ERDC/CERL TN-21-2
September 2021

US Army Corps of Engineers®

Autonomous Transport Innovation: The Regulatory Environment of Autonomous Vehicles

by Emma L. Smith, Julie L. Webster, and Annette L. Stumpf

PURPOSE: This technical note series under the Autonomous Transport Innovation research program is intended to be a primer on autonomous vehicles (AVs), their testing, and associated infrastructure. A review of the regulatory environment for autonomous vehicles is necessary to define rules imposed on technology or operations of autonomous vehicles in various capacities. Acknowledging such regulation will aid in productive closed-course site development by structuring the course based on what autonomous vehicle developers and manufacturers must program their vehicles to adhere to in a given setting.

INTRODUCTION: The National Highway Traffic Safety Administration (NHTSA) estimates that nearly 94% of automobile accidents are attributed to human error (NHTSA, n.d.). According to former NHTSA administrator Mark Rosekind in an interview conducted by The Eno Center for Transportation (2018), for many years, the approach to automotive safety had been *reactive.* Rosekind further explains that autonomous technology is allowing for the transition to a *proactive* approach by aiming to eliminate the human error component.

The development of advanced AV technologies is noticeably agitating the automobile regulatory environment. Regulators need to achieve a careful balance to avoid hindering innovation but still provide a foundation of certainty in which to promote safety and marketability. The following will provide a comprehensive outlook of current regulation in a top-down fashion including overarching federal guidance, state-level legislation, local action, and military context.

SOCIETY OF AUTOMOTIVE ENGINEERS (SAE) LEVELS OF AUTOMATION: The SAE produced information outlining six levels (0–5) of driving automation. The levels are a widely used standard to guide the integration of driver assistance technologies on public roadways. The US Department of Transportation (USDOT) endorses the SAE (2018) level definitions as outlined in standard JS3016 *Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles.* Aided by authors Lee and Hess (2020), the six levels of driving automation are described below in layman's terms:

- **SAE Level Zero:** This level encompasses limited warning and momentary emergency interventions. Level Zero is beginning to reach the cusp of becoming obsolete as more cars today are being manufactured with some degree of advanced driver-assistance technology.
- **SAE Level One:** This level includes braking/acceleration support **or** steering interventions.
- **SAE Level Two:** This level implements both braking/acceleration **and** steering support systems.
- **SAE Level Three:** This level is the first that implements *automated* driving features. In Level Three, the vehicle can drive itself under defined limited conditions and **requires** a driver to be present and attentive to take over certain driving tasks.

- **SAE Level Four:** Level Four is similar to Level Three in that it will operate in limited conditions under a defined domain. However, it does not require a driver to be present to take over a driving task.
- **SAE Level Five:** This level is completely autonomous and can operate without any restriction of location or conditions.

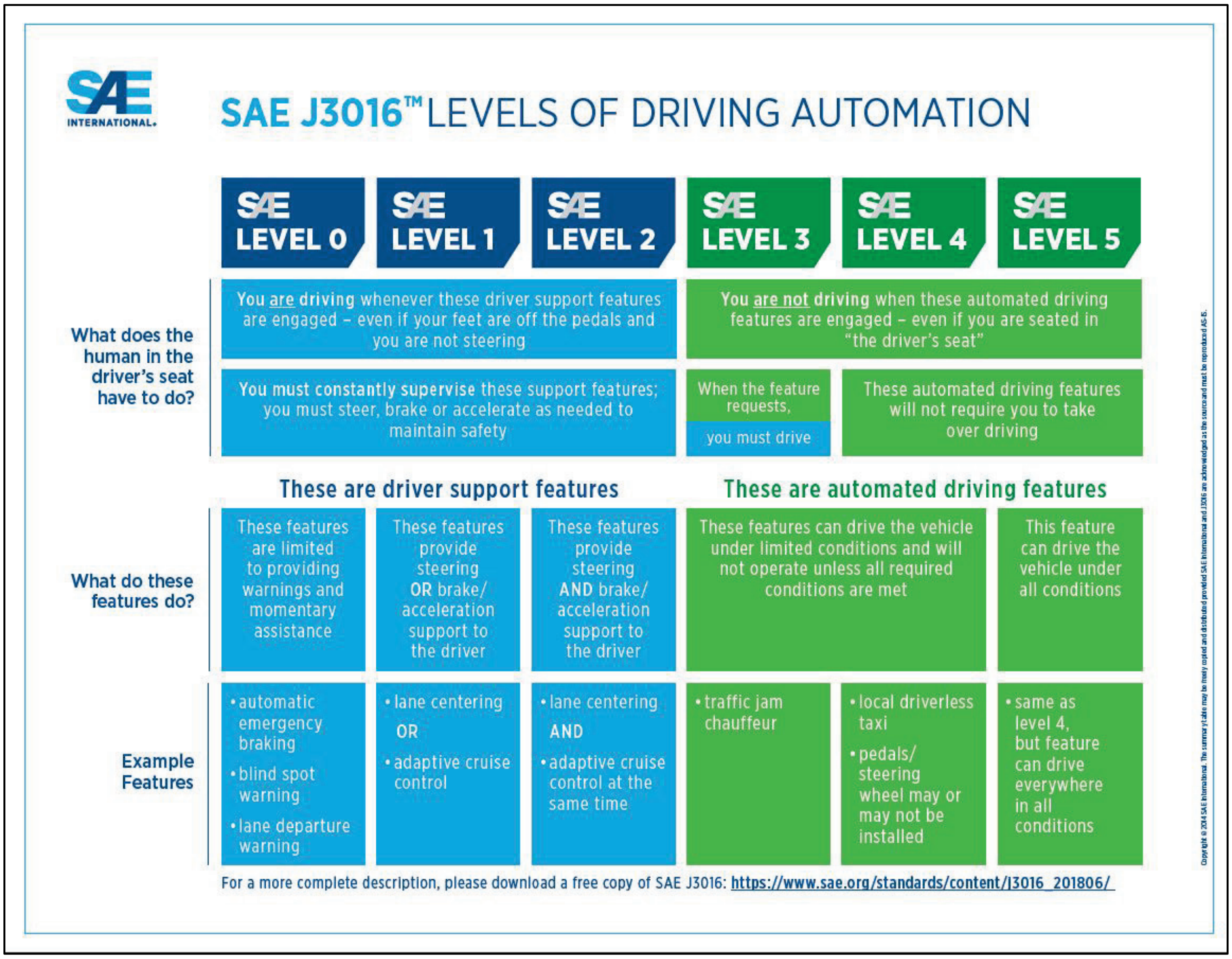

Figure 1. SAE levels of driving automation (SAE 2018).

The USDOT uses the term automated *vehicle* to describe a vehicle fitted with **any** form of driving automation Levels 1 through 5 (Hess and Lee 2020). An automated driving *system* under SAE definition is used to refer to Levels 3 through 5 (Hess and Lee 2020). In an interview with Scott Totman, vice president of engineering at DivvyCloud, Totman explains the difference between using the terms *automated* versus *autonomous*. Matteson (2019) notes that whereas an automated system runs within a defined set of parameters, performing a specific function repeatedly and efficiently, an autonomous system is self-thinking, making its own decision on an action to perform in a non-determined environment.

SAE TAXONOMY FOR DRIVING AUTOMATION: Beyond detailed levels, SAE has provided a taxonomy of definitions for supporting terms related to driving automation in standard J3016. This information was developed to provide a framework for automation specification and technical requirements, provide clarity and stability in communication regarding driving automation, and help to define scope in emerging policy environment (SAE 2018). Many enacted state-level bills regarding autonomous operations have implemented the taxonomy into their legislation for clarity and consistency. Below are examples of that standard language to aid in an informed understanding of the AV environment apparent in the remainder of this report.

Table 1. Definitions of terms related to driving automation systems (SAE 2018).

