December 21, 2021

Keely Martin Bosler, Director
California Department of Finance
915 L Street
Sacramento, CA 95814

Dear Director Keely Martin Bosler,

In accordance with the State Leadership Accountability Act (Leadership Accountability), the Department of Justice submits this report on the review of our internal control and monitoring systems for the biennial period ending December 31, 2021.

Should you have any questions please contact Chris Prasad, Director, at (916) 210-6271, chris.prasad@doj.ca.gov.

GOVERNANCE

Mission and Strategic Plan

The Office of the Attorney General (OAG) was established by the California Constitution in 1850 to uniformly and equally enforce California's laws. The Office carries out its responsibilities through the divisions and programs of the Department of Justice (Department/DOJ).

Following his appointment, on April 23, 2021, Rob Bonta was sworn in as the 34th Attorney General of the State of California. The Attorney General heads the DOJ as the state's chief law officer and is responsible for protecting and serving California's people and interests through a broad range of duties, including promoting public safety, safeguarding California's natural resources and environment, enforcing civil rights laws, protecting Californians' right to access affordable healthcare, and helping victims of illegal business practices, fraud and other consumer crimes. The Attorney General also provides regulatory oversight, oversees charitable organizations in the state, coordinates with law enforcement agencies (LEAs) to carry out enforcement efforts, and conducts state-level investigations.

Attorney General Bonta, with the help of his dedicated employees, represents the People in matters before the appellate and Supreme Courts of California and the United States, serves as legal counsel to state agencies, coordinates inter jurisdictional efforts to fight crime, provides identification and information services to criminal justice agencies, and pursues projects in his independent capacity to protect the People of California from fraudulent, unfair, and illegal activities.

The Department consists of seven divisions and executive programs. The Chief Deputy Attorney General (CDAG) and the Chief of Staff, under the direction of the Attorney General, lead an executive team of seven chiefs and a Solicitor General that oversee the following divisions and offices:

- Division of Law Enforcement (DLE)
- Legal Programs:
    - Civil Law Division

  - Criminal Law Division
  - Division of Medical Fraud and Elder Abuse
  - Public Rights Division
  - Office of Solicitor General
- California Justice Information Services Division (CJIS)
- Division of Operations (OPS)

The Department consists of approximately 5,000 employees including attorneys, peace officers, auditors, information technology specialists, accounting and administrative professionals, executive staff, and security personnel. In addition to investigative field offices statewide, the Department's primary legal offices are located in Sacramento, Los Angeles, San Francisco, San Diego, Oakland, and Fresno.

Attorney General Bonta has placed a priority on consumer protection, environmental justice, criminal justice reform, civil rights, healthcare, addressing hate crimes, and rebuilding trust between communities and law enforcement. To that end, in July 2021, Attorney General Bonta launched the Office of Community Awareness, Response, and Engagement (CARE), which works directly with community organizations and the public to raise the level of diverse perspectives in the state's work, and provides opportunities for the public to learn about and directly engage with the OAG. CARE focuses on cultivating relationships with historically marginalized and underrepresented communities in line with DOJ's commitment to diversity, equity, and inclusion for all.

In order to ensure public safety in a dynamic political and legal landscape, DOJ's other current initiatives focus on certain emerging and long-standing matters, including:

- Protecting consumers, housing opportunities, and public heath efforts during the COVID-19 crisis;
- Enforcing laws prohibiting price gouging during a state of emergency;
- Safeguarding affordable healthcare through the Affordable Care Act;
- Enhancing data privacy and cybersecurity;
- Combatting human-trafficking and gun trafficking operations;
- Reestablishing trust between law enforcement and the communities they serve, and promoting accountability through pattern and practice investigations, MOUs, and otherwise overseeing local LEAs;
- Addressing racial bias and hate;
- Advocating for environmental justice and enforcing environmental laws;
- Honoring California's indigenous and tribal communities;
- Putting a stop to recycling fraud schemes;
- Prosecuting white collar crimes;
- Improving oversight of charitable giving on online platforms;
- Combatting sexual assault and domestic violence;
- Assisting local LEAs with eliminating the back log of untested rape kits;
- Protecting service members and vulnerable communities from scams and predatory practices;
- Safeguarding elders from physical and financial abuse;
- Guiding and informing tenants and homeowners of their rights and protections under Californian law;

