February 3, 2016

Marybel Batjer, Secretary
California Government Operations Agency
915 Capitol Mall, Suite 200
Sacramento, CA 95814

Dear Ms. Batjer,

In accordance with the State Leadership Accountability Act (SLAA), the State Personnel Board submits this report on the review of our systems of internal control and monitoring processes for the biennial period ended December 31, 2015.

Should you have any questions please contact Mark Rodriguez, Chief, Administrative Services Division, at (916) 322-6351, Mark.Rodriguez@spb.ca.gov.

BACKGROUND

Established by the State Constitution, the State Personnel Board (SPB) is charged with overseeing the merit-based, job-related recruitment and selection process for the hiring of state employees who provide critical services to the people of California. SPB provides direction to departments through simplifying civil service laws, rules, and policy. In addition, SPB conducts compliance reviews of departments for merit system compliance, and adjudicate employee appeals from disciplinary actions.

SPB also investigates and adjudicates alleged violations of civil service law, which are filed by employees, applicants, and members of the public.

RISK ASSESSMENT PROCESS

SPB Division chiefs performed a high level review of their respective programs and determined which current issues could potentially be a risk to SPB over the next two years. The risk assessment identified are:

* Identification of critical business functions
  * Determination of risk factors: high, medium, or low
  * Description of risks to the department
  * Creation of an action plan that resolves or mitigates the risk

As outlined below, SPB’s greatest concerns are with technology and data security. Integrity and security for SPB’s electronic files remains the focal point for evaluating risk to all operations. Some systems rely upon complex databases utilizing a robust document management system and document repository as the primary user interface. Impairment in the operations of any of these programs could result in substantial delay in performing program obligations. Further, corruption of core pieces of data may require substantial efforts to reconstruct damaged files which would also impair the ability of SPB to render services. Currently, SPB relies upon strong encryption, timely application of patches and upgrades, recurrent backup procedures, and appropriate system supervision. To accomplish these tasks, SPB relies upon the Department of Human Resources (CalHR) to provide technical support for all information technology processes.

EVALUATION OF RISKS AND CONTROLS

Operations- Internal- Physical Resources—Maintenance, Upgrades, Replacements, Security
SPB headquarters does not have adequate security within the six-floor facility. Security is stationied only on the ground floor and is unable to perform security checks on the remaining floors of the facility without leaving the visitor counter unattended. The SPB maintains confidential files concerning various personnel issues. Personnel from other tenants in the building have been observed entering onto a floor occupied by SPB.

SPB personnel are trained to inform management when non-approved visitors are observed within SPB space. Management will take steps to have the person leave the premises. The Department of General Services (DGS) has informed SPB that additional tenants will be co-locating within SPB headquarters within the next year. It is critical that access to SPB floor remain restricted to SPB staff only.

**Operations- Internal- Technology—Data Security**

SPB staff may accidentally alter electronic files or release confidential files.

The Appeals Division staff are trained on the appropriate protocols for editing data maintained in case files. Release of data to outside requestors is managed by the records office which works closely with the SPB Legal Division.

**Operations- Internal- Technology—Inadequate Support, Tools, Design, or Maintenance**

All appeals and complaints are maintained in digital format (electronic files). Should the system catastrophically fail, SPB would be unable to perform its constitutional and statutory duty to process appeals from disciplinary actions and other merit-based determinations.

Primary responsibility for maintaining the integrity of SPB’s electronic data rests with the Information Technology Division at CalHR. Accordingly, responsibility for maintaining the computer programs housing the electronic files is under the direct control of CalHR. To mitigate risks associated with SPB’s electronic data, it is imperative that all related computer programs receive timely updates and maintenance. Further, all electronic data and associated systems, must be digitally backed up and appropriately stored in an offsite location to facilitate recovery in case of a system failure. Security protocols shall meet requirements by the Department of Technology and SPB staff will continue ongoing training for security awareness and appropriate practices. It is critical that CalHR continue to work with SPB to ensure the security of all electronic data.

**Operations- Internal- Technology—Data Security**

Necessity to store documents (physical and electronic) which may contain highly sensitive personal and personnel information regarding individuals in the performance of compliance review.

When provided with physical documentary information from departments pertaining to compliance reviews, staff are instructed to utilize scanners to scan pertinent information into their assigned laptops and then directly into a secure database. Scanned documents are returned to the department. No physical or documentary information other than software is to remain on the hard drives. In the event that hard copy documents are brought to the office, then the “clean desk policy” is utilized when reviewing documents. When review is finished for the day, all documents are locked in cabinets. Once a review is completed, hard copy documents are scanned and destroyed. Scanned information is retained in a secure database according to SPB’s retention policy.

**Operations- Internal- Technology—Data Security**

Necessity for staff to utilize portable computing devices (laptops) in the performance of compliance reviews.
All laptops and databases are encrypted and password protected. Staff are instructed to take special care to secure laptops when out of the office and on-site at departments. Staff are prohibited from leaving laptops in automobiles, and laptops are to be stored in a secure location outside the office.

**Operations- External- Technology—Data Security**

All appeals and complaints are established and maintained in digital format (electronic files). Some appeal and complaint files contain personal information required to be treated as confidential. Malware and hacking activities would disrupt the functionality of the system. Further, any impairment to the system’s security may result in the inadvertent disclosure of confidential information.

Primary responsibility for maintaining the integrity of SPB’s electronic data rests with the Information Technology Division at CalHR. Accordingly, responsibility for maintaining the computer programs housing the electronic files is under the direct control of CalHR. To mitigate risks from malware, viruses and hacking activity, CalHR employs antivirus on clients and servers, an intrusion prevention system to mitigate network attacks, and controlled access via firewalls for protecting internal and external resources. In addition, web filtering and spam filtering systems are in place in order to prevent web and email attacks. Further, it is imperative that all related computer programs receive timely updates and maintenance while all electronic data and associated systems, are digitally backed up and appropriately stored in an offsite location to facilitate recovery in case of a system failure. Security protocols shall meet requirements by the Department of Technology and SPB staff will continue ongoing training for security awareness and appropriate practices. It is critical that CalHR continue to work with SPB to ensure the security of all electronic data.

**Operations- External- Staff—Recruitment, Retention, Staffing Levels**

Administrative Law Judges (ALJ) continue to be paid a lower salary than the equivalent attorney classification. Recruiting high quality attorneys from within state civil service from the highest job classifications is nearly impossible.

Currently, there is no control available to the Appeals Division at this time. SPB will strive to continue quality recruitment to the extent possible.

**Operations- External- Business Interruption, Safety Concerns**

The Appeals Division adjudicates cases involving employee discipline. Appellants may become emotionally charged over the issues arising in these matters resulting in threats of violence or actual violence towards Appeals staff.

Cases are reviewed for issues related to potential violence, and, when appropriate, a CHP officer is present during a hearing.

**Operations- External- Business Interruption, Safety Concerns**

SPB headquarters is not equipped with fire sprinklers.

The SPB building is managed by DGS. SPB does not have any control over the facility.

**Operations- External- Business Interruption, Safety Concerns**

SPB ALJs travel throughout the state to conduct hearings. Each ALJ is provided a laptop while traveling to record SPB hearings. Theft of the laptop may result in the dissemination of confidential information and may impair the ability to provide a complete administrative record for the hearing.

ALJs receive training concerning their obligation to ensure the security of assigned SPB
equipment, including laptops. Each laptop is password protected and all data storage units have encryption software.

**ONGOING MONITORING**

Through our ongoing monitoring processes, the State Personnel Board reviews, evaluates, and improves our systems of internal controls and monitoring processes. As such, we have determined we comply with California Government Code sections 13400-13407.

**Roles and Responsibilities**

As the head of State Personnel Board, Suzanne Ambrose, Executive Officer, is responsible for the overall establishment and maintenance of the internal control system. We have identified Mark Rodriguez, Chief, Administrative Services Division, as our designated agency monitor(s).

**Frequency of Monitoring Activities**

SPB holds monthly management meetings and various ad hoc meetings, as necessary. In addition, the Appeals Division meets on a bi-weekly basis with managers and staff from CalHR’s Information Technology Division. System vulnerabilities are continuously identified and evaluated.

**Reporting and Documenting Monitoring Activities**

SPB requires reports from each unit on a quarterly basis. These reports inform management of the monitoring practices being conducted, improvements needed, and the overall monitoring success or weakness within each unit. This information is summarized and reported to the SPB Executive Officer.

SPB will ensure all staff receive information vital to the effectiveness and efficiency of controls by requiring management to update their teams bi-monthly. SPB encourages staff to speak with their supervisors if they discover an issue that should be addressed to better assist SPB with fulfilling its mission, goals, and objectives.

**Procedure for Addressing Identified Internal Control Deficiencies**

Management holds regular meetings to review any deficiencies either noted in the quarterly reports or recently identified.

SPB has a policy that all deficiencies will be mitigated within sixty days. If a mitigation procedure takes longer than sixty days, SPB requires that executive management receive bi-weekly notices until the deficiency is adequately addressed.

Finally, SPB will send an internal email to all staff to inform them of policy or procedure changes to assist in the mitigation of any deficiencies discovered.

**CONCLUSION**

The State Personnel Board strives to reduce the risks inherent in our work through ongoing monitoring. The State Personnel Board accepts the responsibility to continuously improve by addressing newly recognized risks and revising risk mitigation strategies. I certify our systems of internal control and monitoring processes are adequate to identify and address material inadequacies or material weaknesses facing the organization.
Suzanne Ambrose, Executive Officer

cc: Department of Finance
Legislature
State Auditor
State Library
State Controller
Secretary of Government Operations