Term	Definition
Automated Driving System (ADS)	The hardware and software that are collectively capable of performing the entire Dynamic Driving Task (DDT) on a sustained basis, regardless of whether it is limited to a specific operational design domain (ODD).
Conventional Vehicle	A vehicle designed to be operated by a conventional driver during part or all of every trip.
Driving Automation	The performance by hardware/software systems of part or all of the DDT on a sustained basis.
Dynamic Driving Task (DDT)	All of the real-time operational and tactical functions required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints, and including without limitation the following: • Lateral vehicle motion control via steering (operational) • Longitudinal vehicle motion control via acceleration and deceleration (operational) • Monitoring the driving environment via object and event detection, recognition, classification, and response preparation (operational and tactical) • Object and event response execution (operational and tactical); maneuver planning (tactical) • Enhancing conspicuity via lighting, signaling, and gesturing, etc. (tactical).
Dynamic Driving Task (DDT) Fallback	The response by the user to either perform the DDT or achieve a minimal risk condition after occurrence of a DDT performance-relevant system failure(s) or upon ODD exit, or the response by an ADS to achieve minimal risk condition, given the same circumstances.
Minimal Risk Conditions	A condition in which a user or an ADS may bring a vehicle after performing the DDT fallback to reduce the risk of a crash when a given trip cannot or should not be completed.
Object and Event Detection and Response	The subtasks of the DDT that include monitoring the driving environment (detecting, recognizing, and classifying objects and events and preparing to respond as needed) and executing an appropriate response to such objects and events (i.e., as needed to complete the DDT and/or DDT fallback).
Operational Design Domain (ODD)	Operating conditions under which a given driving automation system or feature thereof is specifically designed to function, including, but not limited to, environmental, geographical, and time-of-day restrictions, and/or the requisite presence or absence of certain traffic or roadway characteristics.

Human Driver	A user who performs in real time part or all of the DDT and/or DDT fallback for a particular vehicle.
Conventional Driver	A driver who manually exercises in-vehicle braking accelerating, steering, and transmission gear selection input devices to operate a vehicle.
Remote Driver	A driver who is not seated in a position to manually exercise in-vehicle gear selection input devices (if any) but is able to operate the vehicle.

Regulatory Roles. It is critical to define the current roles involved in the automotive industry to understand how they will apply in the autonomous era. Traditionally, the federal role, as prescribed by the NHTSA, involves regulating the performance of motor vehicle and motor vehicle equipment. In other words, the federal level regulates the safety of the vehicle itself. Meanwhile, states and local entities hold regulatory responsibility in terms of the human driver and vehicle operation. They are conventionally responsible for licensing drivers, registering vehicles, establishing rules of the road, and formulating liability and insurance policy. In its 2018 guiding document, *Preparing for the Future of Transportation: Automated Vehicle 3.0* (AV 3.0), the USDOT highlights its reliance on entities to stay aligned with these traditional roles, stating that they are generally well suited for automation. However, conventional roles likely face a more complex relationship with higher automation levels — who regulates and holds responsibility when the car itself is doing the driving?

FEDERAL LEVEL INVOLVEMENT IN AV REGULATION: At the federal level of involvement, there are many entities overseeing various aspects of the Nation's transportation system. Primary authorities include NHTSA, the Federal Motor Carrier Safety Administration (FMCSA), the Federal Highway Administration (FHWA), and the Federal Transit Administration (FTA). Each entity is adapting to incorporate safety and to address policy issues in the face of automation.

NHTSA has overarching authority of automated driving system (ADS)-equipped vehicles themselves and other automated vehicle technologies. No state or local government may enforce a law on the safety performance of a motor vehicle or equipment that diverges from the NHTSA standard (USDOT 2018).

FMCSA regulates the safety of commercial motor carriers, their drivers, and operations. They uphold a core mission of reducing fatalities and crashes involving commercial vehicles. The Department of Transportation (DOT) prescribes the best way to accomplish this mission is to avoid unnecessary barriers to ADS development (USDOT 2018).

The FHWA is another key body in the AV environment as it supports state and local governments in the design, construction, and maintenance of the Nation's roads. Quality of road marking, signage, and traffic control devices are a key part in safe driving for both humans and AVs (USDOT 2018). The FHWA and other stakeholders are conducting research to improve the prescribed standards for traffic control devices to better fit the needs of emerging AV technologies (USDOT 2018).

The FTA has roles in safety oversight authority in public transportation systems. Through its Public Transportation Agency Safety Plan, it will evaluate the safety impacts of automated buses

(USDOT 2018). The agency aims to prepare for automation in transit through enabling research to achieve effective deployments, demonstrate technologies, and transfer knowledge (USDOT 2018).

Federal Motor Vehicle Safety Standards (FMVSS). NHTSA, under legislative mandate, issues FMVSS for motor vehicles and their associated equipment. Steven Wernikoff, partner and co-leader in data security and privacy litigation practice at Honigman LLP in Chicago (Wernikoff 2020), details that by complying with these standards, manufacturers aim to protect against risks as a result of automobile design, construction, or performance. Unfortunately, most AVs do not comply with said standards as many refer directly to a human driver and manually operated control systems including brake pedals or steering wheels, for example. Currently, NHTSA can annually exempt up to 2,500 vehicles per manufacturer from safety standards if proven the vehicle can operate in a comparably safe, or safer, manner than if it followed the standards (Wernikoff 2020). Seeking an exemption is one way AV manufacturers can place their vehicle on public roads. Another way Wernikoff mentions to expedite the process is to comply with safety standards that are relevant. For example, many conventional vehicles that otherwise comply with standards are being modified with autonomy kits. Likewise, manufacturers can simply wait for standards to be amended, a movement that has already been initiated with proposed changes to applicable standards (Wernikoff 2020).

The Case of Nuro: First Approved FMVSS Exemption for Autonomous Operations. Nuro Inc. is a company that developed an AV for local goods delivery. The organization made history in February of 2020 as the first manufacturer to be granted an exemption by NHTSA for AV operations. It was granted an exemption to three specific standards including the requirement for (1) rearview mirrors, (2) windshields, and (3) backup cameras.

Nuro did not need to provide information about how well the vehicle drove to receive an exemption. According to the official NHTSA exemption Federal Register 85 FR 7826 (NHTSA 2020), automated driving capabilities are not necessarily a factor as they are currently not regulated under the FMVSS. This case involved a low-speed, exclusively cargo-carrying vehicle. Conversely, driving capabilities may be assessed in an automated passenger vehicle operating at conventional speeds. Overall, the success of Nuro may be a critical tipping point for both development and acceptance of AV technologies in conjunction with the regulatory environment.

Figure 2. Nuro autonomous delivery vehicle (Davies 2019).

Attempted Federal Law: SELF DRIVE/AV START Act. In 2017, the certainty that manufacturers and municipalities alike were looking for appeared for the first time on the federal legislative stage. The SELF DRIVE (House)/AV START Act (Senate) drew in five key components to regulate AVs and their development:

1. The Act would mandate safety self-assessments. Developed by NHTSA in 2017 as a voluntary measure, the safety self-assessment is an outlet for AV developers or manufacturers to reveal to the public how they are addressing safety in their testing of their technologies.
2. The Act would review and update FMVSS. As mentioned in the preceding, many FMVSS are currently directed to conventional vehicles, making autonomous operations non-compliant.
3. The Act would increase exemptions to FMVSS. NHTSA can currently exempt 2,500 vehicles per entity each year from complying with these standards. The act would allow exemption for an estimated 80K to 100K vehicles.
4. The Act would require a written cybersecurity plan detailing potential threats, protection measures, and a plan of action given a system breach.
5. The Act would require a written privacy plan detailing how the entity would protect the collection, use, and sharing of Personally Identifiable Information.

The bill did not pass when it was proposed in the Senate. According to Wernikoff (2020), one of the main reasons the bill was brought to a halt was that there were several accidents involving AVs around the time the law was nearly enacted. However, out of these occurrences emerged a necessary dialogue on AV safety. A report by the Congressional Research Service (2020) noted other key areas of controversy that led to the bill not passing including: the extent to which regulatory roles would change, the number of vehicles that would be operating on the road exempt from safety standards, amount of detail in legislation addressing cybersecurity, and extent to which different entities have in accessing data collected by the vehicle.

