THE ROAD TO ELD CERTIFICATION

Recommendations of ATA's Working Group on ELD Fraud

SAFETY POLICY COMMITTEE

NOVEMBER 2026



Background & Mission

Adherence to and enforcement of commercial drivers' hours of service regulations is critical to the safety of commercial drivers and vehicles on America's roadways. Since 2014, electronic logging devices (ELDs) have served as a source of ground-truth data for drivers' hours of service. However, law enforcement has recently seen an alarming uptick in cases of ELD tampering or fraud. New forms of ELD and hours of service fraud involve new tactics and coordination between ELD providers and fleets to illicitly edit a driver's records in ways that are difficult to detect at roadside. This fraud represents an immediate and serious safety risk on America's roadways.

Based on the Commercial Vehicle Safety Alliance's (CVSA)' review of data on ELD tampering violations, fleets that received these types of violations are associated with a 56% higher reportable crash rate and significantly higher rates of driver and vehicle out of service violations. In response to this new type of fraud and the safety issues it presents ATA's Safety Policy Committee voted in October 2025 to update the association's policies on ELDs to support stronger measures of ensuring ELD integrity, including third-party certification of devices. Subsequently, ATA's Safety Policy Committee created a working group to identify the specific government and industry policies which would address these new types of fraud and a pathway to making those policies a reality. This document represents the results of the working group's efforts and recommendations to identify a comprehensive set of policies and actions that will restore trust in the ELD ecosystem in the short term and maintain trust in the ELD system and federal databases of ELD providers over the long term.

Further, ATA applauds the ongoing work of the U.S. Department of Transportation and the Federal Motor Carrier Safety Administration (FMCSA) to target ELD fraud and manipulation. Over the past year, FMCSA has taken steps to reduce ELD fraud and bolster the integrity of hours-of-service compliance. In addition to strengthening the front-end vetting of an ELD's technical specifications before it can be listed in FMCSA's registry, FMCSA actively monitors devices on the market and removes ELDs that fail to meet federal standards. Since 2025, the agency has revoked dozens of noncompliant ELDs and required carriers to transition to compliant systems, with drivers subject to out-of-service orders if they continue using revoked devices after the compliance period. FMCSA has also conducted investigations into alleged device manipulation and removed devices in response. ATA hails the agency's ongoing efforts aimed at preventing falsified logs, unauthorized edits, and other practices that can allow drivers or carriers to evade hours-of-service limits. This report offers recommendations for the agency to continue building upon their ongoing work and calls on Congress to provide the agency with sufficient resources to pave a path towards a third-party certification process

Guiding Principles

ATA's working group members identified five guiding principles as critical to ensure that any recommendations are practical, efficient, effective, and meet the needs of all stakeholders to restore legitimacy and trust in the ELD ecosystem. These guiding principles shaped the recommendations of the working group and should provide continued guidance for future discussions about maintaining the integrity of hours-of-service rules and enforcement.

- **The Federal Motor Carrier Safety Administration (FMCSA) should take a short-term approach that does not require rulemaking to address current known methods of fraud in the existing system**, followed by a long-term approach that utilizes the existing advance notice of proposed rulemaking[1] (ANPRM) to improve protections against future fraud.

- **There is no silver bullet to prevent all fraud.** FMCSA should aim to raise the bar in several areas to make fraud more costly to attempt, more likely to be detected, and more quickly investigated and shut down.

- **FMCSA should utilize third parties for certification processes** and focus its resources on investigation, enforcement, and maintaining technical standards.

- **Stakeholders cannot predict all the ways fraud will be attempted in the future.** The end goal is to create a system in which:
  - Attempts at fraud are minimized at the point of entry into the system,
  - Fraud that does occur can be detected quickly and reliably, and
  - FMCSA and states have the resources to quickly and effectively respond.

- **To reach this goal, FMCSA's long-term actions should create more touch points for devices and suppliers.** No single touch point would catch all fraud, but, cumulatively, their breadth and frequency would increase the overall chances of detection and reduce the window in which they could operate before being detected.



1. https://www.federalregister.gov/documents/2022/09/16/2022-20095/electronic-logging-device-revisions

SPECIFIC RECOMMENDATIONS:

Short-term Actions

ATA's working group believes that these steps can be taken quickly and without rulemaking processes to address devices, providers, and fleets that are currently engaged in fraud. These measures should be taken concurrently with long-term actions discussed later in the document. These measures are meant to restore confidence in the existing registration system while the certification process is being developed and deployed. We recognize and appreciate that FMCSA has already taken several shorter term actions to begin tackling ELD fraud without initiating a formal rulemaking process, and these recommendations aim to complement and build upon those efforts.



