Testing

- Review and analyze documentation
- Conduct interviews
- Perform internal and external penetration testing to:
 - Determine if security defenses sufficiently protected the network
 - Identify network topology/vulnerabilities
 - Use the topology and system vulnerabilities to determine if unauthorized access to internal network is possible
 - Demonstrate identified vulnerabilities
- Document GISRA evaluation and ST&E results
- Prepare ~~work papers~~ work papers and perform supervisory review

Phase III: Reporting

- Conduct meetings with appropriate staff regarding tentative findings
- Complete Tentative Findings Report--Combine GISRA evaluation and ST&E findings
- Perform supervisory review
- Respond to OIG review
- Hold meeting with agency management to discuss the results and recommendations for corrective action.
- Respond to agency review
- Revise Tentative Finding Report and issue Draft Report
- Hold closing meeting with OIG to deliver Final Report

EVALUATION SUMMARY

We found that overall the Department and OSHA have promulgated policies and some procedures covering all of the 17 control objectives. However, additional procedures are needed for the following 12 control objectives:

- Review of Security Controls
- System Security Plan
- Personnel Security
- Physical Security and Environmental Controls
- Production, Input/Output Controls
- Hardware/System Software Maintenance
- Data Integrity
- Documentation
- Incident Response Capability
- Identification and Authentication
- Logical Access Controls
- Audit Trails

We also reviewed OSHA's implementation of the 17 control objectives in the NIST Self-Assessment Guide. While OSHA has implemented many of the requirements under the control objectives, there are still requirements that have not been implemented for each of the 17 control objectives.

While all areas are considered important, the table below identifies the control objectives we considered high and medium priority based. For purposes of assessing priorities for each control objective, we used the following criteria:

High Priority: Control objectives that are characterized by the following: (1) inherently high risk; (2) DOL or agency procedures are limited; or (3) implementation of the procedures is limited.

Medium Priority: Control objectives that are still important, but do not meet any of the above criteria.

| Control Objective Category | High Priority | Medium Priority |
|--|---------------|-----------------|
| Management Controls | | |
| Risk Management | | X |
| Review of Security Controls | | X |
| Life Cycle | | X |
| Authorize Processing (Certification and Accreditation) | X | |
| System Security Plan | | X |
| Operational Controls | | |
| Personnel Security | | X |
| Physical and Environmental Protection | | X |
| Production, Input/Output Controls | | X |
| Contingency Planning | X | |
| Hardware and System Software Maintenance | | X |
| Data Integrity | | X |
| Documentation | X | |
| Security Awareness, Training and Education | | X |
| Incident Response Capability | X | |
| Technical Controls | | |
| Identification and Authentication | X | |
| Logical Access Controls | X | |
| Audit Trails | X | |
| Total | 7 | 10 |

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.1.1)**

Risk Management

Condition:

The CIO's Computer Security Handbook (CSH) provides the risk management policies and procedures to be followed by the DOL agencies.

We confirmed that the OSHA's risk assessments for CHIS and IMIS substantially complied with the CSH. Both risk assessments were completed on November 28, 2000. IMIS does not process classified information but does handle what is considered agency sensitive and proprietary information and contains Privacy Act data.

However, OSHA has not fully implemented the risk management process as required by the CSH. In particular, OSHA has not:

- Conducted final risk determinations and related management approvals are not documented and maintained on file.
- Conducted a mission/business impact analysis subsequent to the recent risk assessment process.

Cause:

Prior to 2000, risk assessments were handled locally without a prescribed methodology, tool, or agency-required documentation requirements. While OSHA has taken significant actions to implement the risk management requirements, it has not prepared a detailed plan of action to identify and prioritize the specific steps of implementation of the selected safeguards which could reduce or eliminate the vulnerability of the systems to the threats.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act* (GISRA) states that the head of each agency shall ensure that the agency's security plan is practiced throughout the life cycle of each agency system.

OMB Circular A-130 states that agencies shall establish information system management oversight mechanisms that ensure major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources.

FISCAM CC-1: states that agencies should have a documented SDLC methodology that details the procedures that are to be followed when applications are being designed and developed, as well as when they are subsequently modified. It further states that policies and procedures should be in place that detail who can authorize a modifications and these authorizations are to be documented.

NIST 800-18: *Guide for Developing Security Plans for Information Technology Systems*, states that an organization should be able to respond quickly when faced with an incident. Specifically, the publication states "Although a computer security plan can be developed for a system at any point in the life

cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle.”

NIST 800-27: *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, this recently released publication (June 2001) presents security principles and their relationship/applicability to each phase of life cycle development.

NIST 800-30: *Risk Management Guide (Draft)* states that all security-related activities are a part of the risk management process and that risk management spans the entire system development life cycle (SDLC).

The CSH requires OSHA to update the SSP as the system progresses throughout its life cycle.

Effect:

The absence of a current and clear understanding by program officials of the vulnerabilities of its systems limits the ability of OSHA to make timely decisions to mitigate risks to the OSHA mission and ability to carry on its normal business operations. Thus, effective security controls needed to ensure that the information in OSHA's systems is adequately protected and can be relied upon for decision-making may not be implemented

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet risk management requirements.

Management Comments:

Condition: We do not agree with paragraph two, sentence two of this section. We are not aware of any proprietary information in the IMIS. We recommend the sentence be changed to read, "IMIS does not process classified information but does handle what is considered agency sensitive information and limited Privacy Act data."

**Review of Security
Controls**

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) provides policy guidance to the DOL agencies regarding conducting periodic reviews of security controls. However, the following procedures are not specifically addressed in the DOL or OSHA guidance documents:

- Review the operating system periodically to ensure the configuration prevents circumvention of the security software and application controls.
- Routinely conduct tests and examinations of key controls (i.e., network scans, analyses of router and switch setting, penetration testing).

Independent reviews were recently conducted by external contractors Troy Systems and SeNet International. Self-assessments were conducted by OSHA. In addition, OSHA has analyzed security alerts/incidents and ensured that corrective actions have been effectively implemented. However, OSHA has not implemented the following requirements:

- Periodic reviews of its systems.
- Perform periodic reviews of its operating system to ensure the configuration prevents circumvention of the security software and application controls.
- Perform routine tests and exams of key controls (i.e., network scans, router and switch setting analysis, penetration testing).