Federal Guidance. In the absence of defined federal regulation, federal *guidance* has been provided to states wishing to implement ADS into their transportation environment. This guidance was dispersed in the USDOT and NHTSA 2017 report, Automated Driving Systems 2.0: A Vision for Safety. The following best practices were outlined for states to consider when creating legislation (AV 2.0 2017):

1. Provide a technology-neutral environment. This practice calls for states to not place any unnecessary limitations on testing or deployment allowing only certain entities into the market. By avoiding such barriers, needed competition and innovation can flourish.
2. Provide licensing and registration procedures. As mentioned in the preceding, states hold the role of licensing and registration. The present goal is to maintain productive information collection of vehicle operations. To do this, NHTSA recommends first updating the definition of "motor vehicle" to include *any* vehicle operating on the state roadways. NHTSA also recommends extending conventional vehicle processes to the new systems including licensing ADS entities and test operators, registering all ADS-equipped vehicles, and establishing proof of financial responsibility (i.e., insurance or equivalent).
3. Provide reporting and communications methods for public safety officials. In this practice, states are advised to develop procedures in reporting incidents involving ADSs to public safety agencies. Having strong and open communication platforms between testing entities and public safety agencies will enhance safety of all road users as a greater understanding of the technology and its capabilities are presented.
4. Review traffic laws and regulations that may serve as barriers to operation of ADSs. This guidance asks states to examine their vehicle and traffic laws and determine if there are unnecessary regulations that would hinder the deployment of AVs on public roads. For example, some states require the human operator to have at least one hand on the wheel while driving.

These initial four best practices were bolstered in the 2018 iteration *Preparing for the Future of Transportation: Automated Vehicles 3.0*. It includes three extra points of guidance to states in crafting legislation and includes engaging USDOT on legislative technical assistance, adopting terminology defined through voluntary technical standards, and assessing state roadway readiness (AV 30 2018).

Recognizing local government's noteworthy influence of land use that will inherently be altered with the emergence of AVs, federal guidance has been provided to local-level leaders as they seek to formulate policies. Five considerations are detailed including (USDOT 2018) the following:

1. Facilitate safe testing and operation of automated vehicles on local streets.
2. Understand near-term opportunities that automation may provide.
3. Consider how land use will be affected.
4. Consider the potential of increased congestion and how it can be managed.
5. Engage with citizens.

STATE LEVEL LEGISLATION FOR AV OPERATIONS: As technology continues to progress at an impressive rate, states have led the movement towards establishing legislation on AVs despite the possibility of future federal policy later preempting their actions. Nevada was the first state to pass an AV law in 2011. According to the National Conference of State Legislators, by 2012 six states had introduced legislation on AVs. This has increased incrementally since then, reaching 89 enacted bills over 37 states as of September 2020.

Many state policies are preliminary in scope. The current enacted legislation follows a very similar packaged format across states, widely taking into account federal guidance. Commonly, the bill will introduce a definition of autonomous systems and associated technology taxonomy. Following, rulings involving operation protocols, licensing, insurance, liability, and/or crash reporting procedures are typically instituted. Many bills also aim to establish a committee or working group to understand the technology and its potential interaction with the state. The most common topic of legislation falls under the commercial realm. The resulting verdict allows for closer following distances of non-lead vehicles in autonomous platoons.

States can be generally placed in three categories dependent on their approach towards AV policy. The three categories, as outlined by Simmons et. al. (2020) are permissive, moderate, and conservative. The authors describe permissive states as those placing their focus primarily on the economic development possibility of AVs. Such states therefore generally engage in a less restrictive policy environment. Moderate states ideally seek a balance between both safety and economic potential (Simmons 2020). The authors detail that these states are welcoming to AV testing but implementing tighter restrictions for public road deployment. Conservative states prioritize safety. Simmons (2020) notes conservative states will have robust requirements and restrictions for AV testing processes. They will also commonly opt for soft measures such as creating committees to study or do research.

Described below are the common policy themes that emerge from the analysis of state-enacted policy:

Research and Policy Development. With fast emergence of new innovation and the desire to regulate it, states have enacted legislation that highlights their interest in continuing to understand and research autonomous systems and their operation potential. To spearhead the operations, states have acted to establish commissions and require studies convening many stakeholders. This action is common by conservative classified states to prioritize safety while still placing a foot forward in the AV environment.

In a broad sense, a commission or research study is lawfully enacted to review the state's current automotive laws and identify disconnects that may exist in autonomous operations. Additional tasks to be completed by these groups may include but are not limited to studying the operation of self-driving vehicles, examining impacts of autonomous systems on safety and economy, and evaluating pilot programs or other state practices. Ultimately, commissions or studies are meant to produce a collective of information to advise in policy decision-making.

Licensing Procedures. Licensing processes vary across state lines. The pending question regards if the person inside a vehicle equipped with autonomous driving should hold a valid driver's license. In the cases where states do require a person to have a driver's license, it is most commonly for one of two reasons. The first is that it is required for a driver specifically in testing situations**.** Test drivers typically have to acquire specific training or authorization in autonomous systems. In the case of vehicle testing, a driver may need to take over where the ADS has failed. Hence, there is a need to be able to functionally, and legally, drive. The second most frequent instance necessitating the need for the driver to have a license is on the commercial front. Commercial vehicle autonomy is often associated with platooning, or the linking of two or more vehicles using connected and/or automated technologies. The technology needs conventional driving methods to navigate first- and last-mile maneuvers. Commercial driving itself is more intensive than conventional driving, requiring a separate class license. Even states that allow remote operators for non-lead platoon vehicles require the remote operator to hold a proper license.

In the permissive states where licensing is **not** required, it is familiar to define the ADS, when engaged, as the operator. The system itself is then considered licensed to drive the vehicle. The claim has roots in the assumption that the system is operating in a fully autonomous mode. Therefore, the ADS is completely responsible for driving tasks and compliant operation.

Operation on Public Roadways. Similar to licensing justification, the states that require someone to be physically in the driver's seat of a vehicle that has autonomous technology engaged is primarily for testing and commercial purposes. Outside of this, several states *will allow* AVs to operate without someone physically present in a driver's seat under certain prerequisites. Some of the most common conditions in legislation are as follows:

1. Vehicle must be capable of achieving minimal risk condition upon failure of its automated driving system to perform the dynamic driving task.
2. Vehicle is certified by manufacturers to be compliant with FMVSS.
3. Vehicle must be capable of operating in compliance with applicable traffic and motor vehicle safety laws of the state.

Additionally, there has been influence in policy on the use of devices while driving. In conventional terms, it is illegal to operate devices with electronic visual displays while driving (e.g., outside of certain exceptions such as the Global Positioning System). However, three states have made it a point to exempt the prohibition for those in an autonomously operated vehicle. This motion highlights permissive tendencies disregarding safety.

Insurance and Liability. Following conventional automobile conditions, whether conservative, moderate, or permissive, no state with enacted legislation explicitly waives the requirement for insurance and registration. Before testing or operating a vehicle equipped with an automated driving system, a person *must* submit an instrument of insurance. For testing purposes, specifically, it is most commonly required to provide proof of insurance coverage in the amount of 5M dollars.

In terms of liability, several state enacted bills actively seeking to protect manufacturers from being liable for incidents if a third party modifies the vehicle with autonomous technology. One state furthered this exemption to mechanics and repair shops on repairing automated vehicles. These protections may be seen as a crucial catalyst to further encourage AV testing.

Additionally, direct instances of liability for accidents are commonly described as subject to common law or applicable federal/state law. Essentially, the presence of an ADS system as driver or operator does not exempt the incident from regulatory provisions. Many states have regulated these processes in the event of a roadway crash involving an AV. The procedures generally follow conventional law in which the vehicle must remain on the scene. However, if no one is inside the vehicle at the time of the incident, the owner or person on behalf of the owner shall report the incident and supply law enforcement with necessary information.

Regulating Local Authority. Fourteen states have taken the action of preempting local governments from regulating AVs to some capacity. States commonly place their state department of transportation as primary authority. They make it a point that the department has jurisdiction over setting standards and requirements on autonomous systems within the state. Consequently, this preempts local entities from imposing taxes, fees, or other requirements on the operation.