RECOMMENDATION 1

Implement checks on ERODS for common indicators of fraud

FMCSA can run algorithmic checks on records of duty status (RODS) for common indicators of fraud. This would allow FMCSA to have better visibility into currently registered devices and maintain visibility in the interim until a third-party certification program is set up. The process could be run on batches or samples of RODS or could even be implemented in real time as records are received. To do so, we recommend that:

- **FMCSA check RODS that it receives for common indicators of today's fraud** like out-of-sequence file numbers, impossible distances, and driver info manipulation.
- **FMCSA follow up on RODS flagged for indicators of fraud with a human review.**
- **Law enforcement only uses what is available to them at roadside to prove violations under current procedures.** Automated checks on RODS for common indicators of fraud should not be implemented at roadside.

State law enforcement currently conducts approximately 250,000 driver inspections per month. Based on this inspection rate, all currently registered devices could have a meaningful sample of ERODS checked using these methods.

RECOMMENDATION 2

Require all companies registering devices to have a verified footprint in the U.S.

FMCSA must be able to hold entities accountable in the event of non-compliance or fraud. By requiring all companies registering devices to have a verified U.S.-based footprint, FMCSA and/or law enforcement will have the necessary tools when they investigate. The working group believes this could be implemented like the National Highway Traffic Safety Administration's existing processes, such as Part 551 designated agents or Part 591 import declarations. This requirement could be incorporated into certification requirements.

RECOMMENDATION 3

Maintain FMCSA responsiveness in investigating potential fraud

To effectively implement these recommendations, FMCSA may need to dedicate additional resources and build out new processes for key stakeholders such as enforcement and ELD vendors to work with the agency. While FMCSA has aggressively jumped into action and pursued short-term approaches to shutting down ELD fraud, we recognize that some of FMCSA's existing processes were not designed to manage the scale of registered devices or the level of engagement necessary for vetting vendors or coordinating investigations with enforcement. To do so, the working group believes:

- **FMCSA needs to be responsive to reports of ELD fraud, particularly those from law enforcement.** This is the last line of defense both in short- and long-term plans to address fraud.
- **Given the recommendations above, FMCSA may need to develop new processes for receiving, reviewing, and investigating flags of potential fraud**, especially those from law enforcement.
- **FMCSA should work on implementing automated checks of ERODS to flag records for additional investigation.** Until FMCSA is prepared to implement real-time checks upon receipt of ERODS, periodic checks of batches or samples of records would provide useful and timely information.
- **The ELDTech email address is not sufficient as an enforcement / investigation tool.** FMCSA should create a formal process for law enforcement reporting which tracks reports from creation to resolution. FMCSA can maintain the email system for industry and public use.
- **The ELDTech email address is also not sufficient for certification-like activities by FMCSA.** Like enforcement reports above, industry needs a formal process for registering and certifying devices. In the short term, FMCSA's vetting processes using ELDTech should provide tracking and visibility into that process for ELD vendors. FMCSA should not conduct certification-like activities on its own through ELDTech without the transparency and formal rulemaking processes described below.

Recognizing the limited agency resources of the FMCSA that may limit its ability to effectively carry out these recommendations, ATA further calls upon Congress to dedicate additional staff and financial resources to FMCSA to accomplish its safety and enforcement goals – including those related to tackling ELD fraud.

SPECIFIC RECOMMENDATIONS:

Long-term Actions

ATA members believe it is necessary to create a certification program to better prevent future attempts at fraud and provide FMCSA with better tools for investigating fraud. The recommendations below build on the 2022 ANPRM to gather necessary feedback from industry, set up funding mechanisms to stand up the certification ecosystem, and ensure that ELD providers can attain certifications within the necessary timeframe.



RECOMMENDATION 4

Build a Certification Program

Certification represents a necessary step for addressing future potential for ELD fraud. A certification structure creates strong disincentives and barriers to fraud by introducing hurdles to entering the market with the intent of fraud, frequent touch points which increase the likelihood of fraud being detected, and better visibility into the ecosystem for investigating fraud. While ATA recognizes that a certification system can't prevent all fraud, it presents significant risks and barriers-to-entry and broad protections against currently understood methods of fraud and unknown future methods of fraud.