Cause:

Until 2000, periodic security review programs were not a high priority with OSHA. However, OSHA has made progress in implementing the requirements related to this area. OSHA has been adhering to guidance as it published and recently updated its SSPs previously prepared under the NIST guidance in 1998. OSHA's Security Program Plan dated July 27, 2001, states that it will develop procedures for review of security controls process. However, OSHA has not developed an action plan, assigned resources, or established a schedule to develop and implement procedures to fully meet all security review control requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act (GISRA)*, requires that the head of each agency ensure periodic testing and evaluating of information security controls and techniques and implement appropriate remedial actions based on the evaluation. In addition, GISRA requires that each agency shall have an annual independent evaluation of the information security program and practices of that agency.

OMB Circular A-130 requires that agencies perform an independent review or audit of the security controls in each application at least every three years or sooner, if significant modification have occurred or where the risk and magnitude of harm are high.

FISCAM SP-5.1 states that "...Periodic assessments are an important means of identifying areas of noncompliance, reminding employees of their responsibilities, and demonstrating management's commitment to the security plan..."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that "... Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest hardware/software "patches"), and penetration testing can assist in the ongoing review of system security measures. These tools, however, are no substitute for a formal management review at least every three years..."

The CSH states that "...An independent review of security controls for each Major Application System should be performed at least every three years ... the results of the review conducted should be analyzed. Include specifics on who conducted the review. If any recommendation or findings were made as a result of the review, the outcome should be addressed..."

Effect:

Without established written procedures, it is difficult to ensure that periodic reviews of OSHA's applications will be performed on a continuous basis, which may leave OSHA's sensitive applications vulnerable to misuse, unauthorized access, and unauthorized modifications.

Recommendation:

2 We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet security review control requirements.

Management Comments:

Cause: We do not agree with sentence one of this section: We recommend the following change to more accurately explain the cause: "Until 2000, security reviews were handled locally without a prescribed methodology, schedule, or agency-wide documentation requirements."

Life Cycle

Condition:

The U. S. Department of Labor (DOL) *Systems Development and Life Cycle Management Manual* (SDLCM) provides the life cycle policies and procedures to be followed by all DOL agencies.

We reviewed the implementation of life cycle requirements for IMIS and CHIS. However, IMIS was developed in the 1970's and CHIS was developed in the mid 1990's. As such system documentation is unavailable and we are unable to assess OSHA's compliance with life cycle requirements in the initiation, development, and implementation phases. Thus, for implementation the scope of our review was limited to the operations/maintenance phase. During this phase the following requirements were not met:

- Periodic review of SSPs of IMIS and CHIS to reflect current conditions and risks.
- Purging, overwriting, degaussing, or destroying of information or media when no longer needed.

Cause:

Since the implementation of the CHIS system, OSHA has experienced frequent personnel and contractor turnover. Original life cycle documents have been either lost or misplaced through the handling by multiple parties. During the redesign of IMIS over the next several years, OSHA plans to follow policies and procedures set forth by the SDLCM. The IMIS redesign is currently in the design phase of the SDLCM.

However, OSHA has not developed action plans, assigned the appropriate resources, or established the timeline for the review and update of SSPs of IMIS and CHIS.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act* (GISRA) states that the head of each agency shall ensure that the agency's security plan is practiced throughout the life cycle of each agency system.

OMB Circular A-130 states that agencies shall establish information system management oversight mechanisms that ensure major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle, meet user requirements, and deliver intended benefits to the agency and affected publics through coordinated decision making about the information, human, financial, and other supporting resources.

NIST 800-27, *Engineering Principles for Information Technology Security*--this recently released publication (June 2001) presents security principles and their relationship/applicability to each phase of life cycle development.

NIST 800-30, *Risk Management Guide (Draft)*, states that all security-related activities are a part of the risk management process and that risk management spans the entire system development life cycle (SDLC).

The CSH requires all DOL agencies to update the SSP as the system progresses throughout its life cycle.

Effect:

Without adequate and proper life cycle documentation, OSHA is susceptible to inadequately funding security resources on a project or system. Without the proper funding, projects may be more vulnerable to security threats because proper security objectives were never developed and implemented. In the absence of a life cycle procedural documentation, OSHA can not be assured that information security objectives are practiced throughout the final stages of the systems' life.

Recommendation:

3

We recommend that OSHA assign appropriate resources and develop and implement actions plans to review and update SSPs for IMIS and CHIS and meet all appropriate life cycle phases requirements for those systems

Management Comments:

Condition: We do not agree with paragraph two, bullet number one of this section. Since 1998, OSHA has had periodic reviews of the IMIS and CHIS SSPs by the OCIO. The documents are on file both in the OCIO and in OSHA's Directorate of Information Technology.

Cause: We do not agree with the part of paragraph two that states OSHA has not "established the timeline for the review and update of SSPs of IMIS and CHIS. The timeline for review and update of both SSPs was established in a documented submitted earlier in FY 2001. Since that time, the IMIS SSP has been updated (see Version 1.1 on file in the OCIO). Version 1.1 includes information on planned revisions.

**NIST Self-Assessment
Guide for Information
Technology Systems
(Section 4.1.4)**

**Authorize
Processing-
Certification &
Accreditation**

Condition:

The CSH and the DOL Management Series 9 (DLMS-9)--*Information Technology* provide policy and some procedural guidance to the DOL agencies regarding authorize processing--certification and accreditation requirements. The DLMS-9 was in the clearance process during this review.

IMIS has an interim authority to operate and has met all requirements that serve as a basis for certification and accreditation, except for implementing signed Rules of Behavior. While OSHA developed Rules of Behavior, they have not been signed off by users.

CHIS has not been certified or accredited and does not have an interim authority to operate. OSHA has developed a security plan and risk assessment (i.e., requirements for certification and accreditation) for CHIS. However, it has not implemented the following requirements that support the certification and accreditation process:

- Established Rules of Behavior that are signed by users.
- Developed and tested a contingency plan.
- Determined that in-place safeguards are operating as intended.
- Initiated prompt action to correct deficiencies.

Cause:

OSHA officials have held discussions with the DOL Office of the Chief Information Officer with respect to certification and accreditation of both IMIS and CHIS and have focused on the recent certification and accreditation of IMIS. OSHA expects to implement the required procedures and obtain certification and accreditation of CHIS in the near future. In addition, OSHA officials plan to incorporate employee sign-off in the security awareness training planned for September 2001. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement authorize processing--certification and accreditation requirements.

Criteria:

OMB Circular A-130 requires that "...A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk or magnitude of harm is high..."

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states "...Management authorization must be based on an assessment of management, operational and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by technical evaluation and/or for security evaluation, risk assessment, contingency plan, and signed rules of behavior...Reauthorization should occur prior to a significant change in the system, but at least every three years..."

