

DEPARTMENT OF INDUSTRIAL RELATIONS

Office of the Director
455 Golden Gate Avenue, 10th Floor
San Francisco, CA 94102
Tel: (415) 703-5050 Fax: (415) 703-5059/8

MAILING ADDRESS:
P. O. Box 420603
San Francisco, CA 94142-0603



DATE: February 4, 2010

TO: Victoria Bradshaw
Secretary of the Labor and Workforce Development Agency

Original signed by:

FROM: John C. Duncan
Director

SUBJECT: Financial Integrity and State Managers' Accountability Act (FISMA) Report

In accordance with the Financial Integrity and State Managers Accountability Act of 1983, Government Code Sections 13400 through 13407, I am submitting the enclosed report describing the review of our systems of internal control for the biennial period ended December 31, 2009.

As statutorily required DIR is in compliance with Government Code Section 12439 in that all positions continually vacant for six consecutive months not meeting the exemption criteria outlined in Section(s) 12439(b) and 12439(c) of the Government Code were abolished, and that a record has been kept for any continuously vacant positions retained in accordance with section 12439(d) of the Government Code.

If you have questions please contact Greg Edwards, Chief Financial Officer at (916) 263-5668, or David Rowan, Chief Deputy Director at (415) 703-5380.

Enclosure(s)

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Executive Summary

This report reflects the steps undertaken by the Department of Industrial Relations (DIR) to comply with the revised Government Code Section 13405(a) that requires each agency to conduct a review of their internal controls and prepare a report on a biennial basis.

Background:

The Department of Industrial Relations (DIR) was established to improve working conditions for California’s wage earners, and to advance opportunities for profitable employment in California. This mission is carried out through its various divisions and programs as shown in Attachment I, DIR Organization Chart.

The Financial Integrity and State Manager’s Accountability Act of 1983 (FISMA), was enacted to reduce the waste of resources and strengthen accounting and administrative control (Government Code Sections 13400-13407). FISMA requires each state agency to maintain effective systems of internal accounting and administrative control, to evaluate the effectiveness of these controls on an ongoing basis, and to biennially review and prepare a report on the adequacy of the agency’s systems of internal accounting and administrative control.

Risk Assessment:

In compliance with the revised Government Code Section 13405(a) *where each agency must conduct an internal review of their controls and prepare a report*, Division Chiefs and key administrative and program personnel were required to respond to a series of control environment questions regarding a variety of potential risk factors, including, but not limited to, those for which a lack of internal control would hinder the achievement of critical mission objectives. Therefore, while the necessary review of internal controls provides the context of the 2009 FISMA Audit and the scope of the review tests and provides recommendations for the strengthening of internal controls, the review does not attest to the sufficiency of those controls. A list of findings and actions underway/pending is detailed on Attachment II, DIR 2009 FISMA Audit Summary.

Attachment III, 2009 FISMA Audit Addendum, List of Review of Previous Audit Findings (completed), provides a summary of actions taken to address findings as a result of the following external audits:

- 2008 Accounts Receivable audit, conducted by the State Controller’s Office
- 2008 Single Audit, conducted by the Bureau of State Audits
- 2007 FISMA, conducted by the Department of Industrial Relations

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Executive Summary

The 2009 FISMA review also includes a review of DIR’s Information Security as required by State Administrative Manual (SAM) Section 5305 and SAM Section 5315.1. DIR updated its Information Security Risk Assessment in July 2008.

In general, the department has made progress in addressing previous audit findings and strengthening internal controls (see completed findings as noted on Attachment III). As mentioned above, a listing of those findings that still require mitigation are summarized on Attachment II. In addition to identifying those findings that have not been fully addressed, this review (for the two-year period ending December 31, 2009) highlights additional concerns which pose a risk to DIR’s capacity to effectively achieve mission critical objectives, and/or its ability to sufficiently safeguard state assets.

One of the most significant steps that the department has taken to address the underlying internal control weakness that has led to prior audit findings is to redirect resources in preparation for establishing an internal audit unit. This redirection, coupled with the resources provided by a 2009/10 Budget Change Proposal to correct inadequacies in the accounts receivable function, will provide the framework necessary to help ensure and maintain an effective system of internal accounting and administrative control.

However, going forward it is imperative that DIR replace its multiple and antiquated databases and accounting subsystems with integrated recordkeeping system(s) that facilitate reconciliation, reduce duplication, accelerate the collection of state revenues, and reduce the risk of fraud.

The following narrative summary briefly highlights those findings that, if effectively addressed, could significantly strengthen the department’s internal and administrative controls.

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Narrative Summary of Findings

Those findings identified during the 2009 review period that could present the most significant risk to DIR’s capacity to effectively achieve mission critical objectives, and/or its ability to sufficiently safeguard state assets are briefly summarized below:

I. Strategic Plan

In 2008/09 the department began to revise its strategic plan, outlining specific outcomes/deliverables for each division. Going forward, the department should continue these efforts, but it must improve its ability to objectively and effectively monitor and measure performance. Absent a real performance measurement framework and credible management reports that are reviewed and effectively utilized regularly by Executive management, the department cannot assure its stakeholders (the administration, legislature, and the public) of the efficiency and cost effectiveness of its operations.

Moreover, it is unreasonable to assume that certain year-to-year mission critical objectives can be achieved without sufficient funding and/or the allocation of adequate resources (staff, etc.). Therefore, the annual objectives and strategies of the strategic plan must be aligned with the annual Governor’s Budget development cycle, and inform DIR’s internal budget allocation and legislative strategy.

Recommendation:

1. Establish objective performance measure targets that can be independently validated, with an emphasis placed on increasing operational efficiencies which save time and dollars.
2. Develop/enhance management reports that are regularly reviewed by Executive management, with an emphasis placed on those reports that facilitate monitoring of accounts receivable compliance in accordance with State Administrative Manual Section 8776, and help maximize the collection of state revenues.
3. Align annual objectives with available resources, allowing the strategic objectives to inform and set priorities for program and administrative staff, with an emphasis placed on synergizing and prioritizing the workload of existing information technology staff to support the department’s highest priority operational efficiency strategies.

II. Information Security

As required by State Administrative Manual (SAM) Section 5305 and SAM Section 5315.1, DIR updated its Information Security Risk Assessment in July 2008.

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Narrative Summary of Findings

A summary of those risks that require mitigation can be found on Attachment IV, Security Risk Mitigation Plan). The entire Information Security Risk Checklist has been included for reference (please see Attachment V, Risk Assessment Check List).

Recommendation:

1. Specific time frames and due dates should be developed for each action listed on Attachment IV, Security Risk Mitigation Plan.

III. Sustainability and Sufficiency of Funding

In order to offset year-to-year inflationary pressures it is imperative that the department maximize its operational efficiency (see recommendation #1 under strategic plan heading) to lessen the need to increase fees in future years.

Likewise it is also important that the department closely monitor the cost of delivering service to ensure that its fee structure and/or the framework of fines and penalties are sufficient to achieve its statutory mandate. In particular, the degree to which fees, fines and and/or penalties actually support both the cost of enforcement and the cost of collecting said fines and penalties has not been reviewed for some time. Absent such a review, there is moderate to high risk that a “gift of state services” could occur. This is particularly true in those cases where employers are charged a “fee” for inspection or other services rendered.¹ In addition, in those instances in which fines and penalties are deposited into the general fund, any failure to properly reflect the cost of enforcement and/or collection diminishes annual recoveries to the General Fund.

Lastly, there is an inherent fiscal risk associated with an over reliance upon fines and penalties derived from non compliance with the law. Given that DIR’s mission (ultimately) is to increase compliance, a funding structure that depends upon sustained annual infractions carries a risk that cannot be fully evaluated at this time.

Recommendation:

1. Review the hourly rate and ancillary costs charged for all services rendered and compare that charge to actual program costs (also see recommendation # 2 under Strategic plan heading).

¹ This includes but is not limited to reimbursement for ancillary mediation services, ensuring that citations for wage claims and apprenticeship wage enforcement contemplate the cost of enforcement and collection, and that the fee structure for elevator and other inspection and/or consultative services properly reflect the cost of providing the service in question.

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Narrative Summary of Findings

2. Analyze historical and emerging trend data to develop a better understanding of the vulnerability associated with the reliance on “non compliance” as a means of sustaining ongoing operations.

IV. Recordkeeping / Safeguarding of State Assets

The 2007 FISMA Audit identified the need to address a number of findings related to Property (see Attachment III-C, “Property Fixed Assets”). A recently completed physical inventory of equipment revealed incongruities between the record-keeping of stock received reports, and the reconciliation of procurement, payment, and inventory records. These unreconciled irregularities point to a serious internal control weakness.

Further, a recently completed single audit by the Bureau of State Audits identified inconsistencies between the department’s accounting records and close out reports submitted to the US Department of Labor, and that DIR lacked adequate controls to ensure that it only charged to the award costs resulting from valid obligations of the funding period, and that it liquidated these obligations not later than 90 days after the funding period.

The 2008 Controller’s Audit identified “serious control weaknesses” in the Division of Labor Standards Enforcement’s Bureau of Field Enforcement’s cashiering function. While DIR took action to address this specific finding (see Attachment II, finding # 3), there are several other decentralized field-based locations which administer cashiering functions that have not been reviewed.