SCOPE

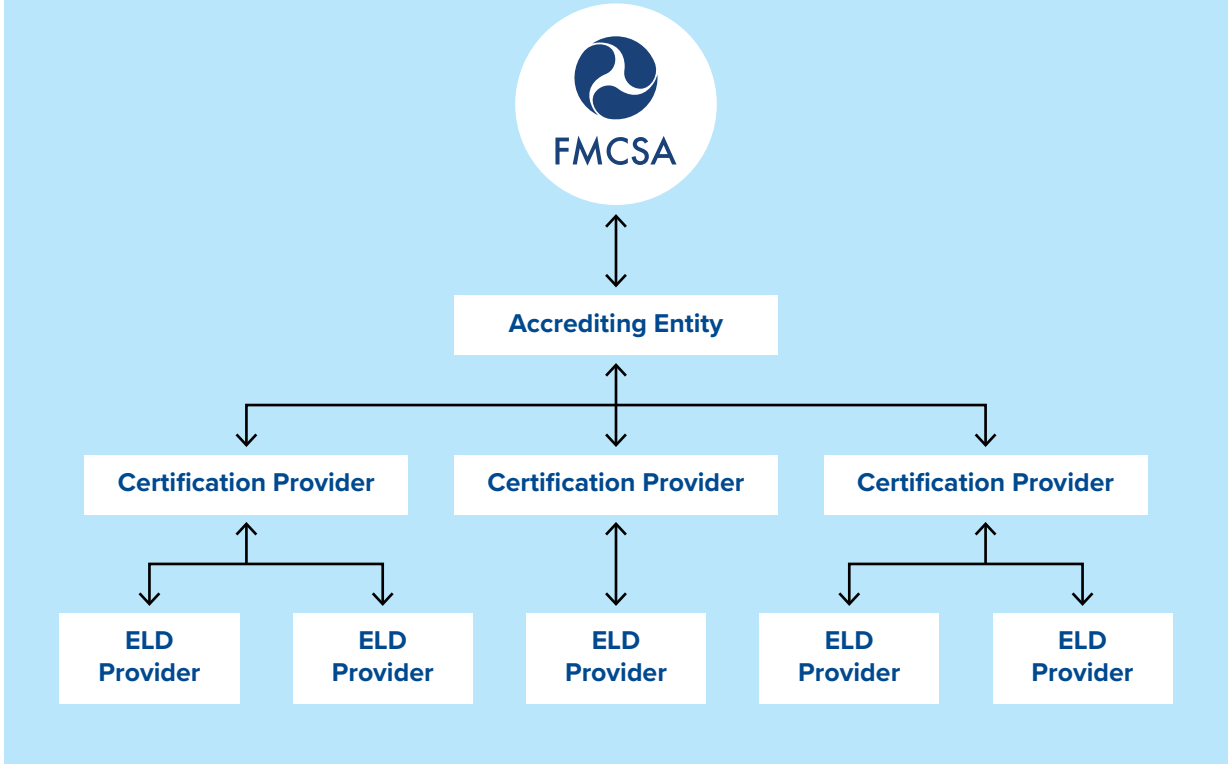
ATA's working group began developing its recommendations around a long-term certification program by establishing the program's ideal scope and structure. In doing so, the working group sought to design an approach that focuses resources on the most significant sources of fraud, creates meaningful incentives for organizations with the necessary technical expertise to participate in the certification process, remains cost-effective for both industry and government, and is structured to remain

viable. The working group also recognized that no certification framework can reasonably be expected to eliminate every potential avenue for fraud. Rather, the objective should be to establish a strong and credible barrier to fraudulent or noncompliant devices entering and remaining in the marketplace and on FMCSA's certified list.

Consistent with that objective, the working group recommends that FMCSA focus the certification program primarily on the software components of ELDs, where the most significant opportunities for manipulation and fraud exist, while establishing appropriate minimum requirements for the hardware on which that software operates. This approach would allow the certification process to concentrate on technical review and testing where it can have the greatest impact without unnecessarily increasing the complexity or cost of certification. In other words, the goal would not be to design a system capable of preventing every imaginable form of fraud or misuse, but rather one that makes fraud substantially more difficult to conduct and easier for FMCSA to identify and address.

The working group also recommends that FMCSA build upon existing certification mechanisms rather than create an entirely new model from the ground up. In particular, the Canadian ELD certification framework provides a useful structural model for how independent technical expertise can be incorporated into an effective certification regime. However, ATA believes FMCSA should establish and maintain its own certification program, tailored to the U.S. regulatory environment and administered separately from the Canadian system. Whenever possible, FMCSA should seek to maintain alignment between the two programs, particularly with respect to technical requirements and testing approaches. Doing so would reduce unnecessary friction for ELD providers operating in both markets

Structure of ATA's working group's proposed third-party certification system



while still preserving FMCSA's authority and flexibility to establish requirements appropriate for the United States.

Under this model, FMCSA would retain responsibility for establishing and maintaining the underlying technical requirements for ELDs, as well as investigating potential violations and taking appropriate enforcement action. The agency should, however, contract with qualified non-governmental entities to perform the technical functions necessary to operate and maintain the certification program. Leveraging outside technical expertise would allow FMCSA to focus its resources on the regulatory and enforcement functions for which it is uniquely responsible while helping ensure that the certification process has access to the specialized expertise necessary to evaluate increasingly sophisticated ELD software.

Taken together, these recommendations are intended to create a certification framework that is rigorous without being unnecessarily burdensome, sustainable over the long term, and capable of adapting as ELD technology and methods of circumvention evolve. By focusing certification on the areas of greatest risk, leveraging qualified third-party technical expertise, and maintaining appropriate alignment with Canada, FMCSA can establish a durable certification program that raises the barrier to fraud while remaining workable for regulators, providers, motor carriers, and other stakeholders.

STRUCTURE

ATA's working group also considered how a third-party certification system could be established and administered in a manner that is both technically credible and sustainable over the long term. ATA's working group recommends that FMCSA fund the development of an accreditation program to support a third-party ELD certification framework. Under this approach, FMCSA would retain responsibility for establishing and maintaining the technical requirements, resolving questions of regulatory interpretation, and conducting investigation and enforcement activities, while qualified third-party organization(s) would administer accreditation and certification. This structure would allow FMCSA to focus its personnel and resources on its core regulatory and

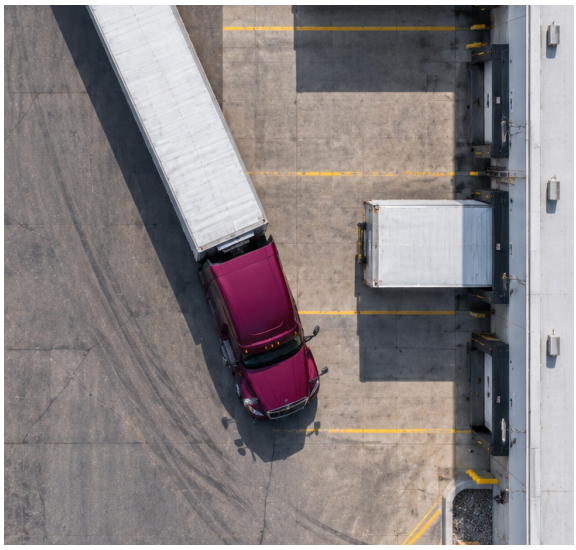


enforcement responsibilities while leveraging outside technical expertise.

FMCSA could utilize a research contract to begin developing the accreditation and certification framework concurrently with the regulatory process, including through organizations with relevant technical and standards expertise such as the Institute of Electrical and Electronics Engineers (IEEE), American National Standards Institute (ANSI), SAE International, or universities. The resulting framework should establish requirements for certification providers; processes and timelines for accreditation, certification, and re-accreditation; data-sharing requirements; procedures for incorporating regulatory changes; and a clear mechanism for quickly elevating questions of interpretation to FMCSA and communicating the agency's determinations consistently across the certification ecosystem.

To facilitate a timely launch, FMCSA should provide one-time seed funding to cover the initial fixed costs for the designated accreditor and certification providers to establish the necessary capabilities. Once established, certification providers would pay for accreditation, while ELD providers would pay accredited certifiers for certification services. FMCSA should continue to support the accreditor's fixed costs, with variable costs funded through accreditation fees. In return, the accreditor should provide FMCSA with periodic data and analysis on the certification ecosystem. This approach would provide the initial federal support necessary to establish a credible certification system while creating a sustainable, largely fee-supported model for its long-term operation.

Funding the creation and fixed operating costs of an accreditation program would allow FMCSA to focus its personnel on regulatory and investigation/enforcement actions.



TIMING

ATA's working group recommends that FMCSA use the existing 2022 ANPRM as the foundation for continuing the regulatory process, capitalize on existing momentum to establish an ELD certification model, and issue an NPRM as quickly as practicable. Rather than proposing a firm compliance date at the outset, the NPRM should solicit stakeholder feedback on the time necessary to establish the accreditation and certification infrastructure and certify existing devices. FMCSA should also use the NPRM to gauge interest among prospective accreditation and certification providers and better understand their capacity and requirements for participating in the program.