The NIST FIPS PUB 102, *Guideline for Computer Security Certification and Accreditation*, explains that the certification process is a technical process that produces a judgment, statement of opinion, and complements the accreditation process. Accreditation [FIPS 39] is the authorization and approval, granted to an ADP system or network to process sensitive data in an operational environment,

and made on the basis of a certification by designated technical personnel of the extent to which design and implementation of the system meet pre-specified technical requirements for achieving adequate data security. Accreditation is the official management authorization for operation.

DLMS-9 states that agency heads "...are responsible for...issuing Interim Approval to Operate (IATO) under specified conditions to information systems that need to connect to an operational system(s) before full authorization is possible. This may be done in coordination with the CIO on a temporary basis as a facilitating measure to attain full authorization...The IATO may be granted for no more than a one-year period..."

The CSH requires that the Rules of Behavior (ROB) "...should clearly delineate responsibilities and expected behavior of all individuals with access to the General Support System or major application, and must define the consequences of behavior not consistent with the ROB...It is recommended that the rules contain a signature page for each user to acknowledge receipt..."

Effect:

Without proper certification and accreditation of OSHA's major applications, management cannot be assured that security controls have been designed into its systems as planned, which may leave sensitive data vulnerable to unauthorized access and use.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet authorize processing--certification and accreditation requirements for IMIS and CHIS.

Management Comments:

Condition: We recommend that this section be revised to reflect the following facts:

Currently there is no formal DOL Certification and Accreditation Process in place. However, a DOL Security Workgroup has been formed to address this control objective. OSHA will be a full participant on this workgroup.

System Security Plan

Condition:

The CSH and the CSPP provide policy and some procedural guidance to the DOL agencies regarding the development of SSPs. However, the following procedures are not addressed in the above DOL documents:

- SSPs should be approved by key affected parties and management.
- The summary of the plans should be incorporated into the strategic IRM plan.
- The plan should be reviewed periodically and adjusted to reflect current conditions and risks.

In addition OSHA has implemented all SSP requirements for IMIS and CHIS, except a summary of the security plan in the strategic IRM plan.

Cause:

OSHA has been following OCIO guidance regarding SSP development and recently issued a new OSHA SPP that states OSHA will develop procedures in this area as required. In addition, system re-design work is about to be conducted on both major applications, which will require amendments to their original security program plans to bring them into them into full compliance with SSP requirements. However, OSHA has not developed action plans or assigned the appropriate resources to fully implement SSP requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states "...Each agency shall develop and implement an agency-wide information security program to provide information security for the operations and assets of the agency, including operations and assets provided and managed by another agency..."

OMB Circular A-130 requires Federal agencies to "...Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include: Application Rules, Specialized Training, Personnel Security, Contingency Planning, Technical Controls, Information Sharing, and Public Access Controls..."

OMB Bulletin 90-08 states that "...The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the agency's plan for meeting those requirements. The system security plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system..."

FISCAM SP-2 states that (1) "...Entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it. The plan and related policies should cover all major systems and facilities...", (2) to help ensure that the plan is complete and supported by the entity as a whole, senior management should obtain agreement from all affected parties in establishing policies for a security program, (3) "...To be effective, the policies and plan should be maintained to reflect current conditions...Outdated policies and plans not only

reflect a lack of top management concern, but also may not address current risks, and, therefore, may be ineffective...”.

NIST 800-14, *Principles and Practices for Securing Information Technology (IT) Systems*, states that “...A security plan should be used to ensure that security is considered during all phases of the IT system life cycle...”.

NIST 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that all applications and systems must be covered by SSPs if they are categorized as a “major application” or “general support” system.

The CSH states that “...One aspect of managing an IT system is the development of a System Security Plan (SSP), which is documentation of the protection afforded the system by technical, managerial, and operational means. In addition, it states that, “...A SSP is a living, dynamic document reflecting the current security posture of the IT system. The SSP should be developed during the initial phases of system development and acquisition...The SSP should also be updated on the basis of the subsequent mitigation activity or plan, after a significant system configuration change, or every three years. When the system is decommissioned, the SSP should be updated and stored with system records...”.

The CSPP states that all Federal IT systems have some degree of sensitivity and are required to have a SSP and that all DOL systems will have current and effective SSP.

Effect:

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. Also, by not incorporating the summary of SSP into the strategic IRM plan, increases the risk that information management activities may not be carried out in the most efficient, effective, and economical manner.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet SSP requirements for IMIS and CHIS.

Management Comments:

Condition: the statement that “In addition OSHA has implemented all SSP requirements for IMIS and CHIS, except a summary of the security plan in the strategic IRM plan” is inconsistent with the Condition and Cause statements in Section 4.1.3, Life Cycle.

5

Personnel Security

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) provides policy and some procedural guidance to the DOL agencies regarding personnel security. However, the CSH and OSHA procedures do not specifically require:

- Documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties.
- Distinct systems support functions performed by different individuals.
- Regularly scheduled vacations and periodic job/shift rotations.
- Specific personnel security procedures for hiring and transfer of personnel.

Furthermore, for IMIS and CHIS, OSHA does not:

- Segregate duties based on job descriptions and responsibilities.
- Regularly schedule vacations or periodic job/shift rotations.
- Complete appropriate background screening for assigned positions prior to granting access.

Cause:

While OSHA has performed screening of individuals based on the sensitivity of the position (especially those individuals involved with CHIS), it had in the past decided not to do so where the risk involved did not justify screening costs of trusted employees. OSHA is currently committed to complying with recent OCIO requirements to meet OPM policies regarding personnel security and is in the process of implementing procedures in this area. However, OSHA has not developed action plans or assigned the appropriate resources to fully implement personnel security requirements.

Criteria:

OMB Circular A-130 requires screening of personnel who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.

FISCAM SD-1 states that management should document job descriptions that clearly describe employee duties and prohibited activities.

FISCAM SD-1.1 requires that incompatible duties be identified and policies implemented to segregate these duties.

FISCAM SD-4.1 states "...The security plan should include policies related to the security aspects of hiring, terminating, and transferring employees and assessing their job performance..."

FISCAM SP-1.2 states that "...Documented job descriptions should exist that clearly describe employee duties and prohibited activities..."

FISCAM SP-4 states that management should include policies related to the security aspects of hiring, terminating and transferring employees and assessing their job performance.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that (1) all positions should be reviewed for sensitivity level, and (2) user access be restricted (least privilege) to data files, to processing capability, or to peripherals and type of access to the minimum necessary to perform the job.

Effect:

Without development and implementation of adequate personnel screening requirements, OSHA is exposed to the risk of improper and unauthorized access to its sensitive applications. Improper system access could compromise the efficient working of the systems by misuse, unauthorized modification, viewing of sensitive information, and system disruption.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet personnel security requirements.