Recommendation:

1. Training should be provided to all staff involved in the procurement / record-keeping function to help ensure a more complete understanding of the procedures pertaining to property as outlined in the State Administrative Manual Sections 8600 through 8672.
2. The DIR accounting office must follow its newly implemented procedures to ensure that it only charges valid costs to federal grant awards, and obligations are liquidated no later than 90 days after the funding period.
3. The DIR Internal Audit Unit should incorporate the need to review all cashiering functions into its 2010/2011 Audit Plan.

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Narrative Summary of Findings

V. Reconciliation of Subsidiary Accounting Systems to the Main Accounting System

The 2008 Accounts Receivable audit by the State Controller’s Office identified internal control weaknesses related to DIR’s ability to properly record and reconcile records relating to state revenues (see Attachment II, section “B”).

While the department has taken corrective action as identified in Attachment II, the department’s 2009 internal review has revealed that the department’s ongoing monitoring efforts could be strengthened through the creation of management and/or status reports that are regularly transmitted to and reviewed by Executive Management.

In addition, the review found that the systemic problems associated with DIR’s various disparate and antiquated receivable subsystems must be addressed in order to achieve greater operational efficiency and accelerate and maximize the receipt of state revenue. Due to this inadequacy the department lacks the means to effectively ensure that accounts receivables are set up for all records as required by the State Administrative Manual Section 8776. Specific examples of these internal findings are briefly highlighted below:

- **Multiple Database Systems Track Redundant Information**—Redundant separate office systems create inefficiencies by forcing redundant data entry. Further, case outcomes do not always reflect statutory guidelines. For instance, many businesses regulated by DLSE operate across DLSE’s geographic locations. That is, a single business may operate several stores across a geographic area covered by several DLSE offices. While a claim may be filed against the business that legally would cover all locations, DLSE has no mechanism to identify all business locations without performing manual searches at each field office. As a result, inaccurate penalties are assessed when repeat offenders are treated as first-time offenders due to the geographic origin of the subsequent complaint(s).²

- **Lack of Connectivity or Shared Data Repository**—Multiple systems and lack of connectivity increases reliance on manual processes.

² The information related to fines and penalties for DLSE and/or DOSH is contained on 29 separate FileMaker Pro databases, residing on nine separate servers statewide; and/or 18 different sets of data contained on Oracle databases, residing on two separate servers. With rare exceptions, these data bases are not interconnected and there is very limited shared data, making effective reconciliation between databases and to the main accounting system (CALSTARS) functionally impossible.

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Narrative Summary of Findings

- **Track Chronology of Case**—Current systems do not allow staff to monitor case activity over time.
- **Inability to Track Wage Claim Payments with Other Case Information**—Wage claim payments and receipts are recorded in Oracle databases. These Oracle databases are not integrated with case information.
- **Lack of automation**—Automated tools are not available to transfer, assign, track, and manage workloads from DIR to Franchise Tax Board (FTB).³

DIR is updating its procedures and creating the monthly/quarterly management reports necessary to facilitate ongoing monitoring efforts. While these management reports must be compiled manually and do not constitute a complete solution, they will add a measure of control until a permanent solution to the issue of multiple and redundant databases can be fully addressed.

In addition, DIR is also exploring the viability of working jointly on a project with the Employment Development Department to maximize the recovery of long term delinquent debt (revenue due the state).

Recommendation:

1. Continue current efforts to manually record and reconcile accounts receivable information, with an emphasis on sharpening the efficacy of internal management reports (also see recommendation # 2 under Strategic Plan heading).
2. Continue /finalize recommendation for a remedy and timeline for retiring antiquated legacy systems, automating processes, and improving connectivity through the development and implementation of a new/revised system which will improve the accuracy of accounts receivable information.
3. Continue/finalize plan to partner with EDD to maximize the recovery of long term delinquent debt (revenue due the state).

VI. Staff Training

In January 2009 the department completed an analysis and developed a workforce succession plan. The plan may be viewed in detail by accessing the link below:

<http://www.dir.ca.gov/od pub/DIR Workforce Succession Plan.pdf>

³ DIR currently refers delinquent cases to FTB in an attempt to maximize collection. The lack of an automated tool to transfer, assign, track, and manage this workload further slows the reconciliation and collection process and increases the risk of inaccuracy in DIR’s accounting records.

Department of Industrial Relations – 7350
Financial Integrity and State Manager’s Accountability Act (FISMA) Report
For the Biennial Period Ending December 31, 2009

Narrative Summary of Findings

Recommendation:

1. In light of the analysis and the geographical challenges of recruiting and retaining staff to work in the Bay Area, the department (all divisions) must implement specific training and hiring plans designed to expand the body of knowledge, lessen the dependency on key staff, and prepare for the upcoming retirements of an aging workforce to help lessen this risk.

Attachment I

Department of Industrial Relations
Organizational Chart

**GOVERNOR
Arnold
Schwarzenegger**

**California Labor and Workforce
Development Agency
Victoria Bradshaw
Secretary**

**John Duncan
Director**

David Rowan
Chief Deputy Director

Legal Services - Vanessa Holton
Communications - Dean Fryer

Office of Civil Rights - Holly Hayashida
Legislative - Mark Woo-Sam

**Industrial
Welfare
Commission
5 members**

Issues orders for minimum wages, work, hours, conditions of labor and employment

**CAL/OSHA
Appeals Board
Candice Traeger
Chairwoman
Michael J. Wimberly
Executive Officer
3 members**

Hears appeals of employers and employees from enforcement actions of Division of Occupational Safety and Health

**CAL/OSHA
Standards
Board
John MacLeod
Chairman
Marty Hart
Executive Officer
7 members**

Adopts, amends and repeals occupational safety and health standards

**Commission on Health
and Safety and
Workers'
Compensation
Christine Baker
Executive Officer
8 members**

Monitors, evaluates and recommends improvements to the workers' compensation system and safety and health programs

**Workers' Compensation
Appeals Board
Joseph M. Miller
Chairman
6 Members
Dennis Hannigan
Secretary
Rick Dietrich
Deputy**

Adjudicates workers' compensation claims that have been appealed for reconsideration

**California
Apprenticeship Council
14 members**

**Division of
Administration
Pat Chestnut
Chief**

Provides Administrative support to programs within the Department of Industrial Relations

**Labor Standards
Enforcement
Angela Bradstreet
State Labor
Commissioner**

Enforces wage and labor standards and all labor laws not specifically delegated to another agency

**State Mediation
and Conciliation
Paul Roose
Chief**

Provides for conciliation, mediation and arbitration of labor-management disputes in both employment sectors

**Division of Occupational
Safety and Health
Len Weish
Chief**

Enforces occupational safety and health standards in places of employment and public safety in elevators and pressure vessels

**Self Insurance
Plans
James Ware
Manager**

Regulates workers' compensation self insurance plans

**Division of
Workers'
Compensation
Carrie Nevans
Acting
Administrative
Director**

Administers the Workers' Compensation Act

**Division
of Labor Statistics
and Research
Gregory Govan
Chief**

Compiles and publishes information on labor conditions in California and the Department's administrative statistics

**Division of
Apprenticeship
Standards
Glen Forman
Acting Chief**

Promotes, develops, and manages apprenticeship and other on-the-job training programs

Greg Edwards
Chief Fiscal
Officer

Accounting
Flora Casuga

Budget
Vacant

**Business
Management
Karen Wong**

**Information
Systems
Jim Culbeaux**

**Labor
Relations
Cheryl Combs**

**Personnel
Ann Rose**

**Return to Work
Rick Giani**

**Denise Padres
Deputy Chief
Labor
Commissioner**

**Robert
Roginson
Chief Counsel**

**Wage Claims
Adjudication**

**Enforcement of
Labor
Standards**

**Licensing and
Registration**

**Deputy Chief
of Health**

**Deputy Chief
of Safety
Chris Lee**

**CAL/OSHA
Consultation,
Service**

**Legal Unit and
Bureau of
Investigations**

**Elevator, Ride
and Tramway
Unit**

**Pressure
Vessel Unit**

**Certifications
and
Deposits**

**Claims
Auditing and
Compliance**

**Deputy
Administrative
Director**

**Debbie Overpeck
Chief Counsel
& Legal Unit**

**Vacant
Medical Director
& Medical Unit**

**Audit
and
Enforcement**

**Disability
Evaluation**

**Information
and
Assistance**

**Programmatic
Services**

Rehabilitation

Research Unit

**Special Funds
Unit**

**Kevin Star
Court
Administrator**

**WCAB
Local Workers'
Compensation
Courts**

**Maria Robbins
Deputy Chief**

**Industrial
Relations
Research**

**Occupational
Injury and
Illness
Statistics**

Deputy Chief

**Renee Bacchini
Special assistant
to the Chief**

Attachment II

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

A. FROM 2009 FISMA REVIEW			
CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
Finding #1. Strategic Plan			
Finding Details:			
<ul style="list-style-type: none"> Absent a real performance measurement framework and credible management reports that are reviewed and effectively utilized regularly by Executive management, DIR cannot assure its stakeholders (the administration, legislature, and the public) of the efficiency and cost effectiveness of its operations. 	<ul style="list-style-type: none"> In 2008/09, DIR began to revise its strategic plan, outlining specific outcomes/deliverables for each division. 	<ul style="list-style-type: none"> Establish objective performance measure targets that can be independently validated, with an emphasis placed on increasing operational efficiencies which save time and dollars. Develop/enhance management reports that are regularly reviewed by Executive management, with an emphasis placed on those reports that facilitate monitoring of accounts receivable compliance in accordance with State Administrative Manual Section 8776, and help maximize the collection of state revenues. Align annual objectives with available resources, allowing the strategic objectives to inform and set priorities for program and administrative staff, with an emphasis placed on synergizing and prioritizing the workload of existing information technology staff to support the department's highest priority operational efficiency strategies. 	

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
<p>Finding #2. Information Security</p>			
<p>Finding Details: A. Organization and Management Practices</p> <ul style="list-style-type: none"> •<u>Security Program Governance</u> DIR Executive Management has not assigned roles and responsibilities for information security across the organization. •<u>Security Categorization</u> Procedures to classify systems and information that is stored, processed, shared, or transmitted with respect to the type of data (e.g., confidential or sensitive) and its value to critical business functions are not in place. 	<ul style="list-style-type: none"> •DIR hired a full time Information Security Officer (ISO) and a full time Privacy Officer who will work closely with their counterparts within and without the Agency to bring DIR's policies and procedures in line with state standards. •The Privacy Officer will conduct interviews of all business units in DIR to identify and categorize all confidential and sensitive data throughout DIR. 		
<p>B. Personnel Practices</p> <ul style="list-style-type: none"> •<u>Security Awareness</u>. No training is provided to all employees and contractors on an annual basis that addresses acceptable use and good computing practices for systems they are authorized to access. •<u>Position Categorization</u>. There are no procedures in place to identify system access needs by job function and screening criteria for individuals performing those functions. •<u>Personnel Screening</u>. Employee history and/or a background check is not performed on employees who work with or have access to confidential or sensitive information or critical systems. <p>C. Physical Security Practices</p> <ul style="list-style-type: none"> •<u>Environmental Controls</u>. DIR server rooms have no emergency power and air conditioning is inadequate. 	<ul style="list-style-type: none"> •DIR has obtained an online Cyber Security Awareness training program from the Office of Information Security that is used in many departments. •The ISO has identified a background check process that is available through another state agency. •DIR is in the process of moving assets to sites with adequate air conditioning and emergency power. 	<ul style="list-style-type: none"> •Roll out training program to all staff. •DIR needs to complete the categorization of data before developing access criteria. DIR needs policy to be developed before starting background checks. 	

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
<p><u>D. Data Security Practices</u></p> <p>•<u>Data Classification.</u> Policies and processes to classify information in terms of its value, legal requirements, sensitivity, and criticality to the organization are not in place.</p> <p>•<u>Access Controls.</u> Policies and procedures are not in place for appropriate levels of access to computer assets.</p>	<p>•Departmental wireless routers are encrypted, but rogue wireless access points can still be installed by end users until port security can be implemented. The department is half way through encrypting all mobile devices.</p>	<p>•The Privacy Officer will conduct interviews of all business units in order to identify and categorize all confidential and sensitive data throughout the department.</p> <p>•Conduct periodic audits of controls and privileges.</p>	
<p><u>E. Information Integrity Practices</u></p> <p>1. <u>Identification and Authentication.</u> Policies and procedures for identification and authentication to address roles and responsibilities, and compliance standards are not in place.</p> <p>3. <u>Device Identification and Authentication.</u> No information systems/applications are employed to identify and authenticate specific devices before establishing a connection with them.</p> <p>4. <u>System and Information Integrity.</u> Policies and procedures for system and information integrity to address roles, responsibilities, and compliance standards are not in place.</p> <p>9. <u>Software and Information Integrity.</u> There are no information systems/applications that are in place to detect and protect against unauthorized changes to software and information.</p>	<p>•DIR needs to complete the categorization of data before developing access criteria.</p> <p>•DIR has procured hardware and software to support System Control and Configuration Manager.</p> <p>•The Privacy Officer is working with the Information Systems Officer to address all of the policy needs of the department.</p>	<p>•Set up the system.</p> <p>•New products and services need to be evaluated and procured to help in this effort.</p>	

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
<p>10. <u>Information Input Accuracy, Completeness, and Validity.</u> There are no information systems/applications in place to check data inputs for accuracy, completeness, and validity.</p> <p>F. Software Integrity Practices 2. <u>Software Integrity Practices.</u> Policies and procedures associated with system and services acquisition and product acceptance are not in place.</p> <p>G. Personal Computer Security Practices 2. <u>Lock-Out for Inactive Computing Devices.</u> The automatic locking of the computing device after a period of inactivity is not enforced.</p>	<p>•Software installation restrictions are in place in half of the department, with the rest expected to be completed by March.</p>	<p>•New products and services need to be evaluated and procured to help in this effort.</p> <p>•Application security testing is not in place at this time.</p> <p>•Group policy for lock-out of inactive computers is scheduled for deployment after the software installation restrictions are in place in March.</p>	
<p>Finding #3. Sustainability and Sufficiency of Funding</p>			
<p>Finding Details: •Many of DIR's operations derive the majority, if not 100%, of their funding from fines, penalties, and fees. There is an inherent fiscal risk associated with funding ongoing operations exclusively by fines and penalties derived from non-compliance with the law. Given that DIR's mission (ultimately) is to increase compliance, a funding structure that depends upon sustained annual infractions carries a risk that cannot be fully evaluated at this time.</p>		<p>•DIR will review the hourly rate and ancillary costs charged for all services rendered and compare that charge to actual program costs. DIR will analyze historical and emerging trend data to develop a better understanding of the vulnerability associated with the current user funding structure.</p> <p>•Analyze historical and emerging trend data to develop a better understanding of the vulnerability associated with the reliance on "non compliance."</p>	

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
<p>Finding #4. Safeguarding of State Assets</p>			
<p>Finding Details:</p> <p>1. <u>Physical Inventory</u>. A recently completed physical inventory of equipment revealed incongruities between the recordkeeping of stock received reports, and the reconciliation of procurement, payment, and inventory records.</p> <p>2. <u>Field Office Cashiering Functions</u>. The 2008 Controllers' Audit identified "serious control weaknesses" in the Division of Labor Standards Enforcement; Bureau of Field Enforcement's cashiering function. While DIR took action to address this finding (see Attachment II, Prior Audit, finding #3), there are several other decentralized field-based locations which administer cashiering functions that have not been reviewed.</p>		<ul style="list-style-type: none"> • Training should be provided to all staff involved in the procurement/ recordkeeping function to help ensure a more complete understanding of the procedures pertaining to property as outlined in the State Administrative Manual. • The DIR Internal Audit should incorporate the need to review all cashiering functions into its 2010/2011 Audit Plan. 	

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
Finding #5. Reconciliation of Subsidiary Accounting Systems to the Main Accounting System			
<p>Finding Details:</p> <ul style="list-style-type: none"> •DIR's internal review found that while DIR has taken corrective action as identified herein, the department did not engage in the ongoing monitoring necessary to ensure continued compliance. In addition, the systemic problems associated with DIR's various disparate and antiquated receivable subsystems do not ensure that accounts receivables are set up for all records as required by the State Administrative Manual Section 8776. <p>1) <u>Multiple Database Systems Track Redundant Information</u> - Redundant separate office systems create inefficiencies by forcing redundant data entry.</p> <p>2) <u>Lack of Connectivity or Shared Data Repository</u> - Multiple systems and lack of connectivity increases reliance on manual processes.</p> <p>3) <u>Track Chronology of Case</u> - Current systems do not allow staff to monitor case activity over time. 4) <u>Inability to Track Wage Claim Payments with Other Case Information</u> - Wage claim payments and receipts</p>	<ul style="list-style-type: none"> •Detailed invoice aging reports of the Cal-OSHA subsystem was developed. •Additional management reports are being developed. Policies, procedures, and processes are being reviewed and documented. •DIR is currently exploring the viability of working jointly on a receivable collection project with the Employment Development Department. 	<ul style="list-style-type: none"> •Continue current efforts to manually record and reconcile accounts receivable information, with an emphasis on sharpening the efficacy of internal management reports (see recommendation #2 under Strategic Plan). • Continue/finalize the recommendation for a remedy and timeline for retiring antiquated legacy systems, and automating processes and improving connectivity through the development and implementation of a new/revised system which will improve the accuracy of accounts receivable information. 	
Finding #6. Staff Training			
<p>Finding Details:</p> <ul style="list-style-type: none"> •DIR is faced with the geographical challenges of recruiting and retaining staff to work in the Bay Area; and, as in other state agencies, DIR is faced with the devastating threat of a large number of retirements of an aging workforce. 	<ul style="list-style-type: none"> •In January 2009 the department completed an analysis and developed a workforce succession plan. The plan may be viewed in detail by accessing the link below. <p>http://www.dir.ca.gov_odpub/DIR_Workforce_Succession_Plan.pdf</p>	<ul style="list-style-type: none"> •In light of the analysis and the geographical challenges of recruiting and retaining staff to work in the Bay Area, the department (all divisions) must implement specific training and hiring plans designed to expand the body of knowledge, lessen the dependency on key staff, and prepare for the upcoming retirements of an aging workforce to help lessen this risk. 	