Taking such action originally aims to remove unnecessary barriers by preventing conflict between state and local authorities. However, as Fleming (2020) discusses in her Issue Paper regarding technology outpacing vehicle policy, she provides that such action can be counterproductive if there are already overlapping authorities. Additional tensions could arise in the regulatory environment if the state preempts local governance but fails to provide proper state level regulation, distinctly stifling innovation (Fleming 2020).

Platoon Operations. As mentioned, platooning is the most widely and consistently regulated AV function amongst states. It is a common operation in the commercial sector. Even conservative classified states will commonly permit platooning even if they do not allow AV technology for other purposes. To date, 20 states have regulated platooning. Overall, such regulation most prominently seeks to exempt non-lead vehicles in a platoon from the laws regarding minimum following distance requirements. This allows the connected vehicles to operate more closely together in the hopes of increased efficiency and reduced congestion.

In most cases, to commence operation, the person or organization associated with the potential platoon must file a general operation plan to an associated state contact (department of transportation, commissioner, etc.) who will accept or deny the request. The plan of operation may include, where applicable, information such as length and configuration of the platoon, proposed route and timing, and license or registration certification. Some states also place a cap on the number of vehicles allowed in a platoon or require licensed drivers to occupy the driver's seat for consistent observation, for example.

California: The Model State. The State of California is widely recognized as a model state for not only its position at the heart of innovation in AV technology but also for its regulatory approach. California is arguably the most successful moderate state in balancing the economic and safety aspect of emerging autonomous driving. The regulation itself is permissive with three designated permit levels allowing up to full operations on public roads without a human safety driver. The balancing factors are the safety conditions a testing entity must meet and document before getting the approval to operate. Each of the three permit levels (testing with safety driver, testing driverless, and permit to deploy on public streets) have varying requirements for operation given their differing safety risks. Descriptions of the permits and levels can be found in the Appendix A. The State of California Department of Motor Vehicles (DMV) (2018) requires **all** entities involved in the permit system must submit yearly disengagement reports that reveal how often the vehicles disengaged from autonomous mode during tests. The DMV also requires documentation of compliance with FMVSS and a functional safety plan identifying potential hazards that can occur during testing. As of September 1, 2020, there were 61 Autonomous Vehicle Testing Permit holders.

Autonomous technology will inherently be a collector of significant amounts of potentially sensitive information. Another focus placing California first in the AV stage is that it is the only state that has comprehensive legislation governing data privacy **and** security. In a white paper published by Dentons Law Firm in 2019, it details the California Consumer Right to Privacy Act. Recently established in 2020, it gives consumers overarching control of information that is collected about them (Dentons 2019). The connected device legislation mandates that Internet of Things devices incorporate reasonable security features to prevent unauthorized use of collected information (Dentons 2019).

LOCAL LEVEL ACTION TOWARDS AV ADVANCEMENT: On a smaller scale, cities themselves hold a unique role in the AV landscape. Local governments have control over a large portion of the Nation's roadways and parking infrastructure. There is also a significant influence of land use via zoning at the local level. Additionally, local government leaders are the closest contact point to citizens. According to the National League of Cities (NLC) Municipal Action Guide (NLC 2018), a lack of federal regulation has allowed cities and AV pilots to develop agreements at will. In this manner, cities can craft a localized approach that pairs AV pilots with specific municipal goals (NLC 2018).

One regulatory power that cities can express to further AV advancement is enacting executive orders or city council resolutions. According to the NLC, such active action can initiate the arrival of pilots by spearheading legislation around the issue. The Municipal Action Guide (NLC 2018) outlines an executive order or city council resolution does not expressly need to amend or make new laws but can rather be utilized to convey interest in hosting pilots and direct officials to engage with the private sector. The action aims to send a signal that the private sector is welcome and addressing automation is a priority for the city. Another feasible regulatory approach for cities is a public request for proposal or request for information (RFI). These mechanisms are an effective way to establish direct dialogue with the private sector if an organic AV presence does not emerge (NLC 2018). Washington, DC, is an example of such success whereas it had a line added in the municipal code in 2013 allowing AVs to operate in its streets (NLC 2018). However, it was not until it released an RFI in 2018 that it secured a pilot.

As discussed in the preceding, some states make the decision to preempt local governments from regulating AVs in their jurisdiction. While the original intent is to prevent conflicting rules between the two entities, it may quickly become more complex. To reduce such inconsistencies among varying regulatory levels, cities and states can work in tandem. By co-releasing their regulations or orders, it will provide a clear trajectory towards AV deployment. In Boston, for example, the mayor signed an executive order directing the transportation department to create guidelines for AV testing (NLC 2018). Meanwhile, the governor of Massachusetts released a corresponding executive order establishing an AV working group and requiring pilots to enter a memorandum of understanding (MOU) with the Massachusetts DOT and the municipality where testing would occur (NLC 2018).

RELATED POLICY FOR AV OPERATIONS IN THE MILITARY: The development of autonomous technologies has a promising future for both defense and non-defense applications in military systems throughout the Nation. For the operation of AVs on military installations, it is important to note that military bodies operate under their own jurisdiction, developing their own set of guiding regulations. In general, military installations operate in a similar respect to a traditional city but with higher security fundamentals.

Risk Management. One noteworthy influence towards permissible operations is risk aversion. Autonomous technology is continuously changing and developing, posing many uncertainties in terms of safety in operating capabilities. Therefore, before testing AVs on a military installation, whether in an on- or off-cantonment setting, entities must collaborate with local commanders to identify their attitudes on risk aversion. What a commander will permit will likely vary across different installations. Only a person with command authority of the area in which a platform will be tested can authorize its use. Activity on prospective testing areas will also be considered, impacting necessary operating protocols. For example, training areas that are considered a range complex have an inherently higher risk. In this manner, additional paperwork would be required to allow interested parties onto the specific facility to test an AV.

To aid in understanding the risk of AV testing, the Army Risk Management Framework will likely be utilized. The framework operates to identify, assess, and control risk. The Department of the Army (2014) details five key steps to be implemented to achieve the risk management goal including the following:

1. Identify the hazards.
2. Assess the hazards.
3. Develop controls and make risk decisions.
4. Implement controls.
5. Supervise and evaluate.

The Risk Management Framework classifies risk based on two elements: severity and frequency. There are four levels of severity ranging from negligible to catastrophic. The five levels of frequency range from unlikely to frequent. Using the matrix provided in Figure 3 below, risk is determined in one of four iterations from low to extremely high. When risk is determined, proper safeguards can be established. Before an activity with potential risk is performed at an Army installation, the entity performing the action must fill out a Deliberate Risk Assessment Form (see Appendix B). The form outlines full documentation of each of the aforementioned five steps. The form is saved for use in an assessment by the Army Safety Center at Fort Rucker in the event of an incident.

Risk Assessment Matrix		Probability *(expected frequency)*				
		Frequent: Continuous, regular, or inevitable occurrences	**Likely:** Several or numerous occurrences	**Occasional:** Sporadic or intermittent occurrences	**Seldom:** Infrequent occurrences	**Unlikely:** Possible occurrences but improbable
Severity *(expected consequence)*		A	B	C	D	E
Catastrophic: *Mission failure, unit readiness eliminated; death, unacceptable loss or damage*	I	EH	EH	H	H	M
Critical: *Significantly degraded unit readiness or mission capability; severe injury, illness, loss or damage*	II	EH	H	H	M	L
Moderate: *Somewhat degraded unit readiness or mission capability; minor injury, illness, loss, or damage*	III	H	M	M	L	L
Negligible: *Little or no impact to unit readiness or mission capability; minimal injury, loss, or damage*	IV	M	L	L	L	L
Legend: **EH** - Extremely High Risk **H** - High Risk **M** - Medium Risk **L** - Low Risk						

Figure 3. Risk assessment matrix (DOA 2014).

