

Office of Inspector General

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

Government Information Security Reform Act (GISRA) Evaluation of ESA's OFCCP Information System

This report was prepared by KPMG 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: 23-01-008-04-001
Date Issued: September 25, 2001

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION	4
Background	4
Objective, Scope and Methodology	4
FINDINGS AND RECOMMENDATIONS	6
High Priority Control Issues	7
Moderate Priority Control Issues	16
ACRONYMS	21
APPENDIX	
Management Response to Tentative Findings and Recommendations	A

EXECUTIVE SUMMARY

The Department of Labor (DOL), Office of Inspector General (OIG), has contracted with KPMG LLP, to perform an independent evaluation of information security programs and practices within DOL's Employment Standards Administration's (ESA) Office of Federal Contract Compliance Programs (OFCCP). This evaluation was conducted pursuant to guidance articulated by the Office of Management and Budget (OMB) and the National Institute for Standards and Technology (NIST), in order to satisfy OIG reporting requirements under Title X, Subtitle G of the 2001 Defense Authorization Act, the Government Information Security Reform Act (GISRA).

The purpose of this review was to assess the OFCCP security program and OFCCP Information System (OFIS). The evaluation team was guided in their assessment by standards and policies set forth by NIST in support of the Security Act, as well as other key authoritative sources of guidance for accessing Federal information security programs.

Positive Security Control Observation

To improve its security, OFCCP has implemented portions of a System Development Life Cycle (SDLC) methodology into the development of its systems. OFCCP anticipates that the SDLC methodology will also be integrated into OFCCP's security program plan.

Summary of Findings and Recommendations

A Tentative Findings and Recommendations (TFAR) document was issued to the OFCCP Management on August 16, 2001. ESA's Acting Assistant Secretary provided written responses to each of the evaluation's tentative findings. Management's comments are summarized in each finding and are included in their entirety in Appendix A of this report.

ESA management did not concur with all of our findings. We evaluated their response to our findings and concluded there was no additional evidence presented that would change our findings and recommendations. The findings, which need to be addressed by the Agency Head, are presented below:

High Priority Control Issues: We identified five high priority control issues during our evaluation. High priority control issues are defined as findings that present a level of risk that requires immediate address by OFCCP management.

1. The OFIS application security plan is not application specific. Additionally, it has not been updated to reflect results of the current Risk Assessment.

Recommendation: Update the application security plan to reflect the attributes of the OFIS application's specific requirements.

2. The appropriate level of security for the OFIS system has not been established based on the current risk assessments.

Recommendation: Update the controls over the OFIS system based on a predetermined level of risk.

3. The risk assessment that was performed on the OFIS application does not address risk at an application level. In addition, the assessment only addresses risk in monetary terms and does not take into account qualitative attributes such as program responsibilities and reputation.

Recommendation: Supplement the current risk assessment with an application specific risk assessment. This assessment should include quantitative and qualitative factors.

4. The current ESA Disaster Recovery plan is designed for the Year 2000 contingency, not for the current environment. The OFIS system uses this non-current plan as a basis for its business continuity planning.

Recommendation: Develop and implement a disaster recovery program that would enable it to provide an appropriate level of service continuity for all its systems, including OFIS.

5. There is no formal computer security incident procedure in place that enables computer incidents to be reported to the OCIO.

Recommendation: Develop and implement an agency incident response capability. This capability should comply with the DOL Computer Security Handbook guidelines on incident reporting.

Moderate Priority Control Issues: The remaining three control issues were identified as moderate priority. Moderate priority control issues are conditions that present a level of risk that should be corrected by OFCCP management in a timely manner.

6. ESA Security Awareness program has not been fully implemented. In addition, the program does not include employees with specific security responsibilities.

Recommendation: Ensure that the ESA security awareness program is fully implemented and all OFCCP employees receive the appropriate training level based on their responsibilities and job description.

7. Based on discussions with OFCCP officials, OFCCP employees, in general, use the same Network Application IDs and passwords.

Recommendation: Perform a risk based security assessment to determine and implement additional safeguards to the protect OFIS information.