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
B. FROM PRIOR AUDIT - State Controller's Office Review of Accounting for and Collecting of Debt Due the State - Report Date August 2008, Notwithstanding any previous actions taken, the 2009 FISMA Review determined that additional actions were necessary to strenghten internal controls.			
Finding #1. The DIR is able to collect only a fraction of fines imposed.			
Finding Details: <ul style="list-style-type: none"> • Failure to act in a timely manner by failing to file judgment against employers within a one-year period. • Significant delays in referring cases to the DLSE Collections Unit. • The DLSE does not have a formal manual documenting each step of the collections process and/or the roles and responsibilities of DLSE staff working to resolve the case. • DIR management does not have current, accurate, and reliable data to effectively monitor the progress of the collection efforts in DLSE. 	<ul style="list-style-type: none"> • DLSE is continually reviewing open cases to ensure that judgments are filed timely. • The Bureau of Field Enforcement (BoFE) has developed a policy manual that establishes procedures for staff and what is required, as well as a memorandum issued to staff providing instructions for referrals of cases. • The Collections Unit has developed a manual that describes its procedures and the specific duties the individual staff within that Unit are responsible for performing. • The software program to provide accurate and reliable DLSE receivable data is now in operation. 	<ul style="list-style-type: none"> • The CFO has directed accounting to develop management reports, to be reviewed monthly, that will allow for ongoing monitoring of compliance. • The CFO has directed accounting to evaluate corrective actions taken and provide additional recommendations, and/or implement additional process changes to improve the accuracy of accounting records. Also, please see "actions to be taken" for Finding #5 in Section A of this document. 	<p style="text-align: center;">April 2010</p> <p style="text-align: center;">Ongoing/TBD</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
Finding #2. The DIR is circumventing state control requirements by not establishing accounts receivable in its formal accounting records.			
<p>Finding Details:</p> <ul style="list-style-type: none"> •When a citation is issued and a fine is assessed by DLSE, the DIR accounting office is not notified so that it can set up an accounts receivables to record and track the transaction in the accounting records. By neglecting to records fines and penalties as accounts receivables, the DIR, in effect, bypassed the review by outside state control agencies relative to writing off receivables. •The DLSE does not have a formal process in place to ensure the accuracy of data in the Filemaker Pro system after the initial data entry. •The DLSE lacks system controls to prevent unauthorized or inappropriate changes to system data. • Some cases referred to the DLSE Collection Unit were not on its listing of cases. 	<ul style="list-style-type: none"> •There was and is no deliberate attempt to circumvent the state requirements. •The DLSE has an electronic database but the information entered into the system is not always reliable. •The Division does maintain a record of citation books issued and to which deputy the book is issued. The Division is requiring that its supervisors review the citation books to ensure that all of the citations are accounted for in its current database. •DLSE developed a spreadsheet to track all citations issued during the current fiscal year (08/09), along with written instructions to the staff concerning how to complete the spreadsheet. The first report was submitted to DIR Accounting on October 31st. Since that date, DLSE has been submitting updated reports each Friday which summarize new citations issued since the previous report, appeals filed by employers, citations administratively dismissed and payments received on all citations. •DIR Accounting has entered the information into CALSTARS. 	<ul style="list-style-type: none"> •Accounting will develop management reports, to be reviewed monthly, that will allow for ongoing monitoring of compliance. 	<p>April 2010</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
2009 FISMA AUDIT

Attachment II

CONTROL WEAKNESSES IDENTIFIED	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/PLANNED ACTION
Finding #3. The DIR's internal control over collection is weak because collection duties are not clearly defined and adequately segregated.			
<p>Finding Details:</p> <ul style="list-style-type: none"> •The DLSE collection duties are inadequately segregated representing a serious internal control weakness as it does not provide the adequate checks and balances that would prevent errors and irregularities. 	<ul style="list-style-type: none"> •DLSE has moved forward with its plans to centralize the Bureau cashiering function in the Sacramento Office. The affected staff have been reassigned to other programs within the Division and positions are being transferred to the Sacramento Cashiering Unit. All penalties collected after November 15th were handled through the Sacramento office. The centralized Bureau Cashiering Unit was fully functional on January 1, 2009. •A Chief Fiscal Officer (CFO) was hired to better manage the money flow. 	<ul style="list-style-type: none"> •The CFO has determined that additional review is required. The review will be conducted by Internal DIR Audit staff during the 2010 and 2011 audit Plan years. 	<p>2010/11</p>
Finding #4. The accuracy and completeness of the DIR's accounts receivable balance resulting from DOSH-imposed fines is questionable.			
<p>Finding Details:</p> <ul style="list-style-type: none"> •Discrepancies were noted between DOSH's Integrated Management System (IMIS), used for federal reporting purposes, and Oracle, used by DIR accounting as an accounts receivable subsidiary system. •DIR accounting does not receive updated information from DOSH regarding any cases that have been appealed via internal hearings and/or the court system. 	<ul style="list-style-type: none"> •The DIR reconciles the IMIS and Oracle data on a monthly basis. •The DIR streamlined its Cal/OSHA penalty collection process resulting in shorter collection processing time. <ul style="list-style-type: none"> •DIR Accounting and the Occupational Safety and Health Appeals Board (OSHAB) are now reconciling open cases. •A Chief Fiscal Officer (CFO) was hired to better manage the money flow. 	<ul style="list-style-type: none"> •The CFO has determined that additional review is required. The review will be conducted by Internal DIR Audit staff during the 2010 and 2011 audit Plan years. 	<p>2010/11</p>

Attachment III

2009 FISMA REVIEW

Summary of Other Audit Findings: 2007-2009

Greg Edwards, Chief Financial Officer

2/3/2010

The pages that follow detail the actions taken and/or are ongoing to address audit findings by the Bureau of State Audits, State Controller's Office, and the 2007 FISMA Audit that were not necessarily reviewed in the context of the 2009 FISMA Review.

DEPARTMENT OF INDUSTRIAL RELATIONS
 RESPONSE TO THE CALIFORNIA SINGLE AUDIT REPORT NO. 24-09-612-10-001 CONDUCTED BY
 CALIFORNIA'S BUREAU OF STATE AUDIT FOR THE YEAR ENDED JUNE 30, 2008 (FEDERAL COMPLIANCE)

A. FINDING RESULTING IN DISALLOWED COSTS

Finding Number	Federal Program	Category of Finding	American Recovery & Reinvestment Act		2007-08 Finding Status		
			Related?	Explanation	Status	Explanation	Correction Date
2008-8-10	17.503	<p><u>Period of Availability</u> - Questioned Costs</p> <p>The auditors' questioned \$4,053.21 costs related to the OSHA State Plan Program.</p> <ul style="list-style-type: none"> •Industrial Relations had obligations of \$4,042.79 for federal fiscal year 2007 that were not based on a valid order placed during the funding period. •Industrial Relations had obligations of \$10.42 for federal fiscal year 2007 paid after December 31, 2007. 			A	Reduced federal charges by \$4,042.79.	12/07/2009
					A	Reduced federal charges by \$10.42.	12/07/2009

DEPARTMENT OF INDUSTRIAL RELATIONS
 RESPONSE TO THE CALIFORNIA SINGLE AUDIT REPORT NO. 24-09-612-10-001 CONDUCTED BY
 CALIFORNIA'S BUREAU OF STATE AUDIT FOR THE YEAR ENDED JUNE 30, 2008 (FEDERAL COMPLIANCE)

B. FINDINGS REQUIRING CORRECTIVE ACTION

Finding Number	Federal Program	Category of Finding	American Recovery & Reinvestment Act		2007-08 Finding Status		
			Related?	Explanation	Status	Explanation	Correction Date
2008-2-8	17.503	<u>Allowable Costs/ Cost Principles</u> - Industrial Relations lacked adequate controls to ensure that the personal services costs it charged to the California Occupational Safety and Health program are allowable. Industrial Relations did not require employees who were expected to work solely on the program to complete required certifications.			A	As recommended, DIR will conduct it's initial semi-annual certification (October 1, 2008 through March 31, 2009). A memo to managers of employees who work solely on this program is to be issued on August 7, 2009 to certify Federal grant participation.	8/7/2009
2008-3-12	17.503	<u>Cash Management</u> - Industrial Relations does not obtain written authorization prior to requesting an advance. Industrial Relations does not then follow appropriate procedures to reconcile the advance to actual expenditures incurred during that period.			A	For FY 2008/09, there was no advance requested. If an advance is necessary, it is now Accounting Unit's policy and procedure to prepare and submit SF-270, Request for Advance or Reimbursement, to the federal Department of Health and Human Services Division, to be approved by the accounting administrator. Reimbursements were reconciled to actual expenditures incurred during that period.	8/21/2008
2008-8-10	17.503	<u>Period of Availability</u> - Industrial Relations lacked adequate controls to ensure that it liquidated all obligations incurred not later than 90 days after the end of the funding period.			A	DIR Cal/OSHA division routes all invoices to Accounting/Federal Grants Unit for proper work phase and PCA coding to ensure that no invoice is paid with federal fund after closeout.	3/31/2009
2008-12-14	17.503	<u>Reporting</u> - Industrial Relations submitted an inaccurate closeout report for the 2007 federal award associated with the California Occupational Safety and Health Program (program), and did not provide accounting records to demonstrate that unliquidated obligations were paid with state funds.			B	For the 2008 federal award associated with Cal/OSHA that closed on 12/31/2008, DIR will provide accounting records which will show that unliquidated obligations on 12/31/2008 are paid with state funds after 12/31/2008.	8/31/2009