With upholding safety and avoiding unnecessary risk as a primary factor of effective site development to test autonomous technologies, an official application will likely be developed to allow site operators to control the usage. The form will be intentionally constructed to record thorough information regarding the testing entity, person or persons operating the vehicle, vehicle technologies and capabilities, as well as the desired testing needs. Applications can be rigorously reviewed on a case-by-case basis to ensure that testing entities are upholding proper safety procedures. The documentation may also serve as a useful aid in research processes as testing plans and specific technology used in testing may be outlined. The information can allow for partners to identify traceable trends in innovation among other topic items. A draft example of an application document is provided in Appendix C.

Licensing Processes. Licensing requirements for military operators of Army motor vehicles diverge slightly based on if the operator will be exclusively operating on the installation or driving off of it in any event. According to Army Regulation 600-55 (2019), if driving off the installation, operators must have a valid OF 346 (US Government Motor Vehicle Operator's Identification Card) or DA Form 5948-E (Operator's Permit Record). However, such form requirements can be waived by commanders for operation of small (under 10,000 pounds) non-tactical administrative vehicles (DOA 2019). The regulation also states the operator must possess a valid civilian driver's license (DOA 2019). When driving exclusively on an installation, operators must have valid OF 346 or DA Form 598-E but are not required to have a civilian license for tactical vehicle operations (DOA 2019). However, operator will still need to be licensed for specific equipment as detailed below.

The regulation requires that prospective operators go through various stages of screening that determine physical, mental, and emotional aptitude to be approved for Initial Operator Training. The three-phase qualification training process applies to all wheeled, tracked, and mechanical or ground support equipment that requires operator licensing (DOA 2019). Upon passing all three phases as detailed below, the driver will be permitted to operate the desired vehicle. There is an annual recertification required to maintain license to operate the given Army vehicle.

1. Phase I (Initial Operator Training) is classroom training on administrative, technical, regulatory, and basic skill elements of operating Army equipment.
2. Phase II (Equipment Training) is classroom and hands-on instruction for the piece(s) of equipment the prospective operator is to be licensed.
3. Phase III (Training Validation/Performance Road Test) is a comprehensive event certifying the trainee is proficient in vehicle operations and equipment. It includes a preventative maintenance checks and services test, a vehicle control test, and a road test.

Traffic Supervision. Army Regulation 190-5 Motor Vehicle Traffic Supervision (DOA 2006) provides that installation commanders hold responsibility in developing traffic planning and codes to allow safe and efficient movement on the property. Pertinent to the emergence of AVs, traffic codes developed will contain rules of the road. The regulation details that codes will, where possible, conform to the code of the state in which the installation is located (DOA 2006). Three guiding standards the installation codes must incorporate include (DOA 2006):

1. Highway Safety Program Standards (23 USC 402) – developed by each state in compliance with uniform guidelines to reduce traffic accidents and resulting personal or property damage.
2. Applicable portions of the Uniform Vehicle Code and Model Traffic Ordinance – guide for developing standard state motor vehicle and traffic laws.

While these regulations are based on conventional vehicle operations, it is likely commanders will need to establish their own variations of rules for AVs on their installations. This is especially applicable in states that have only passed soft measures for AVs, or none at all. Where this is true, installations could have a role in paving the way in aiding state function or understanding of AV regulation. The introduction of codes will likely vary across installations once again depending on the commander's attitude towards risk. Additional considerations when developing AV traffic codes may include an overview of activities taking place at the installation and overall characteristics to determine if AVs can provide positive, safe, and logistically feasible use.

Insurance and Liability. The United States Government is entirely self-insured on its vehicles. Claims issued against the government are backed by the credit of the United States. The US House of Representatives (n.d.) outlines claims are payable under the Federal Tort Claims Act, 28 USC § 2671 et seq. (US House of Representatives, n.d.), which provides remedy for any party injured or property damaged by actions of a federal employee. The United States absorbs the loss, accepting the resulting liability to the same extent an individual would in such circumstances (US House of Representatives, n.d.).

Privately owned vehicles on installations are covered by the owner's individual insurance provider. Similarly, in the case of autonomy, any private entities wishing to test their AV on an installation or military training area would need their own private insurance. Proof of insurance or equivalent would need to be provided to, and approved by, the commander before testing. This process ensures proper mechanisms are in place in the event of an accident.

Vehicle Design. Traditionally, the safety of motor vehicles and associated motor vehicle equipment is regulated under the NHTSA FMVSS. These same standards apply to commercial design vehicles that are purchased, leased, or rented by the Department of Defense (DoD) as per Department of Defense Instruction (DoDI) 6055.04 (DoD 2018). Further, the instruction document (DoD 2018) outlines commercial design vehicles procured and leased by the government be equipped with air bags, anti-lock braking systems, and electronic stability control where available. Additionally, DoDI 6055.04 (DoD 2018) calls for commercial vehicles that are at a high risk of mishap be equipped with a safety monitoring device to “support safe vehicle operations and influence driver behavior.” Design requirements of low-speed vehicles in particular that operate on an installation or public roadways are regulated by Part 571.500 of Title 49, Code of Federal Regulations (DoD 2018).

Regarding tactical and combat vehicles, NHTSA established an overarching exemption recognizing the unique needs of the armed forces. According to an NHTSA interpretation letter responding to Ms. Leah Kelly of the California Department of Motor Vehicles (Glassman 2004), the exemption was based on determination that compliance with the FMVSS may limit the capability of a given vehicle to complete its military mission. The exemption 49 CRF 571.7 (c) states, “no standard applied to a vehicle or item of equipment manufactured for, and sold directly to, the Armed Forces of United States in conformity with contractual specifications.” The exemption would not apply if any modifications made would not further a purpose specific to military operations. Although NHTSA standards do not apply, the DoD requires through DoDI 6055.04 (DoD 2018) that these special purpose vehicles are equipped with safety belts, shoulder harnesses, and occupant rollover protection. Exemptions for such design can be made by the risk acceptance authority. Additional safety characteristics of tactical vehicles are provided in Military Standard MIL-STD-1180B (1). Regardless of type, all government-maintained vehicles are required to pass an annual safety inspection.

Agency Agreements. The development of new AV technologies will continue to require multi-level stakeholder engagement. There are a variety of agreements available to create a formal linear bridge towards achieving beneficial innovation among partners and federal agencies. The most efficient partnering mechanism is reimbursable assistance. This mechanism is only available to US government agencies. Reimbursable assistance authorizes research, development, and technical assistance to other federal agencies through the Economy in Government Act and the Chief’s Economy Act.

The Acts emphasize that when the federal government sends or receives money in an agreement, the operation must not compete with the commercial sector, another noteworthy policy for new partnerships in innovation. In other words, for the usage or development of a site on a military installation for AV testing, it must offer a service that is unique from what is readily accessible in the market. Availability of the facility for testing can also play a role in avoiding a site being deemed competitive. If not, many test sites are available with needed features, the operation of a military site can be utilized in a way that reduces the market pressures, making it viable.

To provide context to policy and agreements, Fort Leonard Wood located in Missouri has entered into agreement with the US Army Engineer Research and Development Center (ERDC), Construction Engineering Research Laboratory (CERL), allowing CERL to be the tenant organization at Training Area (TA)-231 in which it can schedule to use the site for desired research and development operations. This relationship is established through a Memorandum of Agreement providing exchange for funds. With this, CERL plans to develop training course TA-

231 as a closed-course AV testing facility. The site will be outfitted with necessary infrastructure to challenge vehicles and collect data. This agreement establishes CERL as an intermediary between Fort Leonard Wood and federal or private sector entities that want to test their technologies. Thus, CERL must develop additional formal agreements with an entity that wishes to test on its tenant site. Agreements can be further utilized as a framework to understand the entity's autonomy testing needs to pair it with the proper facility or features available.

Classification and data sharing are an additional hurdle in determined partnerships with a federal agency. It is especially difficult in an AV context because the systems capture large quantities of potentially sensitive information. In most technology transfer agreements, the providing agency receiving money does not retain data rights. As in the case example above, ERDC CERL will initially not have rights to the data collected by agencies coming to test on the site. Sharing data requires a specific intergovernmental agreement or MOU that entails extensive legal review, and a classification must be established for each component of the data.