Management Comments:

No comment.

**Physical and
Environmental
Protection**

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) provides policy and some procedural guidance to the DOL agencies regarding physical and environment protection. However, the CSH and OSHA procedures do not include the following requirements:

- Secure unused keys.
- Authenticate visitors, contractors and maintenance personnel through the use of preplanned appointments and identification checks.
- Emergency exit and re-entry of personnel after fire drills.
- Change computer room entry codes periodically.
- Sign-in and escort visitors into sensitive areas.
- Investigate and take remedial action for suspicious access activity.
- Review fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson periodically.
- Install redundant air-cooling system.
- Periodically review electronic power distribution, heating plants, water, sewage, and other utilities for risk of failure.
- Provide an uninterruptible power supply or back up generator.
- Encrypt data files on laptops.
- Store laptops and other portable systems securely.
- Protect system from plumbing lines.
- Limit viewing of computer monitors by unauthorized personnel.
- Control physical access to data transmission lines.

Despite the limited procedures, OSHA has implemented many physical and environment protection controls, such as physical access controls and fire safety measures. However, based on our interviews, review of documentation, and our observations at the OSHA Headquarters Network (GSS) Operations Center, we found the following deficiencies.

- The possibility exists for unauthorized physical access to data transmission lines through phone/data line closets through access to keys to other DOL agency closets, which can also open the phone closets.
- While contractor maintenance is monitored, the contractors are not escorted to the closets.
- Unauthorized persons can gain access to view computer monitors and potentially sensitive information.
- An unprotected door to the IMIS network operations center was identified.

In addition, OSHA has recently undergone contractor transition with respect to CHIS and the physical protection of daily operations of this system could be compromised.

Cause:

OSHA operates in facilities that are controlled by DOL and is limited in its ability to develop and implement procedures over the physical environment. OSHA will continue to try to obtain shared responsibility over the physical environment.

Criteria:

FISCAM AC-3 requires agencies to establish physical and logical access controls to prevent or detect unauthorized access.

FISCAM AC-3.1 requires "...Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment...".

FISCAM SC-2.2 details the policies and procedures that should be in place to prevent potential damage to facilities and interruptions in service and states that "...Environmental controls prevent or mitigate potential damage to facilities and interruptions in service.... Environmental controls can diminish the losses from some interruptions such as fires or prevent incidents by detecting potential problems early, such as water leaks or smoke, so that they can be remedied. Also uninterruptible or backup power supplies can carry a facility through a short power outage or provide time to back up data and perform orderly shut-down procedures during extended power outages...".

FISCAM AC-4 requires agencies to monitor access, investigate apparent security violations, and take appropriate remedial action details the policies and procedures that should be in place in order to maintain critical audit trails and report unauthorized or unusual activity.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, discusses the physical and environmental security controls that "...are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical environmental security program should address the following seven topics--Physical Access Controls, Fire Safety Factors, Failure of Supporting Utilities, Structural Collapse, Plumbing Leaks, Interception of Data, Mobile and Portable Systems. In doing so, it can help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft...".

DOL Management Series 9, *Information Technology*, requires agencies to develop procedures ensuring adequate physical security of network assets.

Department of Labor *Security Program Plan Instructions* state that "...Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation...".

The CSH requires physical and environmental security controls to be implemented to protect the facility housing system resources, the system resources themselves and the facilities used to support the operation.

Effect:

The lack of clearly defined policy and procedures in place for physical and environment protection controls exposes OSHA to interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

Recommendation:

1 We recommend that OSHA, working in concert with DOL assign appropriate resources and develop and implement action plans to fully meet physical and environmental control requirements.

Management Comments:

Cause: We do not agree with sentence two of this section. We are not aware of any OSHA plans to "try to obtain shared responsibility over the physical environment." To be accurate, the sentence should read, "OSHA will continue to try to obtain more detailed information from DOL and GSA about the physical environment and in place and planned controls."

**Production,
Input/Output
Controls**

Condition:

DOL and OSHA have policies and most procedures covering production, input/output control requirements. However, there are no procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media.

In addition, we found that OSHA has implemented some production, input/output controls. However, it has not implemented the following controls:

- Ensuring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Transporting or mailing media or printing.
- Internal/external labeling for sensitivity.
- External labeling with special handling instructions.
- Audit trails for inventory management.
- Physical protection of media storage vault/library.
- Sanitizing media for reuse.

Cause:

In the past, OSHA did not implement more stringent input/output controls, because most data was not considered to be sensitive. More recently, has OSHA developed procedures for input/output controls and is in the process of implementing these procedures. While OSHA is making progress, it has not assigned resources or developed action plans to issue procedures and fully implement requirements related to production, input/output controls.

Criteria:

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology System*, specifically require agencies to develop and implement the following procedures:

- Ensuring that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information.
- Ensuring that only authorized users pick up, receive, or deliver input and output information and media.
- Transporting or mailing media or printing.
- Internal/external labeling for sensitivity.
- External labeling with special handling instructions.
- Audit trails for inventory management.
- Physical protection of media storage vault/library.
- Sanitizing media for reuse.

The CSH requires that production, input/output controls include measures used to protect information that is input into the system (such as raw data), information that is processed by the system, and the information that is result of processing by the system, such as a report. Examples of controls would be marking, storing, and transmitting sensitive documents; procedures for sanitizing electronic media for reuse or prior to maintenance or repair; and installing and updating software to preclude unintentionally degrading system operation or corruption of data.

Effect:

Without the development and implementation of clearly defined policy and procedures related to production, input/output controls, OSHA runs the risk of loss of input/output information and media and possibly exposing sensitive information to unauthorized users.

8

Recommended Corrective Action:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet production, input/output control requirements.

Management Comments:

Cause: In sentence two, the "has" before "OSHA" should be after "OSHA."

**Contingency
Planning**

Condition:

The CSH and the CSPP provide policy and procedural guidance to the DOL agencies regarding contingency planning.

However, CHIS has no contingency plan and no contingency planning procedures have been implemented for CHIS. In addition, OSHA has not periodically tested and readjusted the IMIS contingency plan, as appropriate.

Cause:

OSHA has not assigned resources or developed action plans to fully implement contingency planning requirements for IMIS or CHIS.

Criteria:

OMB Circular A-130 states that with regards to contingency planning, agencies should "...establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support...Experience has demonstrated that testing a contingency plan significantly improves its viability...".

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, "...requires that the agency have procedures that will permit a continuation of essential functions if information technology support is interrupted...The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated...General support systems require appropriate emergency, backup and contingency plans...These plans should be tested regularly to assure the continuity of support...Also, these plans should be known to users and coordinated with their plans for applications...".

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that "...an organization should test and revise the contingency plan. A contingency plan should be tested periodically...". It also indicates the functional steps that an organization should employ when preparing for contingencies and disasters. These steps are (1) develop a business plan, (2) identify resources (3) develop scenarios, (4) develop strategies, and (5) test and revise the plan.

FISCAM, SC-1.3 states that "...In conjunction with identifying and ranking critical functions, the entity should develop a plan for restoring critical operations. The plan should clearly identify the order in which various aspects of processing should be restored, who is responsible, and what supporting equipment or other resources will be needed...".

FISCAM, SC-2.1 states that "...Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions...".

FISCAM, SC-3.1 states that "...Contingency plans should be documented, agreed on by both user and data processing departments, and communicated to affected staff...Staff should be trained in and aware of their responsibilities in preventing mitigating and responding to emergency situations...Training sessions should be held at least once a year and whenever changes to emergency plans are made...[The plan] should identify and provide information on:

- Supporting resources that will be needed,

- Roles and responsibilities of those who will be involved in recovery activities,
- Arrangements for off-site disaster recovery location and travel and lodging for necessary personnel, if needed,
- Off-site storage location for backup files, and
- Procedures for restoring critical applications and their order in the restoration process.” “Multiple copies of the contingency plan should be available with some stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable...”.

Department of Labor Management Series 9, *Information Technology*, requires that a contingency plan/disaster recovery plan for all information systems within a DOL agency must be completed prior to approval of SSPs.

Effect:

Without adequate contingency planning, OSHA is susceptible to operational difficulties related to unexpected IT disasters. In the event of such a disaster, OSHA may not be able to restore their system applications and data in a timely or efficient manner. Without taking the necessary steps to fully implement and test contingency plans, OSHA may not fully and adequately support management’s overall business and security objectives.

Recommendation:

9 We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet contingency planning requirements for IMIS and CHIS.

Management Comments:

Condition: In the opening sentence, the word “some” should be inserted before “policy and procedural guidance.” Also, it needs to be noted that there is no firm, formal DOL policy and procedures for comprehensive contingency plans. Recently, DOL formed a security workgroup to address this control objective DOL-wide. OSHA will be a full participant in this effort.

**Hardware and
System Software
Maintenance**

Condition:

The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding hardware and system software maintenance. In addition, OSHA has promulgated additional procedures that provide additional guidance in this area. However, there are no written procedures for setting default settings of security features in the most restrictive mode.

We also found that OSHA has not implemented procedures to:

- Place restrictions on who performs maintenance and repair activities.
- Restrict access to all program libraries.
- Develop on-site and off-site maintenance procedures.
- Implement an impact analysis to determine the effect of proposed changes on the existing security controls, including the required training needed to implement the control.
- Use software change request forms to document request and related approvals.
- Specify the type of test data to be used.
- Document and obtain management approval for emergency change procedures.
- Set default settings of security features to the most restrictive mode.
- Update contingency plans and other associated documentation to reflect system changes.
- Document the use of copyrighted software or shareware and personally owned software/equipment.

Cause:

OSHA has not developed action plans and assigned the appropriate resources to fully implement hardware/system software maintenance requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states that, "...The head of each agency [should]...(A) adequately ensure the integrity, confidentiality, authenticity, availability, and non-repudiation of information and information systems supporting agency operations and assets..."

FISCAM CC-1.2 states that "...Allowing employees to use their own software, or ever use diskettes for data storage that have been used elsewhere, increases the risk of introducing viruses. It also increases the risk of violating copyright laws and making bad decisions based on incorrect information produced by erroneous software..."

FISCAM CC-2.1 states that "...Once a change has been authorized, it should be written into the program code and tested in a disciplined manner. Because testing is an iterative process that is generally performed at several levels, it is important that the entity adhere to a formal set of procedures or standards for prioritizing, scheduling, testing, and approving changes..."

FISCAM CC-2.3 states that "...Many federal agencies have data processing operations that involve multiple locations and require a coordinated effort for effective and controlled distribution and implementation of new or revised

software...Once a modified software has been approved for use, the change should be communicated to all affected parties and distributed and implemented in a way that leaves no doubt about when it is to begin affecting processing. To accomplish these objectives, an entity should have and follow established procedures for announcing approved changes and their implementation dates and for making the revised software available to those who need to begin using it...”.

FISCAM CC-3.2 states that "...Access to software libraries should be protected by the use of access control software or operating system features and physical access controls. Separate libraries should be established for (1) program development and maintenance, (2) user testing, and (3) production. Also, controlled copies of the source versions of all programs (the code created by programmers) should be separately maintained and protected from unauthorized access. If unauthorized modifications are suspected of a production program, the source code can be recompiles to determine what has been changed...”.

FISCAM CC-3.3 states that "...The movement of programs and data among libraries should be controlled by an organization segment that is independent of both the user and the programming staff...”.

FISCAM SC-2.1 states that "...Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions...”.

FISCAM SS-3.1 states that system software changes are authorized, tested, and approved before implementation.

FISCAM SS-3.2 states that "...When possible, the installation of system software changes and new versions or products should be scheduled to minimize the impact on data processing operations, and an advance notice should be provided to system software users...”.

DLMS-9 establishes policy and procedure governing the authorized acquisition, reproduction and distribution or transmission of licensed and copyrighted computer software in the Department of Labor (DOL).

The CSH requires that SSPs address hardware and system software maintenance controls over (1) servicing equipment on-site and off-site (2) documenting changes and approvals, (3) version control process, (4) distribution and implementation of new or revised software.

Effect:

The results of failing to ensure more complete and implemented hardware and system software procedures, especially in the areas of default settings that could easily be compromised and a lack of emergency change procedures could lead to unauthorized access or unanticipated changes to system applications and hardware.

Recommendation:

10 We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet hardware/system software requirements.

Management Comments:

No comment.

Data Integrity

Condition:

The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding data integrity. The OSHANET SSP also provides OSHA with additional guidance in this area. However, the following procedures are not covered by DOL or OSHA:

- Update virus signature files routinely.
- Use integrity verification programs for applications to look for evidence of data tampering, errors, and omissions.
- Investigate inappropriate or unusual activity and take appropriate actions.
- Execute procedures to determine compliance with password policies.
- Install intrusion detection tools on the system.
- Review intrusion detection reports routinely and handle suspected incidents accordingly.
- Perform penetration testing on the system.