A - fully corrected
 B - partially corrected

DEPARTMENT OF INDUSTRIAL RELATIONS' SIX-MONTH FOLLOW-UP RESPONSE TO
SCO REVIEW OF ACCOUNTING FOR AND COLLECTING OF DEBT DUE THE STATE - Report Date August 2008

Attachment III-B

Finding #	Finding	Finding Details	Initial Response	Action Taken/In Progress	Further Action Required
1	The DIR is able to collect only a fraction of fines imposed.	<ul style="list-style-type: none"> • Failure to act in a timely manner by failing to file judgment against employers within a one-year period. • Significant delays in referring cases to the DLSE Collections Unit. • The DLSE does not have a formal manual documenting each step of the collections process and/or the roles and responsibilities of DLSE staff working to resolve the case. • DIR management does not have current, accurate, and reliable data to effectively monitor the progress of the collection efforts in DLSE. 	<ul style="list-style-type: none"> • The Bureau of Field Enforcement (BoFE) has developed a policy manual that establishes procedures for staff and what is required, as well as a memorandum issued to staff providing instructions for referrals of cases. • The Collections Unit has developed a manual that describes its procedures and the specific duties the individual staff within that Unit are responsible for performing. 	<ul style="list-style-type: none"> • DLSE is reviewing open cases to ensure that judgments are filed timely. • DLSE has been working with the DIR Accounting and Information Systems staff to develop a software program to provide accurate and reliable data. This software program development is currently in its testing phase. 	<ul style="list-style-type: none"> • Continue review of open cases to ensure judgments are filed timely. • Complete the testing phase of the software development project; provide hands-on training to all affected staff. Target go-live date is December 15, 2008.
2	The DIR is circumventing state control requirements by not establishing accounts receivable in its formal accounting records.	<ul style="list-style-type: none"> • When a citation is issued and a fine is assessed by DLSE, the DIR accounting office is not notified so that it can set up an accounts receivables to record and track the transaction in the accounting records. By neglecting to records fines and penalties as accounts receivables, the DIR, in effect, bypassed the review by outside state control agencies relative to writing off receivables. • The DLSE does not have a formal process in place to ensure the accuracy of data in the Filemaker Pro system after the initial data entry. • The DLSE lacks system controls to prevent unauthorized or inappropriate changes to system data. • Some cases referred to the DLSE Collection Unit were not on its listing of cases. 	<ul style="list-style-type: none"> • There was and is no deliberate attempt to circumvent the state requirements. • The DLSE has an electronic database but the information entered into the system is not always reliable. • The Division does maintain a record of citation books issued and to which deputy the book is issued. The Division is requiring that its supervisors review the citation books to ensure that all of the citations are accounted for in its current database. 	<ul style="list-style-type: none"> • DLSE developed a spreadsheet to track all citations issued during the current fiscal year (08/09), along with written instructions to the staff concerning how to complete the spreadsheet. The first report was submitted to DIR Accounting on October 31st. Since that date, DLSE has been submitting updated reports each Friday which summarize new citations issued since the previous report, appeals filed by employers, citations administratively dismissed and payments received on all citations. •DIR Accounting has entered the information into the CALSTARS system. 	<ul style="list-style-type: none"> • Institute the establishment of DLSE receivables into CALSTARS. • Complete the development of DLSE accounts receivable software with a go-live target of December 15, 2008.

Finding #	Finding	Finding Details	Initial Response	Action Taken/In Progress	Further Action Required
3	The DIR's internal control over collection is weak because collection duties are not clearly defined and adequately segregated.	<ul style="list-style-type: none"> The DLSE collection duties are inadequately segregated representing a serious internal control weakness as it does not provide the adequate checks and balances that would prevent errors and irregularities. 	<ul style="list-style-type: none"> The DLSE will be assessing whether a Budget Change Proposal (BCP) would be required in order to implement process enhancements. 	<ul style="list-style-type: none"> DLSE has moved forward with its plans to centralize the Bureau cashiering function in the Sacramento Office. The affected staff have been reassigned to other programs within the Division and positions are being transferred to the Sacramento Cashiering Unit. All penalties collected after November 15th will be handled through the Sacramento office. Wage payments will continue to be paid through the Los Angeles Cashiering Unit until the necessary files are moved and the process to grant access to the Los Angeles data to the Sacramento staff has been completed. The centralized Bureau Cashiering Unit will be fully functional by January 1, 2009. 	<ul style="list-style-type: none"> Complete the centralization of BoFE's cashiering functions. Estimated completion date is January 1, 2009. Restructure the Division of Administration to include a Chief Financial Officer (CFO) in order to better manage the money flow. In coordination with the Department of Finance, Fiscal Systems & Consulting Unit, the DIR is in the process of reinforcing its fiscal staff's knowledge base through a DOF-conducted training sessions on state fund accounting.
4	The accuracy and completeness of the DIR's accounts receivable balance resulting from DOSH-imposed fines is questionable.	<ul style="list-style-type: none"> Discrepancies were noted between DOSH's Integrated Management System (IMIS), used for federal reporting purposes, and Oracle, used by DIR accounting as an accounts receivable subsidiary system. DIR accounting does not receive updated information from DOSH regarding any cases that have been appealed via internal hearings and/or the court system. 	<ul style="list-style-type: none"> The DIR is evaluating the effectiveness of the DLSE's Collections Unit to determine if it could be used as a model for DOSH collections. The DIR is considering establishing a departmental-wide collections unit for all its units' debts. This action would require a Budget Change Proposal and would be implemented over a period of time. 	<ul style="list-style-type: none"> The DIR reconciles the IMIS and Oracle data on a monthly basis. The DIR streamlined its Cal/OSHA penalty collection process resulting in shorter collection processing time. DIR Accounting and the Occupational Safety and Health Appeals Board (OSHAB) are now reconciling open cases. 	<ul style="list-style-type: none"> Accounting to update policy and procedures manual to include monthly reconciliation of IMIS and Oracle data as well as the streamlined and improved collection process. DIR to look into enhancing or revamping the current Cal/OSHA Oracle database. Restructure the Division of Administration to include a Chief Financial Officer (CFO) in order to better manage the money flow. In coordination with the Department of Finance, Fiscal Systems & Consulting Unit, the DIR is in the process of reinforcing its fiscal staff's knowledge base through a DOF-conducted training sessions on state fund accounting.