Engaging with other federal agencies is arguably the most efficient way to proceed in terms of bringing AV testing to a military installation due to potential uncertainties in competition and security that may require extensive approvals. However, there are additional agreements available for coordination with private sector. One such example is the operation of the Olli autonomous shuttle pilot at Joint Base Meyer Henderson-Hall. For this pilot project directed by ERDC CERL, the agency entered into an Educational Partnership Agreement with George Mason University. The agreement establishes ability to share data from the pilot operation in support of the university's academic research. A Cooperative Research and Development Agreement was also established, formally inciting collaboration on a research project of mutual interest. It allows CERL and the non-federal partner to contribute staff, equipment, and supplies to each other for the project duration. The federal partner can receive money but is not able to send. There are several other university agreements pending for related projects.

Privacy and Security. Today's vehicles collect, store, and transmit a significant amount of data. Data can range from information regarding weather, road conditions, people, and location, for example. Some of this information can be deemed sensitive. The more connected a vehicle is to its surroundings, the more vulnerable it may be to breaches or hacking events. According to previously cited Wernikoff (2020), currently, law regulating data privacy and security is widely based on industry without any existing national policy. Addressing cyber incidents requires coordination across all levels of government.

The Driver Privacy Act of 2015 (2015) is one example of industry level security measures. The Act states that the owner or lessee of a motor vehicle is the owner of all the data collected by an Event Data Recorder. For an entity outside the owner or lessee to access the information, the entity must have one or more of the following appointed reasons (Driver Privacy Act 2015):

1. The entity has consent of owner or lessee.
2. The entity has court authority.
3. The entity is conducting investigation authorized by federal law.
4. The entity demonstrates it is necessary to facilitate medical care.
5. The entity is conducting traffic safety research.

Another set of factors in the automotive privacy and security environment are the Automotive Consumer Privacy Protection Principles developed in 2014. This was an agreement of principles among 20 automakers on what would be done with data associated with people or their vehicles. According to Auto Alliance (n.d.) the three guiding commitments include the following:

1. Provide customers with clear notice about the types of information collected and how it is used.
2. Provide ways for customers to manage their data.
3. Not use geo-location, biometrics, or driver behavior information for marketing or sharing with third parties without consent of user.

These principles are incorporated with the Federal Trade Commission (FTC) Act, which aims to protect consumers and competition by preventing unfair and deceptive business practices. The AV guidance document, AV 3.0 (2018), explains that USDOT works closely with the FTC to support said consumer protections and provide information regarding consumer privacy in the transport environment. The DOT also works to consider privacy implications in its own safety regulations and encourages data exchanges to respect privacy (USDOT 2018).

NHTSA has a role in privacy and security through the National Traffic and Motor Vehicle Safety Act. Originally enacted in 1966, this Act was developed to require manufacturers to take action in protecting the public from unreasonable risk of motor vehicle safety. In 2016, NHTSA issued a draft bulletin claiming its authority under the Act extends to software and automated vehicle technologies (Rothenstein 2016). NHTSA also has recall authority over manufacturers if they have not met safety standards or have safety-related defects.

State and local governments also play a valuable role in transportation cybersecurity by investing in improvements to cyber defenses and infrastructure. According to the USDOT in AV 3.0 (2018), these entities "identify, prioritize, and allocate resources to counteract cybersecurity threats." The USDOT (2018) encourages state and local actors to utilize resources provided by the United State Computer Emergency Readiness Team.

LIMITATIONS IN THE POLICY ENVIRONMENT: The lack of clear federal regulation on autonomous systems itself is a noteworthy limitation as its repercussions extend into state and local jurisdictions. States and municipalities have taken actions out of their purview causing a patchwork of regulatory policies. This pattern makes it difficult if one vehicle wants to travel from one state to another. As Wernikoff (2020) notes, it also returns to cause tension in potential federal law, begging the question when the time comes: will federal action preempt well-established state laws?

The policy environment possesses additional uncertainties when examining the SAE levels. Level Three has proven the most questionable resulting in many manufacturers making the decision to skip past it to develop Level Four-oriented technologies. SAE Level Three is complicated as it relies to a certain degree on driver intervention and reaction time for takeover, which is difficult to measure for safety. Claybrook and Kildare (2018) in their article state that humans are inherently bad at monitoring semi-autonomous systems and are easily distracted. Additionally, many become over reliant on the system and its capabilities. This brings attention back to manufacturers and regulators. As Claybrook and Kildare (2018) suggest, manufacturers must find a way to keep the driver engaged in the task, and policymakers must require such engagement in a meaningful way.

Another limitation as defined by Mordue et al. (2020) reveals that although AV technology is posed to be a proactive solution to automotive safety, the speed at which it is advancing may cause policymakers to respond reactively to close apparent gaps. Further, the authors describe three main sources of policy gaps in the AV environment including the following (Mordue et al. 2020):

1. Varied and insufficient knowledge overall regarding AVs.
2. Unbalanced resource availability between regulators and regulated.
3. The complex, multi-stakeholder, and politically sensitive nature of AV policy can take years to develop and implement.

Cultural and ethical considerations are an additional aspect in policy decision-making processes. These considerations must be assessed at the programming level. If an AV is presented with a dilemma situation, who gets to decide how the car should be programmed to react? A survey conducted by Awad et al. (as cited in Mordue et al. 2020) found that some biases were consistent across regions and cultures such as choosing to save more lives rather than few and sparing humans over animals. However, other factors varied such as gender and social status (Mordue et al. 2020). Also presented is what Iyad Rahwan (2016) calls the tragedy of the algorithmic commons that draws upon the traditional tragedy of the commons concept in which a shared resource is depleted from an individual user(s) acting on self-interest. In an AV landscape, Rahwan explains the common good is minimizing total harm and the users are the passengers. The claim is that by individually prioritizing their own safety, they may be diminishing the collective good (Rahwan 2016). It is algorithmic in the sense that it is not the individual making the decisions but rather that the car manufacturers can program to generally maximize safety for *all* clients. In this way, the car may learn that to achieve this program is to have slightly increased risk for pedestrians and cyclists, for example (Rahwan 2016). In traditional Tragedy of the Commons situations, problems that arise can be solved through regulation by defining constraints and monitoring mechanisms (Rahwan 2016). If regulators are asked to *minimize harm* in an AV environment, it inherently implies that drivers or passengers may be at risk when the vehicle is posed with a situation of choosing to spare more lives (Rahwan 2016). Therefore, as Rahwan concludes, by regulating cars to minimize harm more harm may be created as fewer people will opt into the technology even if it is overall safer for human drivers.

A WAY FORWARD: Policy and regulation will arguably have negligible impact if it does not draw upon a foundation of transparency. Vehicles can be fully regulated in every aspect, yet the introduction of AVs will serve little purpose if the user lacks trust in the system. Thus far, the NHTSA voluntary safety self-assessment has provided an outlet for companies to detail how they are addressing concerns regarding safety and public trust. Currently, 23 companies have provided their assessments. A beneficial addition would be to extend similar reporting capabilities for prospective AV military operations.

Closed-course development and operations are an appropriate intermediate response to legislation. Despite varying legislation passed permitting the operation of AVs on public roads, not all manufacturers or private sector developers will be ready to confidently test publicly. Thus, entities can test in a controlled environment to develop their technologies with overall fewer regulatory barriers. Many real-world scenarios can be replicated in a closed course to provide efficient transferability of the AVs learned behaviors. Closed course also offers an advantage of repeatability to ensure successful vehicle response.

While perfect full automation seems distant, there is no need to wait for this to reap the benefits of the technology. This is why policymakers, manufacturers, and other automation-related stakeholders sit at a crucial crossroad in regulation. Building from the preceding, an educational component in policy is **vital** to safety and in turn, greater public understanding. Integrating informed safety into regulation is a potential tool as technology progresses. As Khastgir (2018) defines, in an AV context, informed safety is the act of briefing the operator about the safety limits of the vehicle and software, enabling them to understand when and how to use the technology. Partaking in informed safety measures may act as a supplemental tool where technology is deficient if capabilities and limitations are defined with certainty (Khastgir 2018).