- Fighting against injustice in the workplace;
- Strengthening the protections of skilled nursing facility residents;
- Working to stop gun violence by defending California's commonsense gun laws, and strengthening California's first in the nation Armed and Prohibited Persons System (APPS) program and enforcing laws on ghost guns;
- Protecting voting rights;
- Leading and joining multistate coalitions in support of various lawsuits, including those against opioid distributors and manufacturers, and those which combat anticompetitive practices in multiple sectors, from technology to healthcare; and
- Investigating and prosecuting officer-involved shootings pursuant to Assembly Bill 1506 (McCarty).

Control Environment

Under the direction of the CDAG and the Chief of Staff, the executive team maintains high ethical standards and attentive oversight of the Department. Oversight also occurs as a function of various mandated legislative reporting, with which DOJ regularly cooperates. Financial records are audited as part of the federal single audit facilitated by the Department of Finance (DOF), and DOJ undergoes several audits, including those initiated by the Legislature, the California State Auditor, the State Controller's Office, the Department of General Services, the U.S. Treasury, and the U.S. Office of Inspector General. The CDAG and division chiefs review the results of these audits, develop corrective action plans, and correspond with the auditors and the Legislature regarding implementation of corrective actions and improved internal controls.

As California's primary litigation and law enforcement body, DOJ is committed to upholding the highest standards of ethics and integrity. DOJ maintains the Department of Justice Administrative Manual (DOJAM), Legal Guidelines, and the Division of Law Enforcement Policy and Procedures Manual on the Department's intranet. These manuals are dynamic documents that articulate DOJ policies, procedures, and organizational structure for the entire agency, with particular emphasis on employee conduct in the office and in the field.

DOJ maintains organizational staffing charts and a managerial hierarchy that ensure policies and procedures are developed and disseminated throughout the Department. The Department's organizational structure delegates decision-making authority to the most qualified staff at various management levels. This structure groups employees by division and function to ensure appropriate segregation of duties and ensures sufficient levels of review for staff work. This structure also allows for the effective execution of duties and ensures accountability within the chain of command.

To help identify potential conflicts of interest, DOJ requires staff holding a position that is described in Government Code section 87200 or designated in a local conflict of interest code pursuant to Government Code section 83700, to annually file the Statement of Economic Interest (Form 700). The Department also requires all designated employees to complete a State Officials Ethics Training Course. Legal staff receive additional training on conflicts of interest, recusals, disqualifications, and removals. DOJ also requires staff to sign a Statement of Incompatible Activities that explicitly prohibits employees from using the skills, tools and influence associated with their position for private gain or outside of their prescribed duties for the Department when they are hired.

As part of creating a positive, safe work environment, and to strengthen staffs' understanding of fraud

and adhere to their responsibility for assessing and reporting fraud, DOJ provides staff with several avenues to report misconduct by employees and management. The California State Auditor's (CSA) Whistleblower Hotline is noticed in employee break areas throughout the agency and electronic copies of these brochures are sent to all DOJ employees with email accounts. DOJ monitors staff work and responds to whistleblower inquiries forwarded from the CSA and other avenues. It investigates these internally or cooperates with other state entities to ensure accountability for all employees. To report suspected Workers' Compensation Fraud, brochures of the State Compensation Insurance Fund are placed throughout the Department. Additionally, DOJ works to prevent interpersonal misconduct in the workplace through outreach and education by regularly training employees in the prevention of discrimination, harassment, and retaliation. It also provides access to reporting of these types of complaints internally via its Office of Equal Employment Rights and Resolution, and provides other avenues for resolution at the agency, state, and federal level, depending on the nature of the complaint and the employee's needs and preferences.