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>PROPERTY (FIXED ASSETS)</p>			
<p>1. Physical Inventory Not Performed (Prior Finding 6)</p> <p>Recommendation : Schedule physical inventory counts of all property. Due to DIR's many divisions, it may be more efficient for each division to perform a physical inventory count and then submit to Headquarters for reconciliation to the accounting records. Accurately footnote any circumstances of non-compliance in the financial statements.</p>	<p>Prior to the release of the final audit findings, DIR immediately scheduled a physical inventory count of General Fixed Assets for the department and completed it by the summer of 2006.</p>	<p>Another physical inventory is scheduled to begin in the summer of 2008 and it is anticipated that the physical inventory will be finished in 2009.</p>	<p>Completed in 2009</p>
<p>2. Inadequate Capitalization of Fixed Assets</p> <p>Recommendation : Ensure that property is accurately capitalized and recorded in the property ledger.</p>	<p>Upon completion of the physical inventory, the property ledger and Accounting records were adjusted to accurately reflect the capitalized property.</p>		<p>Completed in 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>3. Inaccurate Property Ledger (Prior Finding 5)</p> <p>Recommendation : Use stock received reports and final vendor invoices to record property in the property ledger. Ensure that Business Services is notified of all changes in property location and these changes are subsequently recorded in the property ledger. Develop procedures to ensure the assets are input timely in the property ledger. Reconcile the property ledger to the general ledger and investigate variances to ensure that accurate totals are reported in the Report 19.</p>	<p>The Business Management Unit has updated their procedures and requires all divisions to report movement of property in a timely manner. Standard property transfer/disposition forms shall be used. These procedures have been communicated to departmental program staff.</p>		<ul style="list-style-type: none"> •January 2006 - Procedures updated •Ongoing - Use of standard property transfer/disposition form
<p>4. Inadequate Property Disposition</p> <p>Recommendation : Develop procedures to ensure that DGS approval is received before the property is disposed of and ensure the property is disposed of within 30 days of DGS approval. Ensure that all dispositions are identified and are accurately posted to the property ledger. Develop procedures to ensure that lost, stolen, or destroyed property is reported on a property survey report within a reasonable time period.</p>	<p>The Business Management Unit has developed procedures to ensure that departmental and DGS approvals are obtained prior to the disposition or transfer of property. DIR staff have been trained to report within a reasonable time period when property is lost, stolen or destroyed.</p>	<p>Employees are reminded in annual training sessions.</p>	<p>Annually</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>5. Lack of a Property Survey Board</p> <p>Recommendation: Establish a Property Survey Board and assign specific individuals to the Board</p>	<p>A Property Survey Board has been appointed and includes staff from Accounting, Business Management, Information Systems unit, and the programs.</p>		<p>January 2006</p>
<p>6. Inadequate Tagging Procedures</p> <p>Recommendation: Tag and record in the property ledger all items under \$500 that are desirable and susceptible to theft.</p>	<p>The DIR decided to maintain the existing policy of tagging and recording items \$500 and over only.</p>		
RECEIVABLES			
<p>7. Unrecorded Accounts receivable (Prior Finding 9)</p> <p>Recommendation: Record all outstanding assessments in DIR's accounting records.</p>		<p>With the delay in the implementation of the DLSE Case Management System, DIR Accounting, in the interim will require DLSE to provide accounts receivable information for proper recording.</p>	<p>January - March 2010</p>
<p>8. Improper posting of Subsidiary Ledger to General Ledger</p> <p>Recommendation: Properly post all subsidiary records to the general ledger and reconcile all subsidiary records to the general ledger monthly</p>	<p>DIR has started implementing the reconciliation of the accounts receivable subsystem to the general ledger (CALSTARS) on a monthly basis. In addition, payroll receivable will be closely monitored so that receivables and payments will be properly posted on both the subsidiary ledger and the general ledger.</p>		<p>Ongoing - Monthly</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>9. Collection Efforts Need Improvement (Prior Finding 2)</p> <p>Recommendation: Apply collection procedures promptly and systematically to all delinquent accounts receivable. In addition, promptly seek approval from the appropriate control agency to write-off delinquent and uncollectible accounts receivable.</p>	<p>The DIR Accounting Office has submitted a request to the State Controller's Office to write-off \$18.4M in uncollectible accounts receivables and \$7.0 M were approved.</p>	<p>DIR will apply collection procedures promptly to all delinquent accounts based on SAM Section 8776.6 and that includes seeking approval from appropriate control agency to write-off delinquent and uncollectible accounts receivable.</p>	<p>January - March 2010</p>
<p>REVOLVING FUND</p>			
<p>10. Salary Advances Controls are not Adequate (Prior Finding 4)</p> <p>Recommendation : Develop procedures to monitor aging salary advances. On a monthly basis, Accounting should send a report to Personnel listing all outstanding salary advances. Personnel should use this report and follow up on all outstanding salary advances. Develop procedures to track previous salary advances to avoid approving excess salary advances. Personnel should use the outstanding salary advances report to check for any previous salary advances given to the employees.</p>	<p>The Accounting Office is currently providing the Personnel Unit a monthly listing of outstanding salary advances for their review and action to clear the salary advances. In addition, existing procedure has been updated and immediately implemented to closely monitor all request for salary advances to check for any previous advances before processing the request. Accounting staff will notify the Personnel Analyst for the outstanding advances to be cleared before processing any new request.</p>		<p>January 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>11. Inadequate UEF and SIF Procedure Manuals</p> <p>Recommendation: With the average case load of 250 cases per Claim Representative, documented procedures of regular duties performed by the Claim Representatives should be developed and included in the administrative guides.</p>	<p>The Claim Representative duty statements were updated to document procedure of regular duties.</p>		<p>January 2006</p>
<p>12. UEF Inadequately Controlled</p> <p>Recommendation: Require original receipts for all reimbursement claims. A verification checklist should be developed to ensure that precautions have been taken to verify the validity of claim.</p>	<p>DIR's internal controls over cash disbursements are sufficient to ensure that cash disbursements are made for allowable purposes and are accurately and promptly posted. In addition, adequate separation of duties exists and bank reconciliations are timely.</p>		<p>January 2006</p>
<p>CASH DISBURSEMENTS</p>			
<p>13. Inadequate Bank Reconciliation</p> <p>Recommendation: The person reconciling the back statement should accurately prepare the bank reconciliation. Moreover, the person who reviews the bank reconciliation should carefully review all items to ensure that accurate information is reported. Make appropriate adjusting entries to remove the uncleared deposits from accounting records, ensure that all future deposits are accurately recorded, and timely research all reconciling items.</p>	<p>Procedures have been re-conveyed to the bank reconciliation staff to ensure that all future deposits are accurately recorded and that timely research of all reconciling items be done.</p>		<p>January 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>14. Uncashed or Unclaimed Checks are not Cleared Timely</p> <p>Recommendation: Establish procedures to continuously monitor uncashed or unclaimed checks and stop payment at least one week prior to the one-year period of negotiability.</p>	<p>Currently, all outstanding checks over one year old have been cleared and credited back to ORF or remitted to an escheat revenue account. DIR has established procedures to continuously monitor uncashed or unclaimed checks to comply with SAM Section 8042.</p>		<p>July 2006</p>
<p>15. Inadequate Accountability of Checks</p> <p>Recommendation: Check signers should reconcile checks with the daily log.</p>	<p>Procedures are already in place to comply with the auditor's recommendation. A log of checks is maintained and check signers reconcile checks signed with the daily log by initialing it.</p>		<p>January 2006</p>
CASH RECEIPTS			
<p>16. Untimely Remittances to the State Treasury</p> <p>Recommendation: Remit cash collections to the State Treasurer's Office (STO) in accordance with SAM.</p>	<p>Since the introduction of the electronic cash remittance process, the Department is now in full compliance with SAM Section 8091.</p>		<p>January 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>17. Inadequate Accountability of Checks</p> <p>Recommendation: Obtain FSCU approval on ICRPs prior to submitting them to the cognizant federal agency.</p>	<p>The ICRP for FY 04/05 and 05/06 was submitted simultaneously on January 31, 2005 to FSCU and Department of Labor (DOL).</p>	<p>In the future, DIR will obtain FSCU approval prior to submitting ICRPs to DOL.</p>	<p>January 2006</p>
<p>18. Reimbursement of Deficiency Claims are Inadequate (Prior Finding I)</p> <p>Recommendation: Ensure that staff clear outstanding deposits timely to prevent cash shortages.</p>	<p>A procedure has been in place wherein outstanding deposits over 30 days are being followed up with the State Treasurer's Office.</p>		<p>January 2006</p>
<p>PURCHASING</p>			
<p>19. Split Purchase Orders</p> <p>Recommendation: Ensure that purchases from the same vendor are combined into one purchase order to avoid the appearance of circumventing state procurement procedures.</p>	<p>Business Management Unit has already corrected the citation of splitting the purchase orders to comply with the rules and regulations set forth by DGS. DIR is purchasing PCs, servers and other IT-related products through the California Strategic Sourcing Contract for big purchases which is mandatory and has no dollar limits.</p>		<p>January 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>20. Inadequate Stock Received Reports</p> <p>Recommendation: Prepare stock received reports or use an approved purchase order to record all necessary information at the time goods are received, and keep a copy of the completed stock received report in the accounting file.</p>	<p>Business Management Unit distributes approved purchase order which includes the File Copy & Copy of Prepared Stock Received Report (SRR) for the program to sign once goods/services are received. Business Management informs the program that the signed SRR will be submitted to Accounting together with the invoice. Also, A copy of the signed SRR must be forwarded to Business Management Unit to close the purchase orders.</p>	<p>Accounts payable staff are reminded to strictly follow the procedure to require the program staff to submit a copy of the SSR when submitting invoices for payment.</p>	<p>Use of SRR - Ongoing</p>
CONTRACTS			
<p>21. Inadequate Contract Monitoring</p> <p>Recommendation: Maintain an expenditure ledger for each contract</p>	<p>The Business Management Unit has developed procedures for maintaining expenditure logs for each contract. These procedures and formats have been distributed to departmental program staff. The Business Management Unit continues to monitor maintenance of these expenditure ledgers.</p>		<p>Use of Expenditure ledgers - Ongoing</p>
<p>22. Splitting of Contracts</p> <p>Recommendation: Obtain DGS approval for multiple contracts to a single contractor if the total exceeds \$50,000.</p>	<p>DIR has consolidated contracts with same scope of work and term and awarded to a single contractor and obtains DGS approval for those that are above \$50,000.</p>		<p>January 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
<p>23. Inadequate Liquidation of Encumbrances</p> <p>Recommendation: Develop procedures to ensure that all contract payments are charged against the appropriate encumbrance.</p>	<p>Accounts payable staff are reminded to strictly follow the procedure to liquidate encumbrances with the right transaction code.</p>		<p>January 2006</p>
PERSONNEL AND PAYROLL			
<p>24. Unauthorized Overtime Requests</p> <p>Recommendation: Overtime requests submitted by employees must be signed and dated by a designated supervisor prior to overtime hours worked or emergency circumstances must be clearly stated.</p>	<p>DIR's practice has been for employees to obtain supervisors' verbal approval for overtime requests prior to the overtime being worked. Therefore, the "authorized" signature/date block is not always signed prior to overtime worked. The Supervisor approves all overtime at the end of the pay period when the Absence and Additional time Worked (Std. 634) and Authorization for Extra Hours (Std. 682) are submitted.</p>		
<p>25. Undeliverable Salary Warrants Not Remitted Timely</p> <p>Recommendation: Actively track the aging of undeliverable warrants and report those warrants over 90 days old to Personnel and deposit warrants after 90 days into the Special Deposit Fund.</p>	<p>A procedure is already in place wherein undeliverable salary warrants over 30 days old are being reported to Personnel. In addition, Personnel is also being advised that warrants over 90 days old will be deposited into the Special Deposit Fund.</p>		<p>Ongoing</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
INFORMATION TECHNOLOGY			
<p>26. Information System Controls Need Improvement</p> <p>Recommendation: Implement procedures to ensure that exiting employees are promptly removed from the network. Furthermore, control access to applications to only authorized personnel by requiring unique passwords for each user.</p>	<p>The DIR employee exit/clearance procedure has been updated to include timely notification to the Information Systems Unit and the Business Management Unit. These procedures have been communicated to departmental program staff and attendance reporting officers.</p>		<p>January 2006</p>
<p>27. Inadequate Daily Batch Reconciliation Procedures</p> <p>Recommendation: Ensure batch reconciliation are properly completed and reviewed daily.</p>	<p>A procedure has been developed to prepare daily batch reconciliation with the right CALSTARS report. The audit findings have been corrected.</p>		<p>January 2006</p>