ADDITIONAL INFORMATION: This Construction Engineering Research Laboratory (CERL) technical note was prepared as part of the US Army Corps of Engineers, ATI program, by Emma L. Smith, Julie L. Webster, and Annette L. Stumpf, US Army Engineer Research and Development Center, CERL, Champaign, IL. Questions pertaining to this CERL technical note may be directed to Annette L. Stumpf, ATI Technical Lead, *Annette.L.Stumpf@usace.army.mil.*

This ERDC/CERL TN-21-2 should be cited as follows:

> Smith, Emma L., Julie L. Webster, and Annette L. Stumpf. 2021. *Autonomous Transport Innovation: The Regulatory Environment of Autonomous Vehicles.* ERDC/CERL TN-21-2. Champaign, IL: US Army Engineer Research and Development Center. *http://dx.doi.org/10.21079/11681/42025*

REFERENCES

Auto Alliance. n.d. *About Automotive Privacy*. *https://www.mcca.com/wp-content/uploads/2019/04/Status-Update-Its-Complicated.pdf*

Claybrook, J., and S. Kildare. 2018. "Autonomous Vehicles: No Driver...No Regulation?" *Science* 361(6397): 36–37. *https://science.sciencemag.org/content/361/6397/36/tab-pdf*

Code of Federal Regulations Title 49. § 571.7 - Applicability.

Congressional Research Service. 2020. *Issues in Autonomous Vehicle Testing and Deployment*. *https://crsreports.congress.gov/product/pdf/R/R45985*

Davies, Alex. 2019. "Softbank Invests $1B in Robo-Delivery Startup Nuro." *https://www.wired.com/story/softbank-nuro-self-driving-investment/*

Dentons. 2019. *Autonomous Vehicles: US Legal and Regulatory Landscape*. *https://ag.hawaii.gov/wp-content/uploads/2019/08/Dentons-US-Autonomous-Vehicles-Whitepaper-August-1-2019.pdf*

Department of Defense. 2018. *DoD Traffic Safety Program*. DoDI 6055.04. *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/605504p.pdf*

DOA (Department of the Army). 2014. *Risk Management*. ATP 5-19. *https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/atp5_19.pdf*

DOA. 2019. *The Army Driver and Operator Standardization Program (Selection, Training, Testing, and Licensing)*. AR 600-55. *https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN22141_R600_55_Admin_FINAL.pdf*

DOA. 2006. *Motor Vehicle Traffic Supervision*. AR 190-5. *https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/r190_5.pdf*

Driver Privacy Act. S.766. 114th Congress. 2015. https://www.congress.gov/bill/114th-congress/senate-bill/766#:~:text=Prohibits%20a%20person%2C%20other%20than,by%20such%20a%20recorder%20unless%3A&text=the%20data%20is%20retrieved%20for,identification%20number%20are%20not%20disclosed

Eno Center for Transportation. 2018. *Autonomous Vehicles and Safety*. YouTube video, 31:58. https://www.youtube.com/watch?v=fAR-OWfnzyQ

Fleming, K. 2020. *Technology is Outpacing State Automated Vehicle Policy*. UC Davis Policy Institute for Energy, Environment, and the Economy. https://escholarship.org/content/qt0k85r9jv/qt0k85r9jv.pdf

Glassman, J. 2004. *California High Mobility Military Vehicle* (CA_HMMV). Received by Kelly, Leah. https://www.nhtsa.gov/interpretations/cahmmv#:~:text=Under%2049%20CFR%20571.7(c,to%20comply%20with%20the%20FMVSSs.&text=In%20establishing%20this%20exemption%2C%20the,not%20be%20sold%20to%20civilians

Khastgir, Siddartha. 2018. *How Safe Does a Driverless Car Need To Be?* YouTube video, 16:52. https://www.youtube.com/watch?v=KrOOXE3SW-A

Lee, D., and D. Hess. 2020. "Regulations for On-Road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization." *Transportation Research Part A: Policy and Practice*. Volume 136: 85–98. https://doi.org/10.1016/j.tra.2020.03.026

Matteson, S. 2019. *Autonomous v. Automated: What Each Means and Why It Matters*. TechRepublic. https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/

Mordue, Greig, Anders Yeung, and Fan Wu. 2020. "The Looming Challenges of Regulating High Level Autonomous Vehicles." *Transportation Research Part A: Policy and Practice*. Volume 132: 174–187. https://doi.org/10.1016/j.tra.2019.11.007

National League of Cities. 2018. *Autonomous Vehicle Pilots Across America*. https://legislature.vermont.gov/Documents/2020/WorkGroups/House%20Transportation/Bills/S.149/Written%20Testimony/S.149~Gwynn%20Zakov~Autonomous%20Vehicles%20Pilots%20Across%20America~4-5-2019.pdf

NHTSA (National Highway Traffic Safety Administration). 2020. *Nuro, Inc.; Grand of Temporary Exemption for a Low-Speed Vehicle with an Automated Driving System*. Federal Register 85 FR 7826. pp. 7826–7842. https://www.federalregister.gov/documents/2020/02/11/2020-02668/nuro-inc-grant-of-temporary-exemption-for-a-low-speed-vehicle-with-an-automated-driving-system

NHTSA. n.d. *Automated Vehicles for Safety*. USDOT. https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

Rahwan, I. 2016. *The Social Dilemma of Driverless Cars*. YouTube video, 13:57. https://www.youtube.com/watch?v=nhCh1pBsS80

Rothenstein, Cliff L. 2016. *NHTSA'S Claimed Jurisdiction over Software and Applications may Stifle Innovation*. https://www.klgates.com/NHTSAs-Claimed-Jurisdiction-Over-Software-and-Applications-May-Stifle-Innovation-04-14-2016

SAE (Society of Automotive Engineers). 2018. *JS3016: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. https://www.sae.org/standards/content/j3016_201806/

Simmons, R. A. 2020. *Driverless Cars, Urban Parking and Land Use*. Chapter 4. London: Routledge. https://doi.org/10.1201/9780429469541

State of California Department of Motor Vehicles. 2018. *Driverless Testing and Public Use Rules for Autonomous Vehicles Approved*. State of California Department of Motor Vehicles. https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/2018/20

USDOT (US Department of Transportation). 2017. *Automated Driving Systems 2.0: A Vision for Safety*. National Highway Traffic Safety Administration. https://www.transportation.gov/av/2.0

USDOT. 2018. *Preparing for the Future of Transportation: Automated Vehicles 3.0*. National Highway Traffic Safety Administration. https://www.transportation.gov/av/3

US House of Representatives. n.d. *Federal Tort Claims Act*. https://www.house.gov/doing-business-with-the-house/leases/federal-tort-claims-act

Wernikoff, Steven. 2020. Autonomous Vehicles Online on Video: Steven Wernikoff on AV regulation. Automotive iQ. Video, 52:26. https://www.automotive-iq.com/autonomous-drive/videos/autonomous-vehicles-online-on-video-steven-wernikoff-on-av-regulation

Appendix A: California Testing Permits and Requirements for Operation

State of California Department of Motor Vehicles, 2018 (via Lee and Hess 2020)

Manufacturers Testing Permit	• Requires human safety driver who is employee, contractor, or designee of manufacturer • Driver must understand limitations and weaknesses of the vehicle • Safety driver must complete a designated training program • Description of training program must be submitted to the state government
Manufacturers Testing Permit – Driverless Vehicle	• Manufacturer must specify the operational design domain of the test vehicle • Provide a list of all public roads in the jurisdiction where vehicles will be tested • Provide date that testing will begin • Provide days and times that testing will be conducted on public roads • Identify number of vehicles to be tested • Identify the types of vehicles to be tested • Provide contact information of the manufacturer • Manufacturer must certify that the vehicle is capable of driving without human presence • Authorities in locations where vehicles will be tested must be provided with written notification • Must be communication link between vehicle and remote monitor