8. Database audit trail reports are not being monitored on a regular basis.

Recommendation: Ensure that routine monitoring of the OFIS database audit trail logs are conducted. The logs will help identify issues that may affect database integrity and overall system security.

INTRODUCTION

Background

Office Federal Contract Compliance Program

The OFCCP is part of the U.S. Department of Labor's Employment Standards Administration (ESA). It has a national network of six regional offices, each with district and area offices in major metropolitan centers. OFCCP administers and enforces all laws pertaining to Federal Government Contractors. OFCCP also shares enforcement authority under Title I of the Americans with Disabilities Act and the Immigration Reform Control Act.

The OFIS is OFCCP's automated tool used to collect, manage, track, plan and report on compliance evaluations and compliant investigations that the OFCCP conducts to ensure the laws that the program administers are enforced. OFIS subsystems include the Case Management System (CMS) and the Executive Information System (EIS).

The OFIS environment is primarily a distributed client-server open architecture made up of various components shared by all entities within the organization. Components include desktops, LANS and various servers providing a multitude of services. The entire infrastructure is tied together by a Wide Area Network which establishes the distributed environment allowing users access to common services as well as mission-related applications required as part of their job responsibilities. OFIS is accessible by way of the ESA General Support System (ESA-GSS). Through the ESA-GSS, ESA is responsible for network security controls over the OFIS application. OFCCP is responsible for the security controls related to the specific OFIS applications. The predominance of OFIS users are located at the National Office in Washington, DC. The remaining users are located in the regional offices of OFCCP and supported by the ESA-GSS as well.

Objective, Scope and Methodology

The objective of this evaluation was to perform an independent evaluation of the OFIS application's security program through a critical examination of the programs security and security-related documents and internal correspondence, and through interviews with knowledgeable OFCCP personnel.

Our evaluation assessed the management, operational and technical security controls that relate to the OFCCP application. The examination was performed in DOL's Washington, D.C., headquarters from June 14, 2001 through August 10, 2001. The evaluation was made in accordance with guidance contained in OMB Memorandum 01-08, Guidance on Implementing the Government Information Security Reform Act (GISRA), dated January 16, 2001, and OMB Memorandum 01-24, Reporting Instructions for the Government Information Security Reform Act, dated June 22, 2001.

The evaluation was performed using draft guidance set forth in the NIST Self-Assessment Guide for Information Technology Systems. The Self-Assessment Guide provides a methodology for evaluating an agency information technology security program and is intended to facilitate improvement. The guide consists of an extensive questionnaire containing specific control objectives that collectively constitute the minimum components of an effective information security program. The guide does not establish new security standards or requirements. The control objectives in the questionnaire are drawn directly from long-standing requirements found in Federal law, regulatory and technical criteria, and guidance on security and privacy.

FINDINGS AND RECOMMENDATIONS

The following section describes the findings and recommendations that have been identified during the fieldwork of the OFCCP's OFIS GISRA evaluation. Each finding includes a description of the condition, the cause of the condition, the criteria against which the condition was identified (e.g., NIST, GAO, OMB, etc.), the potential effects, and a recommendation to address the condition. Additionally, the related OMB requirement is referenced in order to facilitate the OIG reporting requirement process.

We have identified eight findings as they relate to the OMB Reporting Requirements. Five of the findings have been classified as "High Priority Control Issues" and three were classified "Moderate Priority Control Issues."

High Priority Control Issues: The identified condition presents a level of risk that requires immediate address by OFCCP management.

Moderate Priority Control Issues: The identified condition presents a level of risk that should be corrected by OFCCP management in a timely manner.