OSHA has implemented some data integrity requirements. However, the following procedures have not been implemented.

- Update virus signature files routinely.
- Use reconciliation routines for applications (i.e., checksums, hash totals, record counts)
- Execute procedures to determine compliance with password policies.
- Use integrity verification programs for applications to look for evidence of data tampering, errors, and omissions.

Cause:

OSHA has not developed action plans and assigned the appropriate resources to fully implement data integrity requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, *Government Information Security Reform Act* (GISRA), states that, "... The head of each agency ... (A) adequately ensuring the integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting agency operations and assets; (B) developing and implementing information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of the harm resulting from unauthorized disclosure, disruption, modification, or destruction of information collected or maintained by or for the agency..."

OMB Circular No A-130 states "... 'adequate security' means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, availability, through the use of cost-effective management, personnel, operational and technical controls..."

FISCAM SS-2.2 states that inappropriate or unusual activity should be investigated and appropriate actions taken details the policies and procedures that should be taken when inappropriate or unusual activity occur which may contribute to data integrity issues.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, is a comprehensive document that details the policies that should be enforced in regards to securing information technology systems and promoting data integrity.

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, advises that the determination of adequate controls over data integrity requires answers to whether "...Integrity verification programs [are] used by applications to look for evidence of data tampering, errors, and omissions? (Techniques include consistency and reasonableness checks and validation during data entry and processing) ...whether the "...access control mechanisms support individual accountability and audit trails (e.g., passwords are associated with a user identifier that is assigned to a single individual)..."and whether "...system performance monitoring [is] used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?..."

Effect:

The lack of effective data integrity controls could pose security vulnerability through:

- Inaccurate or missing data resulting from unauthorized destruction or tampering of electronic files and records.
- Access to proprietary or sensitive data by unauthorized personnel.

Recommendation:

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet data integrity requirements.

Management Comments:

Condition:

- a. The opening sentence states that "The CSH, DLMS-9, and the SDLCM provide policy and some procedural guidance to the DOL agencies regarding data integrity. Yet, there are no supporting citations from these sources listed under the Criteria section. Is this true? We recommend that "some" be moved from before "procedural" to before "policy."
- b. We disagree with the first bullet under paragraph two. OSHA has implemented procedures to routinely update virus signature files on the OSHANET.

NIST Self-Assessment Guide for Information Technology Systems (Section 4.2.7)

Documentation

Condition:

The CSH and DLMS-9 provide policy and procedural guidance to the DOL agencies regarding documentation requirements. SSPs for OSHANET, IMIS, and CHIS also provide OSHA with additional guidance in this area. However, there are no DOL or OSHA procedures requiring the following:

- Standard operating procedures exist for all the topic areas covered in the NIST Self-Assessment Guide.
- Emergency procedures.
- Contingency plans.
- Certification and accreditation documents and statements authorizing the systems to process.
- Network diagrams and documentation on setups of routers and switched.
- Software and hardware testing procedures and results.

OSHA has implemented some of the documentation requirements. However, OSHA has not completed the following documentation:

- Standard operating procedures exist for all the topic areas covered in the NIST Self-Assessment Guide.
- Emergency procedures.
- Contingency plans.
- Certification and accreditation documents and statements authorizing the systems to process.

Cause:

Information security personnel are in the process of enhancing current security policy, procedures and other applicable security documentation. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement data integrity requirements.

Criteria:

OMB Circular A-130, regarding how agencies will ensure security in information systems, states that agencies must "...incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning...".

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that "...Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures...".

NIST Special Publication 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that "...Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently...".

Effect:

Lack of documentation can lead to difficulty in supporting and enhancing OSHA's systems in the future. The lack of complete documentation could also lead to incomplete security policy and procedure functionality being followed, thus leaving the system vulnerable to threats. In addition, if updated and consistent security documentation is not available for access, users may involuntarily compromise OSHA's security practices, thus leaving its systems unsecured and susceptible to various vulnerabilities and threats, both internal and external.

Recommendation:

12

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet documentation requirements.

Management Comments:

Condition: The opening sentence reads, "the CSH and DLMS-9 provide policy and procedural guidance to the DOL agencies regarding documentation requirements. Is this true? To which DLMS-9 does this refer? Was it fully in place prior to this review, and in sufficient time to allow agencies to comply, or was it in clearance? It is not listed in the Criteria section. Do the policy and procedural guidance in place during this review detail the specific documentation requirements?"

**Security Awareness,
Training and
Education**

Condition:

The CSH provides policy and procedural guidance to the DOL agencies regarding security awareness, training, and education. The CSH is available to all DOL employees through the LaborNet intranet. While OSHA has implemented most of the security awareness, training, and education requirements, rules of behavior were not available for CHIS.

Cause:

Until 2000, computer security awareness, training, and education was addressed locally. There was no agency-wide, formalized effort, with clear policy and procedural guidance.

Criteria:

OMB Circular A130 states that training should be provided to "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system. In addition, this circular requires that agencies "...Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system... Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system...".

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that "...A set of rules of behavior must be established for each system.... The rules of behavior should be made available to every user prior to receiving authorization for access to the system. It is recommended that the rules contain a signature page for each user to acknowledge receipt...".

The CSH requires rules of behavior for all systems. The CSH states that the rules of behavior should clearly delineate responsibilities and expected behavior of all individual with access to each agency system and must define the consequences of behavior not consistent with the rules of behavior.

Effect:

Without enforcing the requirements for rules of behavior, OSHA employees may not be fully aware of their responsibilities relative to the security of OSHA's sensitive systems.

Recommendation:

We recommend that OSHA implement the rules of behavior for CHIS.

Management Comments:

**Incident Response
Capability**

Condition:

The Department of Labor (DOL) Chief Information Officer (CIO) Computer Security Handbook (CSH) and OSHA's OSHANET SSP provide policy and some procedural guidance to the DOL agencies regarding incident response capability. However, the CSH and OSHA procedures do not specifically require:

- Training personnel to recognize and handle incidents.
- Modifying incident responsibility capability procedures and control techniques after an incident takes place.
- Sharing incident information and common vulnerabilities or threats with other organizations with interconnected systems.
- Reporting incidents, vulnerabilities, and threats to Federal Computer Incident Response Capability (FedCIRC) and other Federal and local law authorities.

Despite the limited procedures, OSHA has established and maintained a formal incident response capability and process and does monitor and track incidents until resolution. In addition, management recently developed procedures to expedite helpdesk calls deemed to be potential computer security incidents and has recently hired a contractor to evaluate and update the helpdesk Escalation Procedures for Computer Security Incidents. However, OSHA has not:

- Provided training to recognize and handle incidents.
- Established a process to modify incident handling procedures and control techniques after an incident occurs.

Cause:

While OSHA has taken many actions to implement the incident response capabilities, it has not developed action plans and assigned the appropriate resources to fully implement incident response capability requirements.

Criteria:

The FY 2001 Defense Authorization Act, *Government Information Security Reform Act (GISRA)* states agencies must have "...procedures for detecting, reporting, and responding to security incidents, including...notifying and consulting with law enforcement officials and other offices and authorities...".

OMB Circular A-130 requires that agencies establish formal incident response mechanisms and make system users aware of these mechanisms and how to use them. The circular further states that "...To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide...".

FISCAM SP-3.4 requires "...agencies to establish formal incident response mechanisms and to make system users aware of these mechanisms and how to use them...".

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, indicates that "...when faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident...".

**Identification and
Authentication**

Condition:

The CSH and DLMS-9 provide policy and procedural guidance to the DOL agencies regarding identification and authentication requirements. OSHA also provides additional guidance in this area. However, there are no procedures regarding the following requirements:

- Maintain a current list of approved and authorized users, and their access.
- Prohibit access scripts with embedded passwords.
- Disable inactive user identifications disabled after a specified period of time.
- Do not display password when entered.
- Replace vendor-supplied passwords immediately.
- Terminals, workstations, and networked personal computers are not left unattended when the user ID and password are logged in.
- System owners periodically review access authorization listings to determine whether they remain appropriate.
- User IDs and passwords are immediately removed when users no longer need access to the system.

In addition, OSHA has implemented many of the identification and authentication requirements. However, the following requirements have not been implemented:

- Maintain a current list of approved and authorized users, and their access.
- Change passwords at least every 90 days or earlier, if needed.
- Prohibit access scripts with embedded passwords.
- Data owners periodically review access authorization listings to determine whether they remain appropriate.

Cause:

The geographic dispersion of OSHANET is a major contributing factor to the inconsistent implementation of procedures. Since OSHANET is not centrally managed, it has led to difficulty in monitoring the system. Each region has varying levels of resource expertise and sensitivity to security issues, which has led to inconsistencies in the implementation of policies and procedures. While OSHA intends to resolve these problems, it has not has not developed action plans and assigned the appropriate resources to fully implement identification and authentication requirements.

Criteria:

OMB Circular A-130 states that "...individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job..."

FISCAM AC-2.1 states that "...the computer resource owner should identify the specific user or class users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties... The owner should also identify the nature and extent of access to each

resource that is available to each user...". In general, users may be assigned one or more of the following types of access to specific computer resources: read, update, delete, merge, and/or execute.

FISCAM AC-2.2 states that "...Emergency and temporary access authorization is controlled...". Emergency and temporary access authorizations should be "...documented on standard forms and maintained on file, approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period...". The audit techniques include "...review of pertinent policies and procedures, compare a selection of both expired and active temporary and emergency authorizations with a system-generated list of authorized users, and determine the appropriateness of access documentation and approvals and the timeliness of terminating access authorization when no longer needed...".

FISCAM AC-3.2 states that "...Identification is the process of distinguishing one user from all others, usually through the use of user IDs. User IDs are important because they are the means by which specific access privileges are assigned and recognized by the computer. However, the confidentiality of user IDs is typically not protected. Typical controls for protecting the confidentiality of passwords include the following: password selection is controlled by the assigned user, passwords are changed periodically, about every 30 to 90 days, passwords are not displayed when they are entered, minimum character length, at least 6 characters, is set for the passwords so that they cannot be easily guessed, use of names, words, or old passwords within six generations is prohibited, while use of alphanumeric passwords should be encouraged, vendor-supplied passwords are replaced immediately upon implementation of a new system, and individual users are uniquely identified rather than having users within a group share that same ID or password...".

FISCAM AC-3.2 also states that "...to help ensure that passwords cannot be guessed, attempted to log on the systems with invalid passwords should be limited. Typically, potential users are allowed three or four attempts to log on...". Lastly, another technique for reducing the risk of password disclosure is encrypting the password file. Encryption further reduces the risk that the password file could be accessed and read by unauthorized individuals. NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, states that "...identification and authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system...".

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that "...Passwords should be changed periodically...If passwords are used for authentication, organizations should specify Required Attributes. Secure password attributes such as a minimum length of six, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID should be specified and required...".

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that "...Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability...". NIST 800-12 provides ways of improving password security: password generators, limits on log-in attempts, password attributes (e.g., passwords with a certain minimum length, use of special characters, picking passwords that are

not in an on-line dictionary), periodic changing of passwords, and technical protection of the password file (e.g., one-way encryption).

Federal Information Processing Standards Publication 186-1 lays out a standard in the encryption algorithm.

The CSH requires the analysis of identification and authentication controls in the development of SSPs.

Effect:

Password management involves techniques, procedures and mechanisms that adequately protect the system from unauthorized, unlimited access and usage, and enhances the system's security. Poor or inadequate password management leaves the system vulnerable to such access from both internal and external sources. OSHA will need to develop and implement proper password procedures in order to mitigate against such risks.

Recommendations:

We recommend that OSHA take the following actions as soon as possible:

- 15
- A Set and enforce strong password policy--both in writing and by computer configuration
 - B Require users to change passwords every 90 days
 - C Regularly download passwords from the servers and use password cracking software to test the strength of the passwords.

We also recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet identification and authentication requirements.

Management Comments:

Condition: The opening sentence reads, "The CSH and DLMS-9 provide policy and procedural guidance to the DOL agencies regarding identification and authentication requirements." Is this true? To which DLMS-9 does this statement refer? Was the DLMS-9 in place prior to the audit and in time to allow agencies sufficient time to comply, or was it in the clearance process during the audit? Does the CSH specifically list the requirements noted in this section?

**Logical Access
Controls**

Condition:

The CSH and DLMS-9 provide policy and some procedural guidance to the DOL agencies regarding logical access control requirements. In addition, OSHA has established various policies and procedures through the OSHANET SSP regarding logical access controls over agency data. However, the following procedures are not covered by any of the above documents:

- Restrict access to files at the logical view or field.
- Implement communication software to restrict access through specific terminals.
- Disable insecure protocols (e.g., UDP, ftp).
- Reinitialize all vendor-supplied default security parameters to more secure settings.
- Maintain and review network activity logs.
- Automatically disconnect the network connection at the end of a session.
- Restrict trust relationships among hosts and external entities appropriately.
- Monitor dial-in access.