Concurrently with the rulemaking process, FMCSA should fund research to develop the accreditation framework and assess the anticipated pool of accreditation providers, certification providers, and devices requiring certification. Using the information developed through both the NPRM and this research, FMCSA can establish an appropriate compliance timeline in the final rule that provides sufficient time to stand up the accreditation and certification system and certify existing ELDs before the new requirements take effect.

RECOMMENDATION 5

Sustain compliance and plan to continue updating certification processes

Certification is not a one-time event. It must be maintained throughout the lifecycle of devices. This lifecycle recertification approach facilitates continued compliance and ensures FMCSA maintains visibility as devices and technologies evolve. The working group's key recommendations for FMCSA on operating a certification program that appropriately builds in compliance checks throughout the device's life cycle are as follows:

- Require certified devices to be reviewed regularly to maintain their certification. This could include an approach like the Canadian model of certification providers reviewing 25% of the requirements each year.
- Give accreditors the ability to audit certification providers and/or devices and perform such audits of all certification providers periodically.
- Make room for software updates unrelated to the ELD technical requirements without requiring re-certification of devices. However, such software updates should still require a touch point with any certification providers, accreditors, and/or FMCSA.
- Require companies to reaffirm information they submit to register/certify a device periodically, such as each time a certifier reviews their device for sustained compliance, including their verified U.S.-based footprint.
- Add ELD information to the MCS-150 form. This could help FMCSA investigate other users of a device they are investigating or other devices used by a fleet they are investigating.

RECOMMENDATION 6

Review technical requirements

As technologies evolve, FMCSA should plan to update the technical requirements as needed. FMCSA should plan how updates will impact the certification process to ensure smooth transitions when new requirements take effect.

FMCSA should consider how the technical requirements can be revised to both reduce ambiguity in interpretation and facilitate future certification processes. Adding flexibility for things like geofencing can reduce the need for legitimate changes to RODS, making it easier to flag fraudulent changes. FMCSA should consider how the technical requirements can provide data points for future certification processes, internal checks of ERODS, or roadside enforcement to detect fraud. FMCSA should also ensure that the technical requirements support secure devices for fleets operating in compliance. If/when there are changes to the technical requirements, ELD providers should self-certify that existing devices comply *with those specific changes* until their next periodic sustained compliance review.



Future considerations for sustained compliance

Sustained compliance and periodic renewals for all entities in the process (accreditor, certifier, devices) are critically important. They ensure all parties follow their contractual/regulatory requirements and that FMCSA maintains good visibility into the system for their investigation/enforcement activities. As part of their contractual fixed-cost funding, the accreditor should provide regular data to FMCSA on the system. As part of maintaining their accreditation, certifiers should periodically be audited and provide regular data to the accreditor and/or FMCSA. As part of maintaining their certification, devices should be partially reviewed each year and randomly audited to ensure they are maintaining compliance. All three entities will need to have periodic renewals in the system, and the timing of these three types of renewals needs to be carefully considered so that they do not cause gaps or friction in the future. FMCSA should use the NPRM to gather feedback on these timings and identify any gaps or sources of friction, as well as methods to mitigate them going forward.

Conclusion

ELD fraud presents an immediate safety risk to our industry and those on the nation's roadways, and a long-term threat to confidence in the hours-of-service compliance framework. We commend FMCSA's efforts to implement a more thorough vetting process at the front door to ELD self-certification while also weeding bad actors out of the current registry. To amplify these efforts and more effectively address ELD fraud and noncompliance over the long term, the existing vetting and self-certification model must involve a more robust response system and ultimately a third-party certification process.

ATA's working group recommendations are intended to address both dimensions of that challenge:

1. **By giving FMCSA and enforcement partners practical tools** to identify and respond to current fraud without delay.

2. **By establishing a durable certification framework** that raises the barrier to future manipulation while remaining workable for regulators, providers, motor carriers, and other stakeholders.

Together, these measures would restore trust in the ELD ecosystem by making fraud more difficult to commit, easier to detect, and faster to investigate and resolve. ATA encourages FMCSA to act quickly on the short-term recommendations while advancing the rulemaking, research, and stakeholder engagement necessary to build an effective third-party certification program. A coordinated approach between government, enforcement, industry, and technical experts will be essential to maintaining the integrity of ELDs, supporting compliant carriers, and protecting safety on the nation's roadways.



AMERICAN
TRUCKING
ASSOCIATIONS