provides for a waiver of the Buy America requirements when the application would be inconsistent with the public interest or when satisfactory quality domestic steel and iron products are not sufficiently available. This notice provides information regarding the FHWA's finding that a Buy America waiver is appropriate to use non-domestic high strength steel bars based on the public interest provision in FHWA's policy.

On October 27, 2009, a repair made during the 2009 Labor Day weekend to a cracked eye bar on the San Francisco Oakland Bay Bridge failed, requiring the closure of the bridge. The San Francisco Oakland Bay Bridge carries over 280,000 vehicles per day creating transportation gridlock in the area. Caltrans' goals were to ensure the safety of the bridge and reopen it as soon as possible through an emergency repair contract. Caltrans contacted four steel fabricators regarding their ability to supply domestic high strength bars to meet the schedule for the emergency repairs. They were unable to find a fabricator who had domestic high strength steel on hand that was able to meet their schedule.

In accordance with Division K, section 130 of the "Consolidated Appropriations Act, 2008" (Pub. L. 110–161), the FHWA published a notice of intent to issue a waiver on its Web site for the high strength steel bars (*http://www.fhwa.dot.gov/construction/contracts/waivers.cfm?id=46*) on March 22, 2010. The FHWA received four comments in response to the notice. One commenter suggested that Gerdau Ameristeel manufactures the high strength steel bars domestically. Caltrans contacted Gerdau Ameristeel to verify availability of high strength steel bars during the period of emergency repairs. Gerdau Ameristeel indicated that a lead time is required and the high strength steel bars would not have been available for emergency repairs. Two comments were from Caltrans explaining the circumstances surrounding the project, as well as the efforts made by Caltrans in contacting potential domestic manufacturers. The fourth comment expressed general support for the Buy America requirement.

During the 15-day comment period, the FHWA conducted additional nationwide review to locate potential domestic manufacturers for the high strength steel bars. Based on all the information available to the agency, the FHWA concludes that there were no domestic high strength steel bars ASTM A 722M 150ksi (1⅞ inches diameter) readily available for emergency repairs of the broken eye bars.

In accordance with the provisions of section 117 of the SAFETEA–LU Technical Corrections Act of 2008 (Pub. L. 110–244, 122 Stat.1572), the FHWA is providing this notice as its finding that a waiver of Buy America requirements is appropriate. The FHWA invites public comment on this finding for an additional 15 days following the effective date of the finding. Comments may be submitted to the FHWA's Web site via the link provided to the California waiver page noted above.

(Authority: 23 U.S.C. 313; Pub. L. 110–161, 23 CFR 635.410)

Issued on: June 24, 2010.

Victor M. Mendez,

Administrator.

[FR Doc. 2010–16085 Filed 7–1–10; 8:45 am]

BILLING CODE 4910–22–P

DEPARTMENT OF TRANSPORTATION

Federal Motor Carrier Safety Administration

Guidance to States Regarding Driver History Record Information Security, Continuity of Operation Planning, and Disaster Recovery Planning

AGENCY: Federal Motor Carrier Safety Administration, DOT.

ACTION: Notice.

SUMMARY: The Federal Motor Carrier Safety Administration (FMCSA) announces guidance to State driver licensing agencies (SDLAs) to support their efforts at maintaining the security of information contained in the driver history record of commercial driver's license (CDL) holders. Further, FMCSA provides States with recommendations related to continuity of operation and disaster recovery planning to ensure the permanence of information contained in the driver history record of a CDL holder. This action is in response to the Department of Transportation Office of the Inspector General's (OIG) 2009 report *Audit of the Data Integrity of the Commercial Driver's License Information System (CDLIS).*

FOR FURTHER INFORMATION CONTACT: Selden Fritschner, Chief, Commercial Driver's License Division, E-mail: *selden.fritschner@dot.gov,* Telephone: 202–366–0677, or Kelvin Taylor, Information Systems Security Officer, E-mail: *kelvin.taylor@dot.gov,* Telephone: 202–366–4028. Federal Motor Carrier Safety Administration, 1200 New Jersey Ave., SE., Washington, DC 20590.

SUPPLEMENTARY INFORMATION:

I. Background

In July 2009, the Department of Transportation's Office of Inspector General released the report *Audit of the Data Integrity of the Commercial Driver's License Information System* as required by the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA–LU) (Pub. L. 109–59). CDLIS consists of a database, known as the Central Site, which maintains individual Master Pointer Records (MPR) with identifying information for each CDL holder in the United States. This database directs or points inquirers to the database of each of the 51 CDL-issuing jurisdictions for more complete driver history records. Connectivity for the system is provided through an encrypted communications network. The FMCSA has designated the American Association of Motor Vehicle Administrators (AAMVA) as the operator of the Central Site and the communications network. States are responsible for ensuring their systems comply with the CDLIS specifications and procedures as published by AAMVA.

In preparing its report, OIG evaluated several factors related to the information stored at the CDLIS Central Site and on State databases. Specifically, OIG attempted to determine "whether CDLIS and State department of motor vehicles (DMV) information systems were adequately secured," and "the adequacy of contingency plans to ensure continued CDLIS service to DMVs following a disaster or emergency." (**Note:** The OIG report refers to DMVs. However, as States continue to reorganize their organizations away from all-inclusive DMVs, FMCSA has used the term "State Driver Licensing Agencies" in previous rulemakings to refer to these same agencies responsible for issuing CDLs).

The identifying information on the MPR at the CDLIS Central Site includes the name, date of birth, social security number, State of Record, and driver's license number. Because this information, both as individual and cumulative data elements, is considered personally identifiable information (PII), possessors of the information must take specific steps to prevent unauthorized access and dissemination. At the same time, because the information contained at the CDLIS Central Site and on SDLA databases is crucial to highway safety during the CDL issuance process and at roadside enforcement/inspection, it is paramount that the data be available to all authorized users with minimal disruption.

In its report, OIG noted that FMCSA had neither developed and implemented sufficient comprehensive security policies and procedures to protect the portal it uses to access CDLIS, nor had it developed complete contingency and testing plans for this system to ensure uninterrupted CDL information services in the event of a disaster or system outage. The FMCSA is currently addressing these findings by working directly with its service providers and is reporting its progress to OIG through corrective action plan updates. As the operator of CDLIS, AAMVA is also modernizing the system to adhere to standards established by the Federal Information Security Management Act (FISMA). Similar FISMA standards are being applied to the portal FMCSA owns and uses to access CDLIS.

The OIG also noted similar deficiencies in some State systems and programs. In five of nine States reviewed, the OIG found that information security practices, including continuity of operation and disaster recovery policies and plans, were either non-existent or informal, and that State continuity of operations, disaster recovery, and information system contingency planners had never engaged in adequate testing exercises.

Guidance

As a result of OIG's findings, FMCSA encourages States to evaluate their information security programs and either establish or update policies, plans, and procedures, to provide an adequate level of protection to sustain their operational mission and responsibilities.

While States are not required to meet Federal information security standards, each State should ensure that it has adequate and comprehensive processes and procedures in place to protect PII and sensitive information and to sustain its key operations during an outage. The National Institute of Standards and Technology's (NIST) Computer Security Division maintains a Computer Security Resource Center (CSRC) that provides free information to government and non-governmental entities in an effort to protect information systems against threats and ensure availability of information and services. FMCSA recommends that States consider NIST standards and review the publications available at its Web site: *http://csrc.nist.gov/index.html.*

I. Information Security

The key deficiency in States that OIG noted was the lack of current information security plans. Adequate planning is necessary to document standards and provide for continuous review and improvement. FMCSA strongly encourages States to develop an Information Security Strategic Plan (ISSP) that addresses organizational structure and governance, roles and responsibilities, and enterprise architecture. From this ISSP, the State should develop specific policies and guidance to ensure information security. Further, a coordinated plan allows for systematic monitoring and improvement.

While obviously not intended to be comprehensive for large organizations such as State driver licensing agencies, NIST Interagency Report (IR) 7621, *Small Business Information Security: The Fundamentals* provides basic information about information security issues. Topics in this publication include: Protecting information systems from damage by viruses, spyware, and malicious code; protecting internet connections; using firewalls; updating operating systems and applications; securing wireless access points and networks; controlling physical access to network components; training employees about information security; and limiting employee authority to install software, access certain websites, and gain access to network controls. Though States are not required to comply with FISMA, NIST Special Publication (SP) 800–53, *Recommended Security Controls for Federal Information Systems and Organizations (Rev. 3, August 2009),* provides a comprehensive guide to information security standards. NIST SP 800–100, *Information Security Handbook: A Guide for Managers,* also provides overview information for developing a security plan. NIST currently makes available over 30 additional publications related specifically to information security on topics ranging from wireless network access authentication to enterprise password management.

II. System and Service Unavailability

To mitigate the risks associated with system and service unavailability, FMCSA encourages States to establish and implement:

Continuity of Operations Plan (COOP)—A plan that focuses on restoring an organization's essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations.

Disaster Recovery Plan (DRP)—An information technology plan designed to restore operability of a system, application, or computer facility after an emergency.

Information Technology Contingency Plan (ITCP)—A plan focused on ensuring continuity-of-support for major applications in the event of a disruption in normal operations due to an emergency.

These plans should include a business impact analysis (BIA) to determine: the interdependence of systems and work priorities in the event of a disruption; actions necessary to restore system operations on a short term basis after a disruption until a more permanent solution can be implemented; and actions necessary to reconstitute a disrupted facility or lost data to its previous level of capability. The BIA should also include an analysis of the organization's reliance upon contracted support and connectivity, a prioritization list of the systems necessary for the organization's mission-critical functions, maximum allowable outages for system components (measured in hours or days), and responsibilities associated with restoring critical functions (including a line of succession in cases of staff unavailability). For further information on contingency planning, consult NIST's Special Publication 800–34: *Contingency Planning Guide for Information Technology Systems.*

In addition to establishing plans for service disruption and disaster recovery, it is critical to perform tests that assure the plans will work. These tests should be designed as cost-effective ways of determining if contingency systems and personnel perform as expected. The tests also provide the organization and its personnel with the confidence and experience necessary to respond to a real event. Tests can range from classroom exercises to full system testing that simulates a real event. Tests should be documented and the results examined for lessons learned and improvements necessary to the contingency plans. For further information on contingency testing, consult NIST's Special Publication 800–84: *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities.*

Issued on: June 23, 2010.

Anne S. Ferro,

Administrator.

[FR Doc. 2010–16226 Filed 7–1–10; 8:45 am]

BILLING CODE 4910–EX–P