CHAPTER 18

ELECTRONIC INSPECTION PROCEDURES

REVISED JUNE 2023

TABLE OF CONTENTS

CHAPTER 18

ELECTRONIC INSPECTION PROCEDURES

1. PURPOSE. The purpose of this chapter is to provide departmental policy for the use of the Iteris inSPECT software and associated commercial enforcement program (CEP) software.

2. SCOPE. This chapter applies to all employees assigned to the CEP and uniformed employees who are not part of the CEP but want to maintain their commercial certifications.

3. BACKGROUND.

a. The Department supports the use of the latest technologies relating to CEP operations to increase the efficiency and quality of service provided to the motor carrier industry.

b. In order to meet this goal, an increasing number of information technology (IT) programs have been deployed by the Department. These programs include departmental, third party, and federal systems. Due to the number of programs in use, it is necessary to establish policy to integrate their effective use.

4. GENERAL PROVISIONS.

a. Federal Policy. The Federal Motor Carrier Safety Administration (FMCSA) has specific requirements and policy regarding federal systems and their use by each jurisdiction.

b. Policy Questions. Users working solely with departmental IT programs shall adhere to departmental policy contained in Highway Patrol Manual (HPM) 40.4, Information Security and Administration Manual. Users working with federal IT programs shall follow both departmental and federal policy. In all instances, departmental policy shall take precedence over federal policy. Questions regarding federal IT program policies shall be directed to Commercial Vehicle Section (CVS).

c. Federal Inspection Reporting Standards. Commercial Vehicle Section shall serve as the liaison between CEP personnel and the FMCSA. This is to ensure the federal reporting standards of accuracy and timeliness are being met.

d. Federal Violation Mapping. Violations recorded during a commercial vehicle inspection must be uploaded to the federal database. In order to integrate California violations into the federal system, a violation mapping table has been established, which links California violations to a federal equivalent violation. Commercial Vehicle Section shall make changes required by legislation, case law, or any other mitigating circumstances.

5. REPORTING STRUCTURE.

a. Description. Two CEP personnel from CVS, two CEP personnel from each Commercial Vehicle Enforcement Facility (CVEF), and two CEP personnel from each Division shall be selected and assigned as the Organization Coordinator (OC) and the Organization Coordinator Alternate (OCA), respectively. The OC and OCA shall assist with CEP IT issues in their assigned Division or CVEF. Field personnel shall report and direct all IT questions directly to the Division/CVEF OC/OCA. The Division/CVEF OC/OCA shall report and direct all IT questions directly to the CVS OC/OCA. The responsibilities of the OC/OCA include the following:

(1) Coordinate, support, and assist with FMCSA account applications, processing, maintenance, and IT training.

(2) Adding, updating, and assigning personnel to the Area's Local Area Network (LAN) system.

b. Selection. The OC/OCA shall be selected and assigned as follows:

(1) Each Division Special Services commander shall designate:

(a) One employee assigned to their Division's on-highway CEP.

(b) One employee assigned to their Division's Motor Carrier Safety Unit.

(2) The commander of each CVEF shall designate one employee as the OC and one employee as the OCA from the CVEF.

NOTE: It is recommended the OC and OCA be of supervisory rank or higher.

(3) Selected employees should be familiar with CEP IT programs and have above-average computer skills. The selected employee's name, ID number, and OC/OCA status shall be forwarded to the OC/OCA assigned to CVS. In the event the employee leaves the command or is otherwise unable to fulfill the assigned OC/OCA responsibilities, a new OC/OCA shall be selected and assigned immediately. The new OC/OCA's information shall be forwarded to CVS without delay.

c. Duties.

(1) In order to access federal IT information and applications, the FMCSA requires all state users to have an active FMCSA Portal account. Commercial Vehicle Section is responsible for oversight of all departmental FMCSA Portal account activity, including, but not limited to, assignment of OC and OCA responsibilities.

(2) All OCs and OCAs shall serve as a point of contact between CVS and personnel in their command for matters related to the FMCSA Portal. Information regarding FMCSA Portal accounts associated with each Division and CVEF is available to each OC and OCA within the FMCSA Portal. All OCs and OCAs shall be responsible for ensuring that information related to FMCSA Portal access and use is distributed to all personnel within their command as necessary.

(3) Once the OC's or OCA's name is submitted to and approved by the FMCSA, they shall be responsible for monitoring and maintaining all federal access accounts within the assigned Division or CVEF, including activation, deactivation, or adjustments of any federal IT account. The responsibilities of all OCs/OCAs include:

(a) Utilizing their FMCSA Portal account to approve new employee accounts, as appropriate.

(b) Approve access to the following systems for field personnel:

1 Analysis and Information Enforcement Users.

2 Motor Carrier Management Information System Generic View.

3 Motor Carrier Specialists shall be granted access to the "Auditor Table."

4 Query Central.

5 Safety and Fitness Electronic Records Web Site Access.

(c) The CVS OC/OCA may grant additional system access to headquarters personnel.

(d) Conduct monthly reviews of the list of active federal accounts within the assigned Division or CVEF for accuracy. This review shall include adjusting and closing accounts, as appropriate.

(e) Terminate all access to federal applications and data immediately upon determining a user no longer requires FMCSA Portal access.

1 Accounts shall be closed for the following reasons:

a Personnel who no longer perform duties requiring access to the federal applications or data shall notify their local OC/OCA immediately.

b Upon receipt of the notification or otherwise becoming aware of any personnel who are no longer eligible for, or require access to, federal data or applications, the OC/OCA shall close the account using the FMCSA Portal account manager and the FMCSA IT Accounts Change Request Form available from CVS.

(4) When requesting FMCSA Portal account access, CEP shall use their departmental e-mail address; select e-mail as the preferred contact method; complete departmental ID number, including "A" preceding the digits of nonuniformed personnel's ID numbers (Motor Carrier Specialist personnel shall enter "CA", followed by the last 4 digits of their departmentally assigned ID number, in order to facilitate use of the federal application known as the Compliance Analysis and Performance Review Information system to document and upload carrier and terminal inspection reports); and the physical street address of their assigned Division or CVEF. The FMCSA Portal Account Request Procedures shall be utilized when creating a new account. These procedures are located in the Commercial Commander's Desk Reference located on the CHP Intranet site at: https://chp2go.sharepoint.com/sites/Starpoint/Resources/SitePages/Commercial-Commander's-Desk-Reference.aspx.

6. THE COMMERCIAL DRIVER LICENSE INFORMATION SYSTEM.

a. Description. The Commercial Driver License Information System (CDLIS) is an FMCSA computer system which enables authorized users to check a commercial driver license, as well as a driver's Drug and Alcohol Clearinghouse status. The CDLIS program is used to make simultaneous inquires to several different state and federal databases. This program is Web-based and accessible online at https://cdlis.dot.gov. Although CDLIS is available through the CHP network, it requires an FMCSA Portal account and separate password to log in.

NOTE: Commercial Driver License Information System data may be accessed directly through the CDLIS Web site.

b. Use. The CDLIS shall be used by all CEP personnel. However, CDLIS may not be used until a supervisor has authorized its use and a federal account has been activated. Supervisors shall ensure their personnel who are certified to perform CEP inspections maintain active CDLIS accounts.

c. Policy.

(1) New User Access. Upon creating an FMCSA Portal account, personnel shall complete the single page "CDLIS Account Request Form" which may be obtained from an OC/OCA. The "CDLIS User Identification" box is left blank by CHP personnel. Additionally, CHP personnel shall use their departmental e-mail address as their username. Access to CDLIS will not be available until the user's account has been activated.

(a) The OC/OCA shall submit all completed CDLIS forms via e-mail to CDLIS-Request@chp.ca.gov.

(b) Commercial Vehicle Section shall submit authorization requests to the FMCSA, as appropriate.

NOTE: The FMCSA may take up to four weeks to process requests received by CVS.

(2) Removal of User. Personnel who no longer require access to CDLIS shall immediately notify the OC/OCA to initiate the closing of the account.

7. COMMERCIAL VEHICLE SAFETY ALLIANCE PORTAL.

a. Description. The Commercial Vehicle Safety Alliance (CVSA) Portal contains operational policies and inspection bulletins pertaining to North American Standard (NAS) vehicle inspections. The CVSA Portal also contains online training material related to inspections, as well as a link to the regulation exemptions granted to interstate motor carriers by the FMCSA.

b. Use. The CVSA Portal shall be used by all CEP personnel. Supervisors shall ensure personnel who are certified to perform CEP inspections maintain active CVSA Portal accounts.

c. Policy.

(1) New User Access. Commercial enforcement personnel shall create a user account on the CVSA Web site located online at https://www.cvsa.org and select the following:

(a) "Member Login."

(b) "Create a User Account" under the "New User" heading.

(c) Complete the requested information using their departmental e-mail and the postal code of their command.

(d) "Continue."

(2) Personnel shall not select "Do Not Email?" and shall opt to be provided industry-related updates.

8. ITERIS inSPECT.

a. Description. Iteris inSPECT is a product of the Iteris Corporation and is Web-based software used to record and transmit commercial vehicle inspections for the Department (e.g., the electronic CHP 407F/343A, Driver/Vehicle Examination Report). Iteris inSPECT allows users to access real-time data from several federal and state programs in a single interface. Iteris inSPECT allows users to access programs which include:

(1) The Inspection Selection System (ISS) is a tool used to screen interstate and intrastate motor carrier vehicles by viewing a carrier's record in summary form. The ISS contains the federal interstate and intrastate carrier database and can auto-populate this information into the electronic inspection report.

(2) The CDLIS is a database which is maintained and operated by the states. This database is designed to serve as a clearinghouse and repository of information regarding the licensing of commercial motor vehicle operators.

NOTE: Access to the California Law Enforcement Telecommunications System is still required to search local or national warrants and criminal records.

(3) The Query Central (QC) system is an FMCSA Portal query system designed to provide driver, vehicle, and motor carrier information to state and federal law enforcement personnel. The QC system combines many different functions and has access to the Canadian and Mexico-based motor carrier databases. The QC system is no longer required for general information or population of Iteris inSPECT. The QC system can be accessed for additional information regarding motor carrier authority for carriers (e.g., Out-of-Service letters).

b. Offline. Iteris inSPECT shall be used to document all inspections. Continual connectivity to the CHP Intranet site is not required. The "offline" mode may be utilized to document inspections until the program is back online. Without an Internet connection, the auto-populate feature will not function.

(1) Iteris inSPECT software is designed to be used with a continual network connection as information is continually updating (e.g., vehicle and driver information, ISS scores, company motor carrier authority, unified carrier registration, insurance information). (Refer to the Iteris inSPECT User's Guide located in the "Links" tab of the program.)

(2) Automatic Synchronization (located in the "Settings" tab) commands Iteris inSPECT to keep a copy of the local database up to date when Internet connectivity is available. This process normally runs in the background which allows Iteris inSPECT to continue to be used while the synchronization is running. (Refer to the Iteris inSPECT User's Guide located in the "Links" tab of the program.)

(3) Nothing precludes personnel from using a handwritten CHP 407F/343A to record initial inspection information. All handwritten CHP 407F/343As shall be recreated and transmitted via Iteris inSPECT at the end of each shift by the CEP personnel who completed the inspection.

NOTE: The paper CHP 407F/343A shall be destroyed, in accordance with policy, after entry into Iteris inSPECT and shall not be forwarded to CVS.

c. Policy.

(1) Commercial Vehicle Section is the administrative authority for all user access for Iteris inSPECT.

(a) Supervisors and managers are authorized to request access to Iteris inSPECT for personnel assigned to the CEP. All approved requests for access shall be routed to CVS via e-mail, to CVSinspections@chp.ca.gov.

(b) Commercial Vehicle Section shall create accounts within Iteris inSPECT.

(c) The Division commercial unit supervisors shall ensure all CEP and non-CEP personnel certifications are maintained, provide technical support, and provide commercial refresher training for Iteris inSPECT access. (Refer to Chapter 16, Commercial Enforcement Program Training, of this manual.)

(d) Personnel who are not granted access to Iteris inSPECT may work with a local Mobile Road Enforcement officer or CVEF personnel with the approval of their respective command. For documentation purposes, the name and ID number of such personnel shall be included in the "Notes" section of the inspection report. Personnel working in this capacity shall securely keep copies of their completed inspections in accordance with HPM 40.4.

(2) Iteris inSPECT software shall not be installed on non-departmentally owned computers or network stations.

(3) The Iteris inSPECT setup and configuration shall not be altered. Initial set-up of Iteris inSPECT shall be done by the appropriate OC, OCA, or LAN coordinator. Requests to alter standard Iteris inSPECT setup configurations shall be directed to CVS.

(4) Updates to Iteris inSPECT will be made available through the Department's Software Center. Personnel with access to Iteris inSPECT will be notified of software updates via Iteris inSPECT Training Window messages and shall update their computer upon receiving an update notification.

(5) Iteris inSPECT can archive inspection reports on a computer's hard drive to be accessed later by utilizing the "List" tab. Currently, state policy (State Administrative Manual, Information Technology – Office of Information Security 5350.1, Encryption) necessitates steps be taken to protect inspection data that includes confidential information. Encryption shall be used to secure all computers that hold driver information.

(6) Iteris inSPECT reports shall be uploaded directly to the federal Safety and Fitness Electronic Records (SAFER) System database at the end of a shift, or as soon as practical, not to exceed 72 hours. The upload shall be done by personnel having authorization to transmit. If any inspections are not transmitted within 72 hours of the date of inspection, notifications shall be made to the immediate supervisor of the involved personnel. Supervisors shall notify CVS.

d. Inspection Procedure.

(1) New User. Each new user shall be assigned a unique username and temporary password to access the program. The user shall change the temporary password immediately.

(a) Upon application startup, the Iteris inSPECT and CDLIS login screens require a username and password. The Iteris inSPECT password should

be changed every 90 days. The CDLIS password shall be changed every 60 days. Failure to change the CDLIS password within 60 days will result in a locked account. To resolve a locked account, personnel must contact the FMCSA Gateway Helpdesk, at fmcsasupport@techanax.com, or at (855) 537-7517.

NOTE: Iteris inSPECT and CDLIS will not prompt the user to change the password. The CDLIS password is separate from the Iteris inSPECT login password. Therefore, two separate password changes are required.

(b) The Iteris inSPECT login window has a "Forgot Iteris Password" option for users to reset their Iteris inSPECT password. Users shall supply their CHP e-mail address to activate this feature.

9. CARRIER DATA QUALITY DISPUTES.

a. Description. The FMCSA Compliance Safety Accountability system assigns motor carriers and individual drivers a safety score based on data provided by federal and state inspections. The Department provides data to the FMCSA from inspections completed and transmitted within Iteris inSPECT. Data is also transmitted from the Statewide Integrated Traffic Records System where the data collection is generated from the CHP 555D, Truck/Bus Crash Supplemental Report.

b. Policy. Carriers or drivers wanting to dispute data provided by the Department to the FMCSA shall submit the challenge via the FMCSA DataQs Web site, at https://dataqs.fmcsa.dot.gov/. Commercial Vehicle Section is the contact for data uploaded to the FMCSA.

(1) The carrier or driver shall complete the online form and submit supporting documents electronically. Electronic acknowledgement of the challenge shall be sent to the carrier or driver within ten business days upon becoming aware of the challenge.

NOTE: Challenges shall only be accepted electronically through the FMCSA portal. Telephone or handwritten challenges shall not be accepted. Challenges without supporting documentation shall be denied. Commercial Vehicle Section may, on occasion, request additional information from the data challenger. If documentation is not received within 30 days, the challenge shall be closed and denied.

(2) Disputes pertaining to enforcement actions, crash report coding and documentation, or any violation documented on an electronic CHP 407F/343A shall be reviewed by CVS for final disposition.

(3) The CVS, Credentialing Unit, should review all data challenges. Based on the FMCSA and state reporting criteria, gathered information, and impartial, professional judgement, the reviewing officer shall either deny or grant the challenge. If the challenge is granted, the appropriate information shall be removed, amended, or adjusted through the FMCSA Portal. This will remove or modify the carrier and/or driver safety score. If the challenge is denied, the case shall be reviewed by the reviewing officer's supervisor. If the supervisor concurs with the reviewing officer, the denied challenge is final. The challenger shall be notified electronically through the FMCSA Portal of the denial.

(4) In the event that a carrier or driver is denied a challenge, they are allowed one appeal. They can submit another written request and submit the review, with all supporting documentation, electronically through the FMCSA Portal. All second and final appeals are reviewed by the CVS supervisor who shall make the final determination.

NOTE: The FMCSA does not have the authority to change state-supplied data. Therefore, once CVS has denied or allowed a change, there are no further appeals.

10. CALIFORNIA HIGHWAY PATROL INTRANET SITE COMMERCIAL ENFORCEMENT INFORMATION.

a. Information Queries. All departmental personnel may access the Commercial Enforcement Information Query database located on the CHP Intranet site (also located in the "Links" tab of Iteris inSPECT).

b. Carrier Information Reporting and Evaluation System. The Carrier Information Reporting and Evaluation System is a resource for providing information on carriers. The information available includes basic information on the carrier, terminal inspection summaries, emergency contacts, terminal locations, the employer ID number, and Motor Carrier Permit Status. The information can be obtained through http://cires.eprise.ad.chp.ca.gov/CIRES.

11. PERSONNEL ASSIGNED TO THE COMMERCIAL ENFORCEMENT PROGRAM.

a. Required Access. All departmental personnel assigned to the CEP and non-CEP personnel certified to conduct NAS inspections shall obtain and maintain access to the following applications:

(1) The FMCSA Portal.

(2) The CDLIS.

(3) The CVSA Portal.

(4) Iteris inSPECT.

12. SUPPORT.

a. Hardware and software issues shall be directed as follows:

(1) Departmental Hardware. Contact the Division LAN coordinator.

(2) Federal Software Problems, Passwords, or Login Difficulties. Contact the FMCSA Portal Help Desk at (617) 494-3003, or the CDLIS Help Desk at (855) 537-7517.

(3) Iteris inSPECT. Contact CVS at (916) 843-3400, or at CVSinspections@chp.ca.gov.

(4) Use of Query Central and Training. Contact the local trainer or CEP OC/OCA.

(5) Commercial Driver License Information System. Contact CVS at (916) 843-3400, or at CDLIS-Requests@chp.ca.gov.

THIS PAGE INTENTIONALLY LEFT BLANK