DOJ employees regularly encounter sensitive information as part of their day-to-day work. To safeguard public and personal information, DOJ employees undergo mandated privacy and information awareness training during orientation as well as periodically, as DOJ identifies new resources and training needs related to information security. Additionally, employees accessing highly-sensitive information undergo an extensive background investigation prior to being granted access.

DOJ complies with the California Department of Human Resources workforce and succession plan requirements through its Office of Human Resources (OHR). DOJ has developed a working strategy to recruit, develop and retain a diverse, well-qualified workforce. Furthermore, divisions coordinate with the OHR to develop specific recruiting methods and applicant pools to help add staff, reduce dependencies on certain staff, and to ensure that hiring is fair and unbiased. The Department aims to create hiring programs that attract a diverse field of promising potential employees. The Department ensures equal employment opportunities within DOJ, through its Equal Employment Rights and Resolution Office. The DOJ Equal Employment Opportunity Advisory Committee and its nine Employee Advisory Committees are charged with making recommendations to the Attorney General for improvements and changes to the Department's Equal Employment Opportunity (EEO) program, personnel practices, and other management practices that may impact EEO within the department. Consistent with state law, DOJ ensures that all supervisors receive 80 hours of supervision training upon assuming their leadership roles. In addition, all supervisors and managers are required to receive 20 hours of leadership training every two years. The agency also maintains in-house training staff to coordinate and deliver training across the Department.

Information and Communication

In and across divisions, DOJ's internal communication structure supports a precise and effective flow of information. Departmental policies originate from OPS, the CJIS Information Security Officer, the CDAG, or the Attorney General, depending on the subject matter. DOJ uses email and a robust interoffice mail routing system that ensures that individuals and units receive relevant information in a timely manner. DOJ also uses an internal intranet system to provide ongoing updates, documents, and resources for employees to access.

The Department's Public Inquiry Unit manages all questions and comments from the public. This unit is responsible for routing calls received on the Public Inquiry Hotline to the appropriate individual or team

within DOJ. This hotline allows DOJ to obtain information from the general public to better understand where and how to direct its resources proactively. The Department's Victims Services Unit offers crime victims and their families support and information at every stage of the criminal process. Victims have rights, and the Attorney General is committed to ensuring that those rights are protected. Both of these public facing units reside within the CARE Office.

MONITORING

The information included here discusses the entity-wide, continuous process to ensure internal control systems are working as intended. The role of the executive monitoring sponsor includes facilitating and verifying that the Department of Justice monitoring practices are implemented and functioning. The responsibilities as the executive monitoring sponsor(s) have been given to: Chris Prasad, Director; Matthew Rodriquez, Chief Deputy Attorney General;
Joe Dominic, Chief, Division of California Justice Information Services; and
Chris Ryan, Chief, Division of Operations.

The role of the executive monitoring sponsor includes facilitating and verifying that DOJ's monitoring practices are implemented and functioning and that internal control systems are working as intended. The responsibilities as the executive monitoring sponsor(s) have been given to: Venus D. Johnson, CDAG; Chris Ryan, Chief, OPS; and Chris Prasad, Director, Office of Program Oversight and Accountability (OPOA). DOJ relies on regular meetings, event-driven programming and budget changes, and ongoing insight and consultation with its OPOA to identify and track risks. OPOA is designated as the primary internal audit organization and conducts independent and objective reviews of accounting and administrative controls of programs in order to identify potential fraud, waste, and abuse. OPOA also provides recommendations to streamline operations, increase effectiveness, improve efficiency, and mitigate risk.

The current process for ongoing monitoring is described below. As new information surfaces, the Executive team revises these processes accordingly. On a regular basis (daily, weekly, or monthly):

- DOJ executive management meets to discuss existing and potential risks;
- Management staff throughout DOJ meet to discuss how to address potential and existing risks; and
- Each division chief meets with the CDAG to discuss policies and procedures to address outstanding risks.