DEPARTMENT OF INDUSTRIAL RELATIONS
Internal Control Weaknesses

Attachment III-C

CONTROL WEAKNESSES IDENTIFIED IN 2007 FISMA Audit	CORRECTIVE ACTIONS TAKEN	CORRECTIVE ACTIONS TO BE TAKEN	DATE OF ACTION/ PLANNED ACTION
FIELD OFFICES			
<p>28. Inadequate Separation of Duties</p> <p>Recommendation: Route checks for disbursement by a person other than the check preparer. Separate the following functions: recording, authorization, and access to blank check stock. Change the combination to the safe and keep a record of the date the combination was last changed and who has access to the safe.</p>	<p>The temporary inadequate separation of duties has been corrected. Additional staff have been hired. Processes have been implemented and the combination of the safe is being changed.</p>		<p>January 2006</p>
<p>29. No Prelisting of Cash Receipts</p> <p>Recommendation: Staff responsible for opening the mail should prepare an ongoing prelisting of all cash or negotiable items that are not made payable to the department.</p>	<p>DIR has implemented the recommendation and will prepare an ongoing prelisting of all cash or negotiable items that are not made payable to the department.</p>		<p>December 2009</p>

Attachment IV

Department of Industrial Relations

2009 FISMA Review

Attachment IV

Information Security Risk Mitigation Plan

A. Organizational and Management Practices

1. Security Program Governance – DIR has a full time Information Security Officer (ISO) and has recently hired a full time Privacy Officer. These individuals are working closely with their counterparts within and without the Agency to bring DIR's policies and procedures in line with state standards.

Risk: Low

7. Security Categorization – The Privacy Officer is planning to conduct interviews of all business units in order to identify and categorize all confidential and sensitive data throughout the department.

Risk: Low

B. Personnel Practices

1. Security Awareness Training – DIR has obtained an on-line Cyber Security Awareness training program from the Office of Information Security that is used in many departments. This program has been vetted by Labor Relations and piloted on the Information Services staff; pending final approval from the Chief Counsel in OD Legal before disseminating rolling out to all staff.

Risk: High

3. Position Categorization – DIR needs to complete the categorization of data before developing access criteria.

Risk: Low

6. Personnel Screening – The ISO has identified a background check process that is available through another state agency. DIR needs policy to be developed before starting background checks.

Risk: Medium

C. Physical Security Practices

4. Environmental Controls – Server rooms have no emergency power and inadequate air conditioning. DIR is in the process of moving assets to sites with adequate air conditioning and emergency power as part of a state-wide consolidation effort.

Risk: High

D. Data Security Practices

4. Data Classification – The Privacy Officer is planning to conduct interviews of all business units in order to identify and categorize all confidential and sensitive data throughout the department.

Risk: Low

Department of Industrial Relations

2009 FISMA Review

Attachment IV

5. Access Controls – Departmental wireless routers are encrypted, but rogue wireless access points can still be installed by end users until port security can be implemented. The department is half way through encrypting all mobile devices. Periodic audits of controls and privileges have not started.

Risk: Medium

E. Information Integrity Practices

1. Identification and Authentication – DIR needs to complete the categorization of data before developing access criteria.

Risk: Low

3. Device Identification and Authentication – DIR has procured hardware and software to support System Control and Configuration Manager, which is used for device identification and authentication at other agencies. Currently working on hiring a contractor to set up the system.

Risk: Low

4. System and Information Integrity – The Privacy Officer is working with the ISO to address all of the policy needs of the department.

Risk: Low

9. Software and Information Integrity – New products and services need to be evaluated and procured to help in this effort.

Risk: Medium

10. Information Input Accuracy, Completeness, and Validity – New products and services need to be evaluated and procured to help in this effort.

Risk: Medium

F. Software Integrity Practices

2. Software Integrity Practices – Software installation restrictions are in place in half of the department, with the rest expected to be completed by March. Application security testing is not in place at this time.

Risk: High

G. Personal Computer Security Practices

2. Lock-Out for Inactive Computing Devices – Group policy for lock-out of inactive computers is scheduled for deployment after the software installation restrictions are in place in March.

Risk: Medium

Attachment V



CALIFORNIA OFFICE OF
INFORMATION SECURITY
& PRIVACY PROTECTION



Information Security

Risk Assessment Checklist

**A High-Level Tool to Assist State Agencies
with Risk Analysis**

Updated July 2008

Introduction

Information security is a critical issue for state agencies. Increased access to government information and services has been realized as the state increasingly moves its core activities to the Internet. However, as more information and services become available and dependent on Internet-based technology the risk of potential liability, cost, and national repercussions increases as well. State agencies play a unique role as the managers and caretakers of some of the largest collections of critical systems, applications, and databases. These systems, applications, and databases often house information which is subject to strict controls and protections by law, including the data collected, stored, shared, and transmitted that was once very difficult to obtain. Risk assessment tools, like this one, can assist an agency in determining the gaps in its information security program and provide guidance and direction for improvement.

State Administrative Manual (SAM) Section 5305 requires that state agencies conduct periodic risk assessments, and SAM Section 5315.1 requires agencies submit an annual risk management certification, signed by its director. Use of this simple Checklist is not required, nor is it intended to cover all of the steps that your agency will need for its annual certification, but its use will provide a high-level view of an agency's security posture when measured against general information security practices.

This tool should be used in conjunction with the following steps:

1. This Checklist should be completed by the agency's Information Security Officer (ISO), in cooperation with the Chief Information Officer. A response to the items in each section should be prepared to accurately reflect the "point in time" picture of the agency's security posture.
2. Identify the levels of risk associated with any of the items that result in a "no" response.
3. Develop an appropriate action plan to mitigate the identified risk.
4. Assign roles and responsibilities for implementing and monitoring timely completion of the action plan.

This Checklist was first released in March 2006 and was developed by a workgroup of volunteer ISOs from various state agencies. It was based upon the Risk Management categories outlined in SAM Section 5305.2, Risk Management Program and is arranged to correspond with the categories in this Section. In June 2007, this Checklist was updated with more current and relevant information based upon the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17799:2005(E) standards.

This simple Checklist is just one of several tools available to conduct information security risk assessments. More advanced risk assessment tools can be found on the Office of Information Security and Privacy Protection Web site at www.infosecurity.ca.gov/risk/.

Information Security Risk Assessment Checklist
A High-Level Tool to Assist State Agencies with Risk Analysis

	Yes/No
A. Organizational and Management Practices	
1. <u>Security Program Governance</u> – Executive Management has assigned roles and responsibilities for information security across its organization. This includes, but is not limited to, the following: documenting, disseminating, and periodically updating a formal information security program that addresses purpose, scope, roles, responsibilities, applicable laws and regulations, and the implementation of policies, standards, and procedures.	No
2. <u>Confidentiality Agreements</u> – Implement confidentiality or non-disclosure agreements with contractors and external entities to ensure the agency’s needs for protection of classified information is met.	Yes
3. <u>Risk Assessments</u> – A review process at planned intervals is implemented to ensure the continuing suitability and effectiveness of the agency’s approach to managing information security.	Yes
4. <u>System Security</u> – A formal document that provides an overview of the security requirements for agency information systems and describes the security controls in place (or planned) for meeting those requirements is maintained.	Yes
5. <u>System Certification</u> – An assessment of the security controls in place for existing systems and those planned for new systems is conducted at least once each year. Assessment tools are readily available through security organizations, like National Institute of Standards and Technology (NIST), SysAdmin, Audit, Network, Security (SANS) Institute, and other reputable sources. The agency’s ISO reviews and approves actions taken to correct any deficiencies identified. Responsible technical or operational management are included in the review process.	Yes
6. <u>Configuration Change Control</u> – Changes made to information systems are controlled and documented. The changes are reviewed and approved in accordance with written policy and procedures, including a process for emergency changes.	Yes
7. <u>Security Categorization</u> – Procedures to classify systems and information that is stored, processed, shared, or transmitted with respect to the type of data (e.g., confidential or sensitive) and its value to critical business functions are in place.	No
8. <u>Vulnerability Scanning</u> – A regular occurring (e.g., bi-annual, quarterly, monthly) process using specialized scanning tools and techniques that evaluates the configuration, patches, and services for known vulnerabilities is employed.	Yes
B. Personnel Practices	
1. <u>Security Awareness</u> – Training is provided to all employees and contractors on an annual basis that addresses acceptable use and good computing practices for systems they are authorized to access. Content of training is based on the agency’s policies addressing issues, such as, privacy requirements, virus protection, incident reporting, Internet use, notification to staff about monitoring activities, password requirements, and consequences of legal and policy violations.	No
2. <u>Human Resources Security</u> – Policies and procedures that address purpose, scope, roles, responsibilities, and compliance to support personnel security requirements, such as access rights, disciplinary process, etc. are in place.	Yes

	Yes/No
3. <u>Position Categorization</u> – Procedures for identifying system access needs by job function and screening criteria for individuals performing those functions are in place.	No
4. <u>Personnel Separation</u> – A process to terminate information system and physical access and ensure the return of all agency-related property (keys, id badges, etc.) when an individual changes assignments or separates from the agency is developed and implemented.	Yes
5. <u>Third Party or Contractor Security</u> – Personnel security requirements for third-party providers and procedures to monitor compliance are in place. Requirements are included in acquisition-related documents, such as service-level agreements, contracts, and memorandums of understanding.	Yes
6. <u>Personnel Screening</u> – Employee history and/or a background check is performed on employees who work with or have access to confidential or sensitive information or critical systems.	No
C. Physical Security Practices	
1. <u>Physical and Environmental Program</u> – Policy and procedures that address the purpose, scope, roles, responsibilities, and compliance for physical and environmental security, such as security perimeter and entry controls, working in secure areas, equipment security, cabling security, fire detection and suppression, room temperature controls, etc. are in place.	Yes
2. <u>Physical Access Monitoring</u> – The need for monitored access to business areas is evaluated. In monitored areas, records for approved personnel access and sign-in sheets for visitors are maintained. Logs are periodically reviewed, violations or suspicious activities are investigated, and action is taken to address issues.	Yes
3. <u>Physical Access Control</u> – Physical access to facilities containing information systems is controlled and individual's authorization is verified before granting access.	Yes
4. <u>Environmental Controls</u> – The necessary environmental controls, based on a requirements assessment, which includes but is not limited to backup power to facilitate an orderly shutdown process, fire detection and suppression, temperature and humidity controls, water damage detection and mitigation are provisioned and properly maintained.	No
5. <u>Secure Disposal of Equipment</u> – Processes are in place to permanently remove any sensitive data and licensed software prior to disposal.	Yes
D. Data Security Practices	
1. <u>Operational Recovery Planning</u> – An Operational Recovery Plan (ORP) is in place that supports the current business continuity needs of the agency. The ORP plans for the recovery of technology and communications following any major event that disrupts the normal business environment, provides for periodic updating and testing of the plan, and its documentation includes, but is not limited to:	Yes
• Recovery based on critical and sensitive business needs.	Yes
• Location of regular backups of systems and data, with documentation.	Yes
• Regularly updated information about where copies of the plan reside, including appropriate off-site locations.	Yes
• Training for appropriate personnel.	Yes
2. <u>Information Back-up</u> – Backup copies of information and software are completed on a routine schedule, tested regularly, and stored off-site.	Yes

	YES/NO
3. <u>Monitoring</u> – System logging, and routine procedures to audit logs, security events, system use, systems alerts or failures, etc. are implemented and log information is in place where it cannot be manipulated or altered.	No
4. <u>Data Classification</u> – Policies and processes to classify information in terms of its value, legal requirements, sensitivity, and criticality to the organization are in place.	No
5. <u>Access Controls</u> – Policies and procedures are in place for appropriate levels of access to computer assets. Access controls include, but are not limited to:	
<ul style="list-style-type: none"> • Password management, including the use of strong passwords, periodic password change, and restriction of sharing access and/or passwords. System access is authorized according to business need and password files are not stored in clear text or are otherwise adequately protected. 	Yes
<ul style="list-style-type: none"> • Wireless access restrictions are in place, with organizational control over access points, prohibition and monitoring against rogue access points, appropriate configuration of wireless routers and user devices, and policy, procedure, and training for technical staff and users are in place. 	No
<ul style="list-style-type: none"> • Secure remote access procedures and policies are in place, and are known and followed by users. 	Yes
<ul style="list-style-type: none"> • Mobile and portable systems and their data are protected through adequate security measures, such as encryption and secure passwords, and physical security, such as storing devices in a secure location and using cable locking devices. 	No
<ul style="list-style-type: none"> • The tracking of access and authorities, including periodic audits of controls and privileges is in place. 	No
<ul style="list-style-type: none"> • Networks challenge access requests (both user and system levels) and authenticate the requester prior to granting access. 	Yes
6. <u>Least Privilege</u> – Configuration to the lowest privilege level necessary to execute legitimate and authorized business applications is implemented.	No
7. <u>Data Storage and Portable Media Protection</u> – Policies and procedures to protect data on electronic storage media, including CDs, USB drives, and tapes are in place. Procedures include labels on media to show sensitivity levels and handling requirements, rotation, retention and archival schedules, and appropriate destruction/disposal of media and data.	No
E. Information Integrity Practices	
1. <u>Identification and Authentication</u> – Policies and procedures for identification and authentication to address roles and responsibilities, and compliance standards are in place.	No
2. <u>User Identification and Authentication (typically userid and password)</u> – Information systems/applications uniquely identify and authenticate users when it is appropriate to do so.	Yes
3. <u>Device Identification and Authentication</u> – Information systems/applications identify and authenticate specific devices before establishing a connection with them.	No
4. <u>System and Information Integrity</u> – Policies and procedures for system and information integrity to address roles, responsibilities, and compliance standards are in place.	No
5. <u>Malicious Code Protection</u> – A regular patching process has been implemented to protect against malicious code. The process is automated when possible.	Yes

	YES/NO
6. <u>Intrusion Detection</u> – Tools and techniques are utilized to monitor intrusion events, detect attacks, and provide identification of unauthorized system use.	Yes
7. <u>Security Alerts and Advisories</u> – The appropriate internal staff members receive security alerts/advisories on a regular basis and take appropriate actions in response to them.	Yes
8. <u>Secure System Configuration</u> – The security settings on systems are configured to be appropriately restrictive while still supporting operational requirements. Non-essential services are disabled or removed when their use is not necessary as to eliminate unnecessary risk.	Yes
9. <u>Software and Information Integrity</u> – Information systems/applications detect and protect against unauthorized changes to software and information.	No
10. <u>Information Input Accuracy, Completeness, and Validity</u> – Information systems/applications check data inputs for accuracy, completeness, and validity.	No
11. <u>Flaw Remediation</u> – Information system/application flaws are identified, reported, and corrected.	Yes
F. Software Integrity Practices	
1. <u>System and Services Acquisition</u> – Policies and procedures for system and services acquisition are in place to address roles and responsibilities, and processes for compliance checking.	Yes
2. <u>Software Integrity Practices</u> – Policies and procedures associated with system and services acquisition and product acceptance are in place.	
<ul style="list-style-type: none"> Acquisitions – Security requirements and/or security specifications, either explicitly or by reference, are included in all information system acquisition contracts based on an assessment of risk. 	Yes
<ul style="list-style-type: none"> Software Usage Restrictions – Controls or validation measures to comply with software usage restrictions in accordance with contract agreements and copyright laws are in place. 	Yes
<ul style="list-style-type: none"> User Installed Software – An explicit policy governing the downloading and installation of software by users is in place. 	No
<ul style="list-style-type: none"> Outsourced Information System Services – Controls or validation measures to ensure that third-party providers of information system services employ adequate security controls in accordance with applicable laws, policies and established service level agreements are in place. 	Yes
<ul style="list-style-type: none"> Developer Security Testing – A security test and evaluation plan is in place, implemented, and documents the results. Security test results may be used in support of the security certification process for the delivered information system. 	No
G. Personal Computer Security Practices – Personal computing devices include desktops, laptops, notebooks, tablets, Personal Device Assistants (PDA), and other mobile devices.	
1 <u>Device Hardening</u> – Operating system and application level updates, patches, and hot fixes are applied as soon as they become available and are fully tested. Services on the computing devices are only enabled where there is a demonstrated business need and only after a risk assessment.	Yes

	YES/NO
2. <u>Lock-Out for Inactive Computing Devices</u> – The automatic locking of the computing device after a period of inactivity is enforced.	No
3. <u>Data Storage</u> – Data that needs additional protection is stored on pre-defined servers, rather than on computing devices, for both data protection and backup/recovery reasons. Confidential, sensitive, and/or personal (notice-triggering) information is not stored on computing devices without a careful risk assessment and adequate security measures.	Yes
H. Network Protection Practices	
1. <u>Network Protection</u> – Network and communication protection policies and procedures are in place. These documents outline the procedures to authorize all connections to network services. Authorization is based on an evaluation of sensitive or critical business applications, classification of data stored on the system, and physical location of the system (e.g., public area, private access, secure access, etc.).	Yes
2. <u>Boundary Protection</u> – Equipment designed for public access (i.e. Web servers dispensing public information) is protected. These are segregated from the internal networks that control them. Access into internal networks by authorized staff is controlled to prevent unauthorized entry.	Yes
3. <u>Protect and Secure Network Infrastructure</u> – Policies and procedures for technology upgrades, network equipment (e.g., servers, routers, firewalls, switches), patches and upgrades, firewall and server configurations, and server hardening, etc are in place.	Yes
4. <u>Transmission Integrity and Confidentiality</u> – Data is protected from unauthorized disclosure during transmission. Data classification is used to determine what security measures to employ, including encryption or physical measures.	Yes
I. Incident Response Practices	
1. <u>Incident Response</u> – Incident response policies and procedures consistent with applicable laws and state policies are in place. These include but are not limited to identification of roles and responsibilities, investigation, containment and escalation procedures, documentation and preservation of evidence, communication protocols, and lessons learned.	Yes
2. <u>Incident Reporting</u> – Proper incident reporting policies and procedures are in place. These include training employees and contractors to identify and report incidents, the reporting of incidents immediately upon discovery, and preparation and submission of follow-up written reports.	Yes