A description of the high and moderate priority control issues, ESA management comments, and our response to management's comments are included in the following pages:

High Priority Control Issues

Number of Findings: 5

High Priority Control Issues

References	Finding and Recommendation
<p>Recommendation # 1</p> <p>OMB Reporting Requirement (s): II.B5, II.B6, II.B11 and II.B12</p>	<p>Condition: The OFCCP security program plan is incomplete, specifically in the areas of disaster recovery and incident response. In addition, the OFCCP application security plan is not application specific and does not address security throughout the life cycle of the application. The security plan has not been updated to reflect results of their current Risk Assessment.</p> <p>Cause: The security plan was completed using the ESA agency security plan as a template and was not modified sufficiently to reflect specific application attributes.</p> <p>Criteria: Office of Management and Budget (OMB) Circular A-130, “Management of Federal Information Resources” Appendix III, “Security of Federal Automated Information Resources” A-130, states that agencies should: “Plan for adequate security of each general support system as part of the organization’s information resources management (IRM) planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST).”</p> <p>Effect: The lack of a complete security program plan exposes an agency’s information resources to major damage, loss or harm.</p> <p>Recommended Corrected Action: We recommend the Agency Head update the application security plan to reflect the attributes of the OFIS application’s specific requirements.</p> <p>Management’s Comments: The Security Program Plan for ESA exists at the Agency level and covers all systems within the Agency. ESA does not concur that the plan is incomplete. The Agency Security Program Plan does cover plans to better address both disaster recovery and incident response capability for all systems within ESA, including the systems being reviewed. These plans are currently underway, and timelines were provided to the audit staff in the Agency Security Program Plan.</p>

<p>Finding # 1 (Continued)</p>	<p>ESA concurs that the OFCCP system security plan is not adequately application specific and needs to better reflect specific application attributes. ESA has in its Agency Security Program Plan timeframes established to update these plans and will address this issue during those revisions.</p> <p>Conclusion: We do not concur with ESA’s response regarding the completeness of the ESA security program plan. However, we recognize ESA’s efforts to implement disaster recovery and incident response capabilities. The fact that the disaster recovery and incident response capabilities are not fully implemented or in place indicates that the security plans are not complete.</p> <p>We concur with ESA comments regarding the OFCCP security program plans not being application specific.</p> <p>We do not concur with ESA’s comments regarding the incorporation of the system risk assessment results into the system security plan. There was evidence that there were minor changes made to the risk assessments prior to them being officially issued. However, there is no evidence that the results of the risk assessments were incorporated into the system security plan. Overall, we could not verify that the security plans were developed using a risk based approach.</p>
---	--

References	Finding and Recommendation
<p>Recommendation #2</p> <p>OMB Reporting Requirement (s): II.B5 and II.B10</p>	<p>Condition: The appropriate level of security for OFCCP’s OFIS system has not been established based on the current risk assessment. ESA has chosen a standard level of security for all its systems (this includes OFIS). Additionally, no formal methodology was used to implement the appropriate level of security into the OFIS system.</p> <p>Cause: The program risk assessment does not properly identify risk areas that are used to determine the level of security appropriate to protect OFCCP operations and assets. No additional risk assessments were performed that would identify qualitative risk elements that could supplement the financial based risk assessment.</p> <p>Criteria: <i>OMB Circular A-130, Appendix III</i>, provides guidance on adequate security. It defines adequate security as, “Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.” This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.</p> <p>Effect: Not applying the appropriate level of security based on risk may increase the likelihood of unintentional or intentional damage to OFCCP IT resources.</p> <p>Recommended Corrected Action: We recommend the Agency Head update the controls over the OFIS system based on a predetermined level of risk.</p> <p>Management’s Comments: ESA does not concur that appropriate levels of security for OFIS has not been established. While perhaps not appropriately documented in the system security plan for the application, the security levels for the systems were determined during the development of these applications. Additional controls exist within each application, which provide additional levels of technical, and personnel controls based on the risks associated with the nature of the business each system supports.</p>

<p>Finding #2 (Continued)</p>	<p>Additionally, in early February 2000 using the guidance in NIST 800-18, ESA management (both DITMS and Programs) met to evaluate the level of confidentiality, integrity and availability of these systems and concluded that the current process of establishing a minimum standard set of controls coupled with the additional controls developed into each of the applications was a rational and adequate approach.</p> <p>ESA does agree that the application-specific security plans need to better reflect the additional security measures taken into account and implemented in the development of those systems as well as any other considerations being planned for. ESA will revise these security plans in accordance with the timeframes established in the Agency Security Program Plan.</p> <p>Conclusion: We do not concur with ESA management comments regarding the appropriate level of security for OFCCP's systems. During our review, there was no evidence provided to substantiate that a risk based approach was used to determine the appropriate level of security for OFCCP's systems. We do recognize that there may be adequate controls and security in place for OFCCP's systems. However, that cannot be verified because the process for determining the appropriate level of security was not documented.</p> <p>We concur with ESA's comments regarding the lack of application specific security measures for the OFCCP systems.</p>
--	---

References	Finding and Recommendation
<p>Recommendation # 3</p> <p>OMB Reporting Requirement(s): II.B5 and II.B10</p>	<p>Condition: The risk assessment that was performed on the OFIS application does not address risk at an application level. In addition, the assessment only addresses risk in monetary terms and does not take into account qualitative attributes such as image and reputation.</p> <p>Cause: The application risk assessment was performed at a program level and its methodology was designed to provide risk at a high level in monetary terms.</p> <p>Criteria: <i>OMB Circular A-130, Appendix III</i>, provides guidance on adequate security. It defines adequate security as security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.</p> <p><i>NIST Pub 800-18</i> states: "In every assessment of risk, there will be many areas for which it will not be obvious what kind of controls are appropriate. Even considering only monetary issues, such as whether a control would cost more than the loss it is supposed to prevent, the selection of controls is not simple. However, in selecting appropriate controls, managers need to consider many factors, including: organizational policy, legislation, and regulation; safety, reliability, and quality requirements; system performance requirements; timeliness, accuracy, and completeness requirements; the life cycle costs of security measures; technical requirements; and cultural constraints."</p> <p>Effect: A risk assessment at the program level may not adequately depict risk at the application level. Security and controls over the application may be inadequate, possibly exposing the asset to loss or damage.</p> <p>Recommended Corrected Action: We recommend the Agency Head supplement the current risk assessment with an application specific risk assessment. This assessment should include quantitative and qualitative factors.</p>

<p>Finding # 3 (Continued)</p>	<p>Management's Comments:</p> <p>The OFCCP risk assessment for the OFIS system does address risk at the application level. The risk assessment was acceptable under the Department's FY 2000 risk assessment planning guidelines. ESA agrees that the tool used to develop the risk assessments did not provide qualitative attributes. In developing new assessments of these systems, as scheduled in ESA's Agency Security Program Plan, ESA will use the guidance provided in the latest version of Office of Management and Budget (OMB) Circular A-130, Appendix III. This revision calls for a more risk-based approach to evaluating system security, as opposed to performing costly formal risk assessments, which OMB recognizes as providing "limited tangible benefit in terms of improved security of the systems" and are no longer required under the current guidelines.</p> <p>Conclusion:</p> <p>We agree that the risk assessment may be in accordance with the Department of Labor's guidance. However, we do not concur with comments indicating that the risk assessments were application specific. Specifically, there were no qualitative system specific related attributes addressed within the current risk assessments.</p>
---	---

References	Finding and Recommendation
<p>Recommendation #4</p> <p>OMB Reporting Requirement (s): II.B5 and II.B6</p>	<p>Condition: OFCCP has no formal disaster recovery program in place to ensure service continuity over its information system resources.</p> <p>Cause: The current ESA Disaster Recovery plan is designed for Y2K contingency. Additionally, OFCCP's system security plan uses this as a basis for providing service continuity for their systems.</p> <p>Criteria: The Federal Information Processing Standards (FIPS pub) number 73 states: "Contingency plans should be developed to assure the integrity of the data processed and the continuity of the application's critical functions. The plan must be implemented (i.e., the prerequisite activities such as training of personnel, alternate site selection, selection of backup file storage site, determination of critical functions, etc. must be completed) and maintained in a state of readiness so that responses to emergencies will be timely and successful."</p> <p>Effect: Without a current disaster recovery program, OFCCP and its applications may experience service interruptions that may adversely affect their reputation, capital and the ability to fulfill OFCCP's business objectives.</p> <p>Recommended Corrected Action: We recommend the Agency Head develop and implement a disaster recovery program that would enable it to provide an appropriate level of service continuity for all its systems, including OFIS.</p> <p>Management's Comments: Service continuity of the OFCCP information systems resources are currently covered by ESA's 2000 Business Continuity and Contingency Plan (BCCP). ESA is in the process of enhancing and expanding this Plan and currently has the resources on-board doing this work. As noted in ESA's Agency Security Program Plan, the revisions to the 2000 BCCP are due to be completed by January 30, 2003.</p> <p>Conclusion: We recognize ESA's initiatives to improve their disaster recovery capability. We concur with their comments and encourage them to continue their efforts.</p>

References	Finding and Recommendation
<p>Recommendation #5</p> <p>OMB Reporting Requirement(s): II.B5, II.B6, and II.B8</p>	<p>Condition: OFCCP has no formal computer security incident response capability in place that enables computer incidents to be reported to the Office of Chief Information Officer (OCIO).</p> <p>Cause: The procedures in the DOL Computer Security Handbook, Chapter 5, are not being followed, specifically, in regards to reporting incidents to the OCIO.</p> <p>Criteria: <i>OMB Circular A-130, Appendix III</i>, states an agency shall: “Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.”</p> <p>Effect: Without a formal incident response capability, OFCCP will not be able to respond quickly in a manner that protects both its own information and others that may be affected by that information.</p> <p>Recommended Corrected Action: We recommend the Agency Head develop and implement an agency incident response capability. This capability should comply with the DOL Computer Security Handbook guidelines on incident reporting.</p> <p>Management’s Comments: ESA is in the process of finalizing its formal computer security incident response policy and procedures. This policy and the accompanying procedures, as outlined in ESA’s Agency Security Program Plan, will be published by no later than September 30, 2001. Additionally, OFCCP will provide interim security incident response procedures this month.</p> <p>Conclusion: We concur with the comments made by ESA management and encourage their continued efforts to strengthen their computer security program.</p>

Moderate Priority Control Issues

Number of Findings: 3

Moderate Priority Control Issues

References	Finding and Recommendation
<p>Recommendation # 6</p> <p>OMB Reporting Requirement (s): II.B5, II.B7, and II.B13</p>	<p>Condition: The ESA security awareness program has not been fully implemented. Seventy percent of the ESA national office staff have been trained to date (includes OFCCP). In addition, OFCCP employees with specific security responsibilities have not been trained on their specific duties.</p> <p>Cause: The policy and procedures for implementing an agency-wide security awareness program have only recently been developed. There is no formal policy or procedure to train employees with specific security responsibilities.</p> <p>Criteria: <i>OMB Circular A-130, Appendix III</i>, states an agency shall: “Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.”</p> <p>Effect: Employees who have not been sufficiently trained on their security responsibilities may unintentionally misuse or damage agency IT resources.</p> <p>Recommended Corrected Action: We recommend the Agency Head ensure that the ESA security awareness program is fully implemented and all OFCCP employees receive the appropriate training level based on their responsibilities and job description.</p> <p>Management’s Comments: ESA is in the process of completing its FY 2001 security awareness training plan, which covers all ESA employees and contractors, nationwide. As of the date of this report, over 90% of OFCCP national office employees, and 78% of all OFCCP employees have been trained. ESA is in the process of completing its’ long-range computer security awareness training plan, which will be completed by September 30, 2001.</p>

<p>Finding #6 (Continued)</p>	<p>Employees with specific security responsibilities, such as Program Security Officers, have been and will continue to receive training on their specific duties and responsibilities. Security Officers were given a briefing on their responsibilities during a June meeting of ESA Security Officers; additional topics will be covered during the August meeting. ESA's long-range security awareness training plan will encompass specific training for employees with security responsibilities.</p> <p>Conclusion: ESA has taken significant steps to fully implementing their Security Training program. We encourage them to continue in their efforts. However, there was no evidence presented that verifies that OFCCP employees with significant security responsibilities were formally trained in their duties.</p>
--	--

References	Finding and Recommendation
<p>Recommendation #7</p> <p>OMB Reporting Requirement (s): II.B5</p>	<p>Condition: Based on discussions with OFCCP officials, OFCCP employees, in general, use the same Network and OFIS Application IDs and passwords.</p> <p>Cause: ESA does not enforce its policy that instructs employees to use different network and application IDs and passwords. A formal risk based approach to developing security and controls over the OFIS application was not performed.</p> <p>Criteria: <i>OMB Circular A-130, Appendix III</i>, provides guidance on adequate security. It defines adequate security as, “Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.” This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.</p> <p>Effect: A user’s password and ID could be obtained by an unauthorized individual and grant them access to the application and database.</p> <p>Recommended Corrected Action: We recommend the Agency Head perform a risk based security assessment to determine and implement additional safeguards to the protect OFIS information.</p> <p>Management’s Comments: While users can make their Network and Application passwords the same, the two ID/password repositories are physically separate. ESA believes this can be addressed primarily through user awareness training, but will look at other policy compliance methodologies as well.</p> <p>Conclusion: We recognize ESA plans to reinforce existing policies and concur with their comments.</p>

References	Finding and Recommendation
<p>Recommendation # 8</p> <p>OMB Reporting Requirement (s):</p> <p>II.B5</p>	<p>Condition: OFCCP database audit trail reports are not being monitored on a regular basis.</p> <p>Cause: OFCCP does not have a policy or procedure that requires routine monitoring of its system’s database audit trail log.</p> <p>Criteria: As a best practice, the <i>NIST pub 800-12</i>, advises that audit trail logs be monitored on a regular basis. It states “Audit trails are a technical mechanism that help managers maintain individual accountability. By advising users that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.”</p> <p>Effect: The lack of routine monitoring of audit trail reports may result in unintentional, intentional, or undetected corruption of database elements. Monitoring serves as a preventative or detective control that would enable OFCCP to protect their information resources.</p> <p>Recommended Corrected Action: We recommend the Agency Head ensure that routine monitoring of the OFIS database audit trail logs are conducted. The logs will help identify issues that may affect database integrity and overall system security.</p> <p>Management’s Comments: ESA concurs that better monitoring of audit trail reports will help to ensure the integrity and security of OFCCP systems. ESA will investigate methods for performing better auditing and monitoring of these systems and ensure that procedures are developed which require a more routine monitoring of these systems.</p> <p>Conclusion: We encourage ESA to continue in their efforts to improve computer security and concur with their comments.</p>

ACRONYMS

DOL	Department of Labor
EEO	Equal Employment Office
ESA	Employment Standards Administration
FIPS PUB	Federal Information Processing Standards Publication
GAO	General Accounting Office
GISRA	Government Information Security Reform Act
GSS	General Support System
IRM	Information Resource Management
IT	Information Technology
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OFCCP	Office of Federal Contract Compliance Programs
OFIS	OFCCP Information System
OIG	Office of Inspector General
OMB	Office of Management Budget
SDLC	Systems Development and Life Cycle

U.S. Department of Labor

Assistant Secretary for
Employment Standards
Washington, D.C. 20210



AUG 27 2001

MEMORANDUM FOR ROBERT W. CURTIS
Director, Office of Information
Technology Audits, OIG

FROM:


JOE N. KENNEDY
Acting Assistant Secretary

SUBJECT:

Tentative Findings and Recommendations
Government Information Security Reform Act (GISRA)
Evaluation of ESA's OFCCP Information System (OFIS)
And Wage and Hour Division's Electronic Services
Contract Act Notification System (ESCANS2) and Wage
Determination Generation System (WDGS)

This is in response to your August 16, 2001 memorandum requesting comments on the subject reports. We have reviewed the findings and recommendations for both reports, and our response to each of the five high-priority, and three medium-priority recommendations, which your office provided as part of its GISRA Evaluation, is attached. Please note that because the findings were the same for both the Office of Federal Contract Compliance Programs (OFCCP) and the Wage and Hour Division (WHD), ESA is providing a joint response on the findings and recommendations. It is understood that both WHD and OFCCP have the responsibility to work with the Division of Information Technology and Management Systems (DITMS) to address all of the findings related to their specific applications.

It should be noted that the correct name of the WDGS System is Wage Determination Generation System not Wage Decision Generation System. Additionally, in the WHD report, KPMG's audit team corrected the terms used to describe the priority of the recommendations (high-priority and medium-priority); this still needs to be corrected in the OFIS report. The reports also need to be reviewed for accuracy, as the OFIS report contains references to WHD.

ESA would like to take this opportunity to commend the KPMG audit staff who are working on this evaluation. Their professional, courteous, and responsive manner has engendered a cooperative working relationship with ESA staff and has resulted in recommendations which will allow ESA to ensure the security of its information and information systems.

We understand that the tentative findings and recommendations are subject to revision before being incorporated into a draft report. If you have any questions on these responses, please contact Mary Cline-Buso at 693-0249 or Rose Broadwater of my staff at 693-0285.

Attachment

**ESA RESPONSE TO OIG TENTATIVE FINDINGS AND
RECOMMENDATIONS (TFARS)**

**Government Information Security
Reform Act (GISRA) Evaluation of the
Employment Standards Administration's
Office of Federal Contract Compliance Program's Information System (OFIS) and
Wage and Hour Division's Electronic Services Contract Act Notification System
(ESCANS2) and Wage Determination Generation System (WDGS)**

The following is a detailed response to each of the five high-priority, and three medium-priority recommendations which the OIG provided as part of its GISRA Evaluation. Because the findings were the same for both Office of Federal Contract Compliance Programs (OFCCP) and the Wage and Hour Division (WHD), ESA is providing a joint response on these findings. It is understood that both WHD and OFCCP have the responsibility to work with the Division of Information Technology and Management System (DITMS) to address all of the findings related to their specific applications.

Finding and Recommendation 1:

The OFCCP and WHD security program plans are incomplete, specifically in the areas of disaster recovery and incident response. In addition, the OFCCP and WHD application security plans are not application specific and do not address security throughout the life cycle of the applications. The security plans have not been updated to reflect results of the current Risk Assessment. It is recommended that application security plans be updated to reflect the attributes of the application's specific requirements.

Management's Response:

The Security Program Plan for ESA exists at the Agency level and covers all systems within the Agency. ESA does not concur that this plan is not complete. The Agency Security Program Plan does cover plans to better address both disaster recovery and incident response capability for all systems within ESA, including the systems being reviewed. These plans are currently underway, and timelines were provided to the audit staff in the Agency Security Program Plan.

ESA concurs that the OFCCP and WHD system security plans are not adequately application specific and need to better reflect specific application attributes. ESA has in its Agency Security Program Plan timeframes established to update these plans and will address this issue during those revisions.

ESA does not concur with the finding that the security plans have not been updated to reflect the results of the most recent risk assessments. As shown in evidence to the auditors, the only changes between the original risk assessments and the most recent copies of the assessments were of a cosmetic nature; no changes of substance were made to the risk assessments.

Finding and Recommendation 2:

The appropriate levels of security for OFCCP's OFIS and WHD's ESCANS2 and WDGS systems have not been established based on the current risk assessments. ESA has chosen a standard level of security for all its systems. This standard was adopted using no formal methodology to assess the appropriate level of security. It is recommended that controls over WDGS and ESCANS2 and OFIS be updated based on the level of risk.

Management's Response:

ESA does not concur that appropriate levels of security for OFIS and ESCANS2 and WDGS have not been established. While perhaps not appropriately documented in the system security plans for these applications, the security levels for these systems were determined in the development of these applications. Additional controls exist within each application, which provide additional levels of technical and personnel controls based on the risks associated with the nature of the business each system supports. Additionally, in early February 2000, using the guidance in NIST 800-18, ESA management (both DITMS and Programs) met to evaluate the level of confidentiality, integrity, and availability of these systems. As a result, ESA concluded that the current process of establishing a minimum standard set of controls, coupled with the additional controls developed into each of the applications, was a rational and adequate approach.

ESA does agree that the application-specific security plans do need to better reflect the additional security measures taken into account and implemented in the development of those systems, as well as any other considerations being planned. ESA will revise these security plans in accordance with the timeframes established in the Agency Security Program Plan.

Finding and Recommendation 3:

The risk assessments that were performed on OFIS and WDGS and ESCANS2 applications do not address risk at an application level. In addition, the assessments only address risk in monetary terms and do not take into account qualitative attributes such as image and reputation. It is recommended that current risk assessments be supplemented with an application specific risk assessment. This assessment should include quantitative and qualitative factors. It is recommended that the current risk assessment be supplemented with an application-specific risk assessment. This assessment should include quantitative and qualitative factors.