Under the CDAG's direction, the following actions occur every six months to one year:

- Division leaders update the SLAA Implementation Plan regarding status on controls implementation as required by the DOF;
- OPOA assists each division chief with measuring and tracking progress on internal controls development, implementation, and evaluation; and
- OPOA collects data from divisions to assess the extent of the risk.

Biennially (every two years), under the CDAG's direction:

- Division leaders conduct risk assessments and additional organizational surveys to assist with identifying risks and internal controls at the division and enterprise level;
- Division leaders maintain a list of risks to include in the next SLAA report;

- OPOA reviews strategic initiatives, organizational and environmental challenges, risk assessment results, and other factors to identify enterprise risks and develop controls; and
- Division leaders continuously evaluate risks and threats to DOJ's operations.

RISK ASSESSMENT PROCESS

The following personnel were involved in the Department of Justice risk assessment process: executive management, middle management, and front line management.

The following methods were used to identify risks: brainstorming meetings, employee engagement surveys, ongoing monitoring activities, audit/review results, other/prior risk assessments, external stakeholders, questionnaires, and consideration of potential fraud.

The following criteria were used to rank risks: likelihood of occurrence, potential impact to mission/goals/objectives, timing of potential event, and tolerance level for the type of risk.

The following personnel were involved in the DOJ risk assessment process:

- Executive management;
- Middle management; and
- Front-line management.

The following methods were used to identify risks:

- Brainstorming meetings;
- Employee engagement surveys;
- Ongoing monitoring activities;
- Audit/review results;
- Other/prior risk assessments;
- External stakeholders; and
- Questionnaires and consideration of potential fraud.

The following criteria were used to rank risks:

- Likelihood of occurrence;
- Potential impact to mission/goals/objectives;
- Timing of potential event, potential impact of remediation efforts; and
- Tolerance level for the type of risk, and other factors.

In addition to these risk factors, divisions were asked to assess their level of risk and categorize it according to its strategic, financial, compliance, reporting, or reputational risk.

RISKS AND CONTROLS

Risk: Insufficient Resources

DOJ performs its mandated duties based on annually appropriated resources, but often is unable to meet new legislative mandates with existing staff and resources without compromising current workload.

The Bureau of Firearms needs an urgent infusion of about $5.2 million to ensure the next phases of the Firearms Information Technology Systems Modernization (FITSM). The existing firearms systems utilized by the DOJ, LEAs, and other firearm stakeholders, have reached their end-of-life. A modern network of systems are required for DOJ to respond to changing business needs and legislative mandates. The current systems and their subsequent modifications or enhancements were developed in response to legislative mandates implemented since the first system was built, in 1980. Furthermore, the network of these systems has now become increasingly complex, with each system using different logic that cannot be applied to modifications needed across multiple systems.

Furthermore, these systems have been stitched in a patchwork manner, which is not efficient and has led to a tightly-coupled system. A modification within one application requires timely and extensive testing of many systems to ensure there is no negative impact to other applications. These systems can no longer be enhanced in a cost effective or efficient manner and cannot be further utilized to implement the changing needs of law enforcement and California as a whole. The systems were designed to meet user needs based on outdated system design practices and point-in-time business requirements. The current design method results in significantly longer development times, requires more resources, and requires longer and more extensive regression testing, making it difficult to respond to the constantly evolving landscape of statutory mandates pertaining to firearms. These systems and architecture are time consuming, expensive, and wearing down. If the DOJ is unable to develop and implement the FITSM solution, the result would be an in increase in workload.

In addition, to efficiently provide crime lab services, further resources are required. The Bureau of Forensic Services (BFS) can unite several program areas between the various regional laboratories. Continued bifurcation of program resources and tenancy in dilapidated facilities has led to inefficiencies, staff frustration, and poor fiscal stewardship.

Control: A

Internally, DOJ's legal divisions, DLE, CJIS, and OPS continue to communicate with one another regarding implementation of new statutes in order to monitor and identify mandates that remain unfulfilled due to budget, staffing, and statutory constraints. This helps ensure that DOJ maintains compliance with statutory mandates.

Control: B

As the Department determines workload and identifies necessary resources, DOJ works with the Governor's Office, the DOF and the Legislature to obtain needed resources.

Risk: Data and Information Security

DOJ maintains data that can include confidential and personal identifying information. DOJ manages data security and privacy by implementing appropriate security technologies, as well as developing and implementing information policies, standards, guidelines, and procedures. These technologies and policies are continuously modernized to accommodate the changing demands of a modern environment in public safety and justice. Existing safeguards continue to reduce the likelihood of successful attempts at infiltration of systems and data by malicious actors. Technologies and processes must continuously be explored to ensure a strong security posture since malicious actors continuously try to find ways to exploit vulnerabilities.

External entities and internal DOJ processes rely on timely access to DOJ databases for tasks such as background checks, criminal history searches, case management, and email services. To meet growing demand, DOJ must take steps to modernize its systems and databases to ensure that they are robust and reliable. Furthermore, modernizing these systems will ensure accessibility and scalability to enable DOJ to quickly respond to requests and keep pace with customer demand.

DOJ received $2 million in additional funding to enhance cybersecurity and safeguard the integrity and security of the California Law Enforcement Telecommunications Systems (CLETS) and other DOJ information systems and assets. DOJ established a Cybersecurity Branch as a result. The branch performs security scans of IT assets, reviews security of LEAs, researches organizations that access DOJ data, and monitors cybercrimes and security events. The branch also communicates with the DOJ's IT sections to ensure security of new projects and system changes. However, as cybersecurity rapidly evolves, DOJ needs to have adequate resources and expertise to enhance current safeguards. DOJ must continue to:

- Recruit cybersecurity positions as well as continue to support and advocate for resources to facilitate the development of cybersecurity expertise;
- Update cybersecurity policies and IT standards to ensure compliance with SAM/FBI requirements and address any changes to technology that DOJ has implemented or will implement; and
- Research security products that can either replace legacy products or enhance existing security products to ensure that DOJ can respond to current and future security threats.

Control: A

DOJ must vigilantly maintain data security across all of its systems and databases through continuous security monitoring, or else risk a serious breach of critical, often confidential data in its purview.

Control: B

DOJ will continue to use security awareness training curriculum and continue to perform phishing exercises to train new and current employees on current security policies, practices and threats. DOJ will continue to train staff on how to identify such threats (threat hunting), and the ability to stop threats and remediate actions against DOJ. DOJ is actively sourcing training companies to meet the needs of the curriculum.

Control: C

To mitigate the risk associated with unauthorized use, access, modification, loss, destruction, or disclosure of information assets, the DOJ Information Security Officer will ensure the Cybersecurity Branch sections will maintain and update security policies, standards, guidelines, processes, procedures, and best practices. This will further strengthen DOJ's security program and protect its information assets. DOJ's Cybersecurity Branch will continue to biennially perform third-party independent technical penetration tests of DOJ applications and systems.

Control: D

DOJ will continue to consider modernizing its information assets to ensure the availability confidentiality of the Department's systems.

Risk: Cybercrime

Cybercrime continues to be on the rise, including serious financial crimes, human trafficking rings, and drug sales originating from a segment of the web known as the "dark web." Californians lack a method for reporting and prosecuting cybercrime at the local and state level, as there is no central clearinghouse for these types of crimes. Because DOJ lacks sufficient resources to address these crimes, the majority of LEAs direct cybercrime complaints to the FBI. However, California cannot count on federal regulatory enforcement to reliably investigate and prosecute regional and statewide activities because of its focus on other types of national and international crime. The gap in protection continues to exist for cybercrime as it relates to regional and statewide activity because California lacks resources and expertise.

As cybercrime rapidly evolves, DOJ needs adequate resources and expertise to enhance current safeguards. Subject matter experts in California are needed to help DOJ identify training, skills, tools, and technologies that will assist local law enforcement with cybercrime prevention, detection, and prosecution. Without the necessary resources, DOJ will not be able to adequately monitor cybercrime.

Specifically, to increase monitoring of cybercrimes, DOJ must:

- Continue hiring experts in cybercrime-related matters;
- Facilitate communications with cybercrime experts within DOJ as well as from other state agencies; identify training to strengthen expertise and skills; and pursue opportunities for advancement when it is determined that an expansion in any area of the Department is critical and needed;
- Host webinars to allow digital forensics practitioners from across state service to share information and ideas among cybercrime experts throughout California state government; and
- Continue to support and advocate for additional resources to centralize technical resources for combating cybercrimes.

Control: A

Advocate for increased budgetary resources to facilitate the development of internet crime expertise.

Control: B

DOJ has consolidated its Cyber Security Branch to improve efficacies to the extent possible.

Risk: Inflexible Resources

DOJ's broad authority often leads to the agency being subject to new statutory requirements, such as the recently-enacted AB 1506 (McCarty), which requires the DOJ to investigate all incidents of officer-involved shootings resulting in the death of unarmed civilians in California. Historically, these incidents were primarily handled by local law enforcement and district attorneys. DOJ's new and important public

safety responsibility aims to reestablish trust between communities and law enforcement. DOJ is tasked with following the facts to ensure that every Californian is afforded equal justice. The DOJ estimates that $26.8 million of additional funds will be necessary in fiscal year 2022-23, and an additional $20.3 million in ongoing funding will be needed to recruit and maintain the necessary staff, and to ensure that the necessary equipment, training, and facility space is available.

The BFS has seen continued declines in its revenue sources for the DNA-ID fund (criminal fines and fees). Without a stable funding source, various forensic services may be eliminated, which would lead to delayed or terminated services, and disproportionately affect rural communities. In addition, the Legislature recently directed DOJ to provide a plan for alternate funding mechanisms for BFS by March 10, 2022. This would include an analysis on charging local agencies, but local agencies are also seeking our feedback on other potential alternatives. The result of charging local agencies for a portion of the cost — similar to fee-for-service for state-provided forensic services — is that local LEAs will be more selective with the evidence they submit to the state, which will in turn decrease the cost of running the DOJ laboratory system. In addition, rural local LEAs will not have the funding to pursue forensic services. Requiring local LEAs to pay for forensic services will lead to fiscal decisions that are not in the best interest of victims or public safety. BFS evaluates evidence to decide the most efficient path for analysis regardless of what evidence was submitted. If a local LEA is unwilling or unable to pay, the DOJ lacks a reimbursement mechanism. A decrease in funding would also defer facility maintenance as well as needed updates to equipment and technology. The alternative switch to fee-for-service for BFS operations would likely open a funding hole that the Legislature would be obligated to fill through other sources.

Control: A

DOJ will monitor its annual expenditures relative to annual spending authority to ensure that sufficient resources are available for unanticipated as well as planned work. DOJ will keep the Legislature apprised of its needs to meet all aspects of its mission.

Control: B

In addition, for BFS services, DOJ would identify alternative options to address permanent funding needs. Currently, the Legislature has asked for BFS to submit a report by March 10, 2022, that identifies options outside of the state general fund to cover its various operations. Operational costs should include facility and annual equipment replacement costs. One such option should include sharing costs with local agencies that use BFS services based on the following factors: specific type of forensic services sought, the speed of service, the size of the agency, and any other factors DOJ would like to consider.

Risk: Recruitment, Retention, and Staffing Levels

Due to specialized training needs and skill sets for DOJ classifications, management is challenged in recruiting and directing staff to assume increasingly-mandated responsibilities. Recruitment is difficult in part because DOJ salaries can't compete with the private sector or other public-sector agencies for similar work. Without sufficient staffing, DOJ risks an inability to effectively implement programs. The most impacted positions include:

Attorneys: DOJ has had difficulty recruiting, training, and retaining highly-qualified attorneys due in

part to an approximately 30% pay differential with public sector agencies. On average, DOJ experiences about a 10% vacancy rate. Vacancies force current employees to work beyond their capacity, affecting morale and retention. Some attorneys seek other employment due to heavy workload and "burnout."