OSHA has implemented many of the logical access controls requirements. However, the following requirements have not been implemented:

- Encryption meets Federal standards.
- Key generation, distribution, storage, use, destruction, and archiving process for encryption.
- Restrict access to files at the logical view or field.
- Implement communication software to restrict access through specific terminals.
- Disable insecure protocols (e.g., UDP, ftp).
- Reinitialize all vendor-supplied default security parameters to more secure settings.
- Maintain and review network activity logs.
- Automatically disconnect the network connection at the end of a session.

Cause:

In the past, OSHA did not have regular technical reviews of their security posture to examine existing and emerging threats to its general support system and associated major applications. Improvements have been made through the development of the OSHANET SSP, which analyze their security needs and provide implementation procedures of various security controls. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement logical requirements.

Criteria:

OMB Circular A-130 states that "...individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job..."

NIST SP 800-18 states that "...Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those

accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users...”

FISCAM AC-3.2 states that “...to ensure that access controls are uniformly administered, the security management function should implement and maintain

logical access controls based upon authorizations from appropriate levels within the entity. ...”

FISCAM SD-2.1 indicates that physical and logical controls should be established. It further states that “...both physical and logical access controls can be used to enforce many entity policies regarding segregation of duties and should be based on organizational and individual job responsibilities...”

The CSH defines logical access controls as “...system-based mechanisms that provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make...”. The CSH states that logical controls should authorize or restrict the activities of users and system personnel within the general support system, permit only authorized access to or within the GSS, restrict users to authorized transactions and functions, and detect unauthorized activities.

Effect:

Results of the penetration test showed that complete compromise of the network is possible when passwords are weak, systems lack current patches, and security controls are inconsistently maintained. The penetration test team was able to remotely command the web server over the internet using a well-known vulnerability with Microsoft's web servers.

Recommendations:

We recommend that OSHA take the following actions as soon as possible:

- 16 a • Regularly scan network for vulnerabilities using automated security scanners.
- b • Review the system's password strength by periodically pulling the encrypted passwords from the systems and running a password cracker against the passwords.
- c • Install third party password restrictive software that will force users to choose good passwords.
- d • Keep systems updated on current security patches and security fixes.

We also recommend that OSHA develop action plans and assign resources to fully implement all remaining logical access control requirements.

Management Comments:

Condition: The opening sentence reads, “The CSH and DLMS-9 provide policy and some procedural guidance to the DOL agencies regarding logical access control requirements.” Is this true? To which DLMS-9 does this statement refer? Was the DLMS-9 in place prior to the audit and in time to allow agencies sufficient time to comply, or was it in the clearance process during the audit? Does the CSH specifically list the requirements noted in this section?

Audit Trails

Condition:

Within the last two years, the Department of Labor (DOL) has issued policies and procedures addressing Audit Trails. For example, the CIO's Computer Security Handbook (CSH) provides audit trail policies and procedures to be followed by the DOL agencies. In addition, OSHA also provides policies and procedures covering this area. However, the following procedures are not covered by DOL or OSHA:

- Ensure separation of duties between security personnel who administer the access control function and personnel who administer the audit trail.
- Review the audit trail logs on a regular and continuous basis.
- Utilize keystroke monitoring.

OSHA has implemented many of the audit trail requirements. However, the following procedures have not been implemented:

- Strictly control access to online audit logs.
- Retain off-line storage of audit logs for a period of time and strictly control access to the audit logs.
- Ensure separation of duties exist between security personnel who administer the access control function and those who administer the audit trail.
- Review audit trails frequently.
- Use automated tools to review audit records in real time or near real time.

Cause:

In the past, OSHA took a reactive rather than a proactive approach to this area. The agency did not have a formal, documented, prevention and detection program, or agency-wide regular technical reviews of its security posture to examine existing and emerging threats to its general support system and associated major applications. Improvements have been made through the development of the OSHANET SSP, which analyze their security needs and provide implementation procedures of various security controls. However, OSHA has not developed action plans and assigned the appropriate resources to fully implement logical requirements.

Criteria:

The FY 2001 Defense Authorization Act, Section X, Subtitle G, Government Information Security Reform Act (GISRA) states that the head of each agency shall develop and implement an agency-wide information security program to include "procedures for detecting, reporting, and responding to security incidents..." (emphasis added).

FISCAM AC-4 states that "...security software generally provides a means of determining the source of a transaction of an attempted transaction and of monitoring users' activities (the audit trail). However, to be effective (1) this feature should be activated to maintain critical audit trails and report unauthorized or unusual activity and (2) managers should review and take action on these reports..."

NIST Special Publication 800-18: *Guide for Developing Security Plans for Information Technology Systems*, states that agencies should have "...Audit trails maintain a record of system activity by system or application processes and by user activity...[and should consider whether]...(1) the audit trail support[s] after-the-fact investigations of how, when, and why normal

operations ceased ... (2) the audit trail provide[s] accountability by providing a trace of user actions... (3) access to online audit logs [is] strictly controlled... (4) ... separation of duties between security personnel who administer the access control function and those who administer the audit trail [exists] and (5) how frequently audit trails are reviewed and whether there are review guidelines...".

NIST 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, states that "...audit trails maintain a record of system activity by system or application processes by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification...".

NIST 800-12, *An Introduction to Computer Security: The NIST Handbook*, states that "...an audit trail should include sufficient information to establish what events occurred and who (or what) caused them...". An event record should specify what event occurred, the User ID associated with the event, the program or command used to initiate the event, and the result.

The CSH states that "...audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. Audit trails provide a means to accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis...". Audit trails should provide accountability to users for their actions such as type of event, when the event occurred, the user ID associated with the event, and the program and command used to initiate the event.

Effect:

The penetration test team was able to remotely command the web server over the internet using a well-known vulnerability with Microsoft's web servers. Once administrative control is gained on the servers log files can be modified and deleted. With no intrusion detection system an organization's network can be compromised without ever knowing (i.e., no audit trails).

Without appropriate audit trail procedures, OSHA security is susceptible to unauthorized access to sensitive audit information and unauthorized modification or deletion of audit log information. If audit logs are not reviewed on a regular and continuous basis, system administrator will be unable to detect or recognize incidents or vulnerabilities in a timely manner. Because of its minimal compliance with the audit trail control requirements, OSHA's systems are vulnerable to user misuse and other security compromises.

Recommendations:

We recommend that OSHA independently test and implement an intrusion detection system as soon as possible.

We recommend that OSHA assign appropriate resources and develop and implement action plans to fully meet audit trail requirements.

Management Comments: No Comment.