Management's Response:

The OFIS risk assessment does address risk at the OFIS level, while the WHD risk assessment was for the Wage and Hour Division. Both were acceptable under the Department's FY 2000 risk assessment planning guidelines. ESA agrees that the tool used to develop the risk assessments did not provide qualitative attributes. In developing new assessments of these systems, as scheduled in ESA's Agency Security Program Plan, ESA will use the guidance provided in the latest version of Office of Management and Budget (OMB) Circular A-130, Appendix III. This revision calls for a more risk-based approach to evaluating system security, as opposed to performing costly formal risk assessments which OMB recognizes as providing "limited tangible benefit in terms of improved security of the systems" and are no longer required under the current guidelines.

Finding and Recommendation 4:

OFCCP and WHD have no formal disaster recovery program in place to ensure service continuity over their information systems resources. It is recommended that a disaster recovery program be developed and implemented that would enable it to provide an appropriate level of service continuity for all its systems, including WDGS and ESCANS2 and OFIS.

Management's Response:

Service continuity of the OFCCP and WHD information systems resources are currently covered by ESA's 2000 Business Continuity and Contingency Plan (BCCP). ESA is in the process of enhancing and expanding this Plan and currently has the resources on board doing this work. As noted in ESA's Agency Security Program Plan, the revisions to the 2000 BCCP are due to be completed by January 30, 2003.

Finding and Recommendation 5:

There is no formal computer security incident response capability in place that enables computer incidents to be reported to the Office of the Chief Information Officer (OCIO). It is recommended that ESA and its programs jointly develop and implement an agency incident response capability. This capability should comply with the DOL Computer Security Handbook guidelines on incident reporting.

Management's Response:

ESA is in the process of finalizing its formal computer security incident response policy and procedures. This policy and the accompanying procedures, as outlined in ESA's Agency Security Program Plan, will be published by no later than September 30, 2001. Additionally, OFCCP will provide interim security incident response procedures this month.

Finding and Recommendation 6:

The ESA security awareness program has not been fully implemented. Seventy percent of the ESA national office staff has been trained to date. In addition, employees with specific security responsibilities have not been trained on their specific duties. It is recommended that ESA ensure that their security awareness program is fully implemented and all WHD and OFCCP employees receive the appropriate training level based on their responsibilities and job description.

Management's Response:

ESA is in the process of completing its FY 2001 security awareness training plan, which covers all ESA employees and contractors nationwide. As of the date of this report, over 90 percent of OFCCP and 89 percent of WHD national office employees, and 78 percent of all OFCCP and 62 percent of all WHD employees have been trained. ESA is in the process of completing its long-range computer security awareness training plan, which will be completed by September 30, 2001.

Employees with specific security responsibilities, such as Program Security Officers, have been and will continue to receive training on their specific duties and responsibilities. Security Officers were given a briefing on their responsibilities during a June meeting of ESA Security Officers; additional topics will be covered during the August meeting. ESA's long-range security awareness training plan will encompass specific training for employees with security responsibilities.

Finding and Recommendation 7:

Based on discussions with OFCCP and WHD officials, employees in general use the same Network and Application IDs and passwords. It is recommended that risk-based security assessment be performed to determine and implement additional safeguards to protect WDGS and ESCANS2 and OFIS.

Management's Response:

While users can make their Network and Application passwords the same, the two ID/password repositories are physically separate. ESA believes this can be addressed primarily through user awareness training, but will look at other policy compliance methodologies as well.

Finding and Recommendation 8:

OFCCP and WHD database audit trail reports are not being monitored on a regular basis. It is recommended that WHD and OFCCP routinely monitor the database audit trail logs to help identify issues that may affect database integrity and overall system security.

Management's Response:

ESA concurs that better monitoring of audit trail reports will help to ensure the integrity and security of OFCCP and WHD systems. ESA will investigate methods for performing better auditing and monitoring of these systems and ensure that procedures are developed which require a more routine monitoring of these systems.