	• Must be communication link between local law enforcement and vehicle • Remote operator must complete required training program
Permit to Deploy Autonomous Vehicles on Public Streets	• Manufacturers must provide a description of the levels of automation of the CAV (3,4,5) • Provide the vehicles operational design domain • Prove compliance with all AMVSS standards • Certify vehicle can meet California's traffic laws • Certify that vehicle meets international cybersecurity standards • Vehicle must be equipped with a data recorder • Vehicle must meet current industry standards to help defend against, detect, and respond to cyber-attacks • Provide a copy of a law enforcement interaction plan

Appendix B: Deliberate Risk Assessment Worksheet

DELIBERATE RISK ASSESSMENT WORKSHEET

1. MISSION/TASK DESCRIPTION	**2. DATE** *(DD/MM/YYYY)*

3. PREPARED BY

a. Name *(Last, First, Middle Initial)*	b. Rank/Grade	c. Duty Title/Position
d. Unit	e. Work Email	f. Telephone *(DSN/Commercial (Include Area Code))*
g. UIC/CIN *(as required)*	h. Training Support/Lesson Plan or OPORD *(as required)*	i. Signature of Preparer

Five steps of Risk Management: (1) Identify the hazards (2) Assess the hazards (3) Develop controls & make decisions (4) Implement controls (5) Supervise and evaluate *(Step numbers not equal to numbered items on form)*

4. SUBTASK/SUBSTEP OF MISSION/TASK	5. HAZARD	6. INITIAL RISK LEVEL	7. CONTROL	8. HOW TO IMPLEMENT/ WHO WILL IMPLEMENT	9. RESIDUAL RISK LEVEL
				How: Who:	
				How: Who:	
				How: Who:	
				How: Who:	
				How: Who:	

Additional entries for items 5 through 9 are provided on page 2.

10. OVERALL RESIDUAL RISK LEVEL *(All controls implemented)*:

☐ EXTREMELY HIGH ☐ HIGH ☐ MEDIUM ☐ LOW

11. OVERALL SUPERVISION PLAN AND RECOMMENDED COURSE OF ACTION

12. APPROVAL OR DISAPPROVAL OF MISSION OR TASK ☐ APPROVE ☐ DISAPPROVE

a. Name *(Last, First, Middle Initial)*	b. Rank/Grade	c. Duty Title/Position	d. Signature of Approval Authority

e. Additional Guidance:

DD FORM 2977, JAN 2014

Page 1 of ____ Pages
Adobe Professional X

DELIBERATE RISK ASSESSMENT WORKSHEET

Risk Assessment Matrix		Probability *(expected frequency)*				
		Frequent: Continuous, regular, or inevitable occurrences	**Likely:** Several or numerous occurrences	**Occasional:** Sporadic or intermittent occurrences	**Seldom:** Infrequent occurrences	**Unlikely:** Possible occurrences but improbable
Severity *(expected consequence)*		A	B	C	D	E
Catastrophic: *Death, unacceptable loss or damage, mission failure, or unit readiness eliminated*	I	EH	EH	H	H	M
Critical: *Severe injury, illness, loss, or damage; significantly degraded unit readiness or mission capability*	II	EH	H	H	M	L
Moderate: *Minor injury, illness, loss, or damage; somewhat degraded unit readiness or mission capability*	III	H	M	M	L	L
Negligible: *Minimal injury, loss, or damage; little or no impact to unit readiness or mission capability*	IV	M	L	L	L	L

Legend:
EH – extremely high risk **H** – high risk **M** – medium risk **L** – low risk

13. RISK ASSESSMENT REVIEW *(Required when assessment applies to ongoing operations or activities)*

a. Date	b. Last Name	c. Rank/Grade	d. Duty Title/Position	e. Signature of Reviewer

14. FEEDBACK AND LESSONS LEARNED

15. ADDITIONAL COMMENTS OR REMARKS

DD FORM 2977, JAN 2014 Page ____ of ____ Pages

Appendix C: Draft Testing Application

Note: any place where “[Insert]” is seen is to be filled out by installation stakeholder overseeing the AV testing operations *prior* to a prospective testing entity completing the form.

AUTONOMOUS VEHICLE TECHNOLOGY TESTING RESERVATION APPLICATION

This document and associated supplementary material comprise an application to reserve testing facilities at Fort Leonard Wood. Applications must be submitted and approved **prior** to the use of the testing facility. Applications must be completed by manufacturers themselves or entity responsible for development of technology for manufacturer. Upon approval, [Insert] will administer reservation to test vehicles with SAE autonomy levels 3 through 5.

Fees for processing and requirements are as follows:
[Insert]
Vehicles restricted from testing on this facility include:
[Insert]
For questions or concerns regarding the required submission please contact:
[Insert]

I. Tester Information

Organization Type: ☐ Manufacturer or ☐ Other (please describe) __________
Name of Manufacturer or Associated Entity:
Address:
City: State: Zip Code: Telephone Number:
Mailing Address:
City: State: Zip Code:

II. Vehicles Equipped for Testing

Please list all applicable vehicles. If a vehicle is not listed, it will not be registered with (insert) as a vehicle authorized for testing. All vehicles must be owned by the entity identified above.
Number of Vehicles in Fleet:
License Plate Number:
State Issued:
VIN number:
Year: Make: Model:
SAE International Level of Automation:
Has the autonomous technology on this vehicle been tested previously? ☐ Yes ☐ No
To what capacity? (i.e. virtual simulation, on-road, off-road, etc.) ________________________
License Plate Number:
State Issued:
VIN number:
Year: Make: Model:
SAE International Level of Automation:
Has the autonomous technology on this vehicle been tested previously? ☐ Yes ☐ No
To what capacity? (i.e., virtual simulation, on-road, off-road, etc.) ________________________

License Plate Number:
State Issued:
VIN number:
Year: Make: Model:
SAE International Level of Automation:
Has the autonomous technology on this vehicle been tested previously? ☐ Yes ☐ No
To what capacity? (i.e., virtual simulation, on-road, off-road, etc.) __________________________

III. Safety Operator Information

The entity certifies that each operator shall be adequately trained to ensure safe and legal operation. Please list all applicable employees, contractors, and designees.
Operator Name:
Driver License Number:
Date of Birth:
Training Completion Date:
Operator Name:
Driver License Number:
Date of Birth:
Training Completion Date:
Operator Name:
Driver License Number:
Date of Birth:
Training Completion Date:

IV. Applicant Acknowledgements

I ____________________ as principal agent for ____________________, certify to the best of my ability the following statements to be accurate for each vehicle and safety operator as indicated in the preceding. ***Please initial next to each applicable statement.***

_____ Autonomous vehicle(s) comply with all relevant FMVSS and applicable state stands OR possesses proof of exemption

_____ All designated safety operators have completed accredited autonomous vehicle test driver training (if applicable)

_____ Safety operator (physically inside or remote) is in control of the vehicle or is actively monitoring the operations and is capable of taking control in the event of system failure

_____ Safety operator (physically inside or remote) thoroughly understands the limitations of the vehicle technology

_____ Safety operator (physically inside or remote) is capable of cautiously operating the vehicle in all conditions

_____ Vehicle(s) have a mechanism to engage/disengage autonomous technology that is easily accessible to operator both inside the vehicle *and* remotely

_____ A visual indicator exists inside the vehicle that indicates when autonomous technology is engaged

_____ The AV(s) are equipped with technology to record data before a collision – *in the event of an incident, data shall be made available to the testing facility*

V. Attachments

☐ Testing Plan – *Please describe the following to the best of your ability*

a. Reasons for site testing
b. Proposed timeline for testing (be as specific as possible)
c. Desired training terrain
d. Maneuvers & Functions being tested
e. Operational Design Domain of each designated vehicle

☐ Safety Checklist – *Please provide a thorough account of steps in preparing your vehicle(s) for testing. The checklist should outline both process and system capabilities:*

a. Turn on/ turn off procedure
b. Entrance and exit procedure
c. Emergency stop procedure
d. Camera / LiDAR / Sensor preparation

☐ Detailed description of technology to be utilized during testing **for each vehicle** listed in Section II (i.e., sensors, autonomy kit, etc.)

☐ Applicant's Safety Assessment – *in accordance with NHTSA's vehicle performance guidance*

☐ Summary of previous experience with AV testing (if applