

Initial Statement of Reasons

Title 13, Division 1, Chapter 1

Article 3.6 – Vehicle Industry and Business Enterprises

Vehicle Code section 1685 authorizes the department to establish application requirements. Part of the application requirements include documentation that establishes the department's information security criteria that ensures the department's records are maintained and accessed in a manner that protects the privacy of those records.

The department is amending Section 225.03, related to application requirements for all business partners, to require business partner applicants to submit an Information Security and Disclosure Statement Public/Private Partnerships Employee, EXEC 200X, as part of the application documentation.

The department relies on contracts and permits to regulate these business partners as permitted by Vehicle Code section 1685. In doing such, the department also relies on the business partners to protect and maintain the integrity of the department's database records by ensuring unauthorized persons do not access records, by establishing practices that prevent unauthorized persons from viewing department records, and by confidentially destroying records that are no longer needed. While the business partner is required to provide oversight of the privacy standards, the employees who access records are also responsible for protecting the departments records. The form EXEC 200X provides guidance on methods to ensure the records are kept private. The EXEC 200X requires employees, among other things, to develop strong passwords, to secure workstations, to prevent unauthorized persons from viewing or receiving records, to only update records as required in the course of their work duties, and to report any potential breaches to their supervisor.

The department is requiring the form EXEC 200X as part of the application process to serve as proof that the employee of the business partner has an understanding of their responsibilities to maintain the security of the department's records.

Subsection (d) is amended to require business partner to submit an Information Security and Disclosure Statement Public/Private Partnerships Employee, form EXEC 200X (Rev. 3/2003) as part of the application process. A form EXEC 200X is required of every owner, manager, and employee who manage, administer, supervise, or monitor transactions, inventory, employees, or money; order or account for inventory; and/or process vehicle registration transactions or work directly with customers.

The form EXEC 200X communicates the department's security standards to the user who will be accessing and updating the department's registration database. The EXEC 200X contains the department's information security requirements that ensure users are protecting database information from unauthorized access, use, or disclosure. For that reason, the department has put into place steps that make clear its security requirements of database users. Those requirements include, but are not limited to, the following:

- Accessing information only when necessary to accomplish responsibilities of employment,
- Preventing information from being shared with others,
- Not deliberately performing unauthorized additions, deletions, or alterations of existing records,
- Creating a secure password,
- Reporting suspicious circumstances or unauthorized individuals,
- Taking precautions to prevent documents from unauthorized access or theft, and
- Securing documents that are pending destruction.

Problem being Addressed by this Proposed Regulatory Action

If left unprotected, information could be accessed by unauthorized individuals and could be used to harm individuals that provided information to a school with the understanding that the information they provided would be confidential. Vehicle Code section 1808.21 prohibits dissemination of an address held in a department record. It also restricts the unauthorized dissemination of any department record. By these regulations, the department is prohibiting dissemination of these department records for any purpose other than to fulfill the objective of a functioning database for conveying course completion information to a court. This database is maintained by the department and thus contains department records. Users found to be violating the requirements of Form EXEC 200X will be denied access to the database because complying with the terms of the EXEC 200X is a condition of using the database.

The information required by and contained in the form EXEC 200X are as follows:

The top of the form requires the employee to provide their name and the name of the employer. The information will ensure the department's BPA records reflect that the employee has completed the form EXEC 200X as required in the application process.

The form also contains the following explanatory statement informing the employee of the department's responsibility through federal and state laws to protect personal and confidential information.

The CADMV collects confidential and personal information from the public to administer the various programs for which it has responsibility. The information is maintained according to provisions of various state and federal laws and regulations including the Information Practices Act, the Public Records Act, the California Vehicle Code, the State Administrative Manual and department policies. The CADMV is committed to protect this information from unauthorized access, use, or disclosure. If you are authorized to have access to CADMV information, your responsibilities for the handling and protecting of CADMV information are as follows:

1. You may access information only when necessary to accomplish the responsibilities of employment. You may not access or use information from the CADMV for personal reasons. (Examples of inappropriate access or misuse of CADMV information include, but are not limited to: making personal inquiries or processing personal transactions including your friends and your relatives; accessing information about another person for any reason that is not related to your job responsibilities.)

Provision 1 makes clear that the employee can only access records as necessary to complete their job duties and may not use the information for personal reasons. This provision is necessary as it makes clear that the department's records can only be accessed for authorized transactions. This provision is consistent with 18 US Code § 2721(b)(1), related to permissible uses of records for use by a government agency or a private entity acting on behalf of the state agency in carrying out its functions.

2. You may not disclose or share CADMV information to any person or entity.

Provision 2 prevents an employee from disclosing information to any person or entity. This will ensure that unauthorized persons or entities are not viewing departmental records. This provision is consistent with 18 U.S. Code § 2722 (a), making it unlawful for any person to knowingly obtain or disclose personal information from a motor vehicle record.

3. You may not deliberately perform unauthorized additions, alternations, or deletions to existing data, or enter false or incomplete data on any CADMV document or computer data file.

Provision 3 is included in the form to make clear that the employee cannot make unauthorized updates or deletions to documents or the database.

Updates to documents or database could result in a motor vehicle record being incorrect which could harm the person or vehicle owner.

4. If you are authorized for access to CADMV data, you shall take precautions to create a secure password. A secure password is one that cannot be associated with you or your interests. You may not reveal this password to any person, nor record it on any document. If you have reason to believe another person has determined the nature of your password, you shall immediately change it.

Provision 4 makes the employee aware that they are to create a strong password and provides basic guidance to assist in creating a strong password. A strong password will prevent unauthorized access to records.

5. If you are authorized to access CADMV data using a computer, you shall take reasonable precautions to protect terminals, equipment, and systems from unauthorized access. Reasonable precautions include, but are not limited to: Do not leave the terminal unattended if you are logged on to the system; store user instructions in a secure place; immediately report to your supervisor any suspicious circumstances or unauthorized individuals you have observed in the work area.

Provision 5 requires the employee to store user instructions in a safe place and to not leave a terminal unattended. This provision is necessary to prevent an unauthorized person from accessing a terminal and will prevent the unauthorized person from consulting a user guide that will allow them to access records.

6. If CADMV data is entered on a computer associated with your employer's business, you shall take reasonable precautions to protect the data from unauthorized access. Reasonable precautions include, but are not limited to: Do not leave the computer turned on and unattended; do not copy CADMV data unless authorized by CADMV; report any suspicious circumstances or unauthorized individuals or access you have observed in the work area to your supervisor.

Provision 6 requires the employee to take precautions to protect data from unauthorized access. This provision is necessary as it clearly prohibits an employee from leaving a terminal unattended and from copying data. These steps will prevent the unauthorized access to or viewing of records. The employee is also required to report suspicious circumstances to their supervisor. This will allow the supervisor take immediate steps to verify whether or not a breach has occurred.

7. If you have access to physical documents containing CADMV record information, you shall take reasonable precautions to protect the documents from unauthorized access and theft. Reasonable precautions include, but are not limited to: Move documents that are to be destroyed to a secure area pending destruction; do not remove documents from the firm's premises other than as provided in the Memorandum of Understanding or contract; report to your supervisor any suspicious circumstances or unauthorized individuals or access you have observed in your area.

Provision 7 requires the destruction of records and prevents documents from being removed from the business partner premises. This provision is necessary as it prevents records from being viewed by unauthorized persons. Business partners are already required to destroy documents not in use, this provision will ensure the employee also is aware of their responsibility to destroy records as stated in the partner's contract with the department. Provision 7 also requires an employee to report suspicious activities to their supervisor, who can ascertain whether a breach of records has taken place

8. Federal Law states:

"Any person who knowingly obtains, disclosures, or uses personal information from a motor vehicle record for a purpose not permitted under the Driver's Privacy Protection Act (Title 18 of the United States Code, Section 2721 – 2725), shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court. The court may award:

- actual damages, but not less than liquidated damages in the amount of \$2,500;*
- punitive damages upon proof of willful or reckless disregard of the law;*
- reasonable attorney's fees and other litigation costs reasonably incurred;*
- and*
- such other preliminary and equitable relief as the court determines to be appropriate."*

Provision number 8 is a restatement of 18 US Code § 2724. The restatement of the federal code is necessary to ensure the form accurately identifies the civil damages associated with the unlawful use of the department's records.

I have read and understand the security policies stated above, and have received a copy of them. I understand that failure to comply with these policies may result in civil or criminal prosecution in accordance with applicable laws.

ECONOMIC AND FISCAL IMPACT DETERMINATIONS

- Cost Or Savings To Any State Agency: None.
- Other Non-Discretionary Cost or Savings to Local Agencies: None.
- Costs or Savings in Federal Funding to the State: None.
- Cost Impact on Representative Private Persons or Businesses: The department is not aware of any cost impacts that a representative private person or business would necessarily incur in reasonable compliance with the proposed action. This action requires employees of business partners to complete a form that affirms their intention to maintain the department's records in a safe and responsible manner.
- Effect on Housing Costs: None.
- Local Agency/School District Mandates: The proposed regulatory action will not impose a mandate on local agencies or school districts, or a mandate that requires reimbursement pursuant to Part 7 (commencing with Section 17500) of Division 4 of the Government Code.
- Small Business Impact: This proposed action may impact small businesses. This amendment requires employees of a business partner to complete a form EXEC 200X as part of the business partner's application process. The form instructs the employee on methods to ensure documents and the database are maintained in a safe and responsible manner. There are many business partners that are small businesses, however, this proposed action requires action by the employee and any action that must be taken by the business partner would not be so great that it would be likely to cause any positive or negative impact.
- Potential significant statewide adverse economic impact: The proposed regulatory action will not have a significant statewide adverse economic impact directly affecting businesses, including the ability of California businesses to compete with businesses in other states. The purpose of this amendment is to add an employee privacy form to the documents required during the application process.

ECONOMIC IMPACT ASSESSMENT

(Government Code section 11346.3)

In considering this proposed regulatory action, the department has determined that this action will not result in any of the following:

- 1) The creation or elimination of jobs within the State of California

This proposed action will neither create nor eliminate jobs within California. This action identifies a new privacy protection form that is required as part of the business partner application process. Employees of business partners will be required to complete the form, however, the department does not anticipate this new process will impact jobs in a way that would create or eliminate jobs.

2) The creation of new businesses or elimination of existing businesses within the State of California

This proposed action will neither create new businesses nor will it eliminate existing businesses within California. This action identifies a new privacy protection form that is required as part of the business partner application process. Business partner applicants are required to complete the form to ensure privacy measures are met. The department does not anticipate this new process will impact businesses in a way that would create new businesses or eliminate existing businesses.

3) The expansion of businesses currently doing business within the State of California

This proposed action will not expand businesses currently doing businesses within California. This action identifies a new privacy protection form that is required as part of the business partner application process. Business partner applicants are required to complete the form to ensure privacy measures are met. The department does not anticipate this new process will impact businesses in a way that would cause the expansion of businesses.

This proposed action is unlikely to benefit the state's environment, however, the department anticipates benefits to employee welfare by providing guidance in instruction on how to safely access and maintain records within the department's database and will benefit California citizens who are vehicle owners with records maintained by the department. This proposed action establishes requirements that a business partner applicant must put into place to ensure those records are accessed and maintained in a manner that will ensure their privacy.

DEPARTMENTAL DOCUMENTATION SUPPORTING GOVERNMENT CODE SECTIONS 11346.2(b)(3) THROUGH (b)(5)

- Studies, Reports or Documents - Government Code section 11346.2(b)(3): None.

- Reasonable Alternatives and Department's Response – Government Code section 11346.2(b)(4)(A): No alternatives were presented that would be as effective.
- Reasonable Alternatives That Would Lessen Any Adverse Impact on Small Business – Government Code section 11346.2(b)(4)(B): No alternatives were presented that would lessen any adverse impact on small businesses.
- Evidence Supporting Determination of No Significant Adverse Economic Impact on Business – Government Code section 11346.2(b)(5): The department is not aware of any cost impacts that a representative private person or business would necessarily incur in reasonable compliance with the proposed action. The department is required by statute to adjust specific fees based on the California Consumer Price Index for the prior year, as calculated by the Department of Finance.