Special Agents (Agents): DOJ is challenged in hiring and retaining Agents, who on average are paid approximately 37% —or about $2,200 per month — less than other LEAs. These salary disparities impact the quality of candidates. This is evident in the pre-employment background investigation process, where approximately 28% either withdraw or are disqualified from the process. Retirements are expected to exacerbate this problem: between 30% and 40 % of agent staff are eligible for retirement over the next several years. These factors, compounded by negative cultural attitudes toward law enforcement, contribute to a decreased interest in the profession. The agent classification is understaffed by approximately 34%.

IT Specialist and Investigative/Associate Auditors - It has been challenging to recruit enough IT Specialists to adequately manage and maintain DOJ's IT infrastructure. DOJ also has been unable to adequately recruit and retain auditors to audit the gaming industry, and investigative auditors for investigations of false claims, and Medi-Cal fraud and elder abuse programs. These auditors have specialized technical knowledge of the industry in identifying, tracing, and assessing cash proceeds, related party transactions, conflict of interest due to family and friend-based employment, embezzlement, investment schemes, Medi-Cal fraud, and identity and credit card theft. Auditors in other agencies receive an average of 17% higher compensation. This gap has contributed to up to 33% vacancy rate, resulting in delayed audits.

Control: A

To alleviate recruitment, retention and key dependency issues, DOJ has implemented workforce planning processes to identify needs for staffing and succession. To further enhance recruitment and retain adequate staffing levels, DOJ collects industry and internal data — knowledge, skills, ability, compensation, etc. — to align classifications and tasks, and takes steps to modernize the agency's hiring and recruitment processes.

DOJ will revisit and adjust its recruiting tools, including duty statements and job posting language, to more accurately reflect job duties and highlight some of the responsibilities associated with various positions. It will also leverage social media platforms and employment fairs to recruit applicants, and consider hiring incentives such as hiring above minimum pay and/or salary increases where possible.

Control: B

The Department has established an Attorney Hiring Unit (AHU) and Recruitment Unit to address these concerns, and will continue to advocate for higher salaries and attractive benefits with the applicable parties when possible. The AHU and the Recruitment Unit will continue to strategize on ways to recruit qualified candidates for the legal divisions. In addition, they will work closely with the Classification and Pay Unit and the Labor Relations Office to submit proposals to the California Department of Human Resources to address disparities and improve recruitment and retention when appropriate. The legal divisions will continue to work with the Recruitment Unit and AHU to support agency goals.

Control: C

For Special Agents, DOJ has also resumed a program that allows individuals with less experience to onboard as trainees and to eventually develop into Special Agents. The DOJ has increased the frequency of its recruiting efforts, and is considering changing the minimum qualifications for Special Agents to expand the candidate pool. In addition, a pay increase of 12% was recently negotiated for the Special Agent classification. While the pay increase does not completely provide parity with other LEAs, it is a step in the right direction.

CONCLUSION

The Department of Justice strives to reduce the risks inherent in our work and accepts the responsibility to continuously improve by addressing newly recognized risks and revising risk mitigation strategies as appropriate. I certify our internal control and monitoring systems are adequate to identify and address current and potential risks facing the organization.

Under the direction of Attorney General Bonta, DOJ will continue to provide indispensable public services and openly communicate about its ability to protect and defend the people and laws of the state. We look forward to our ongoing dialogue as we continue delivering the best service possible for the people of California.

Rob Bonta, Attorney General

CC: California Legislature [Senate (2), Assembly (1)]
California State Auditor
California State Library
California State Controller
Director of California Department of Finance
Secretary of California Government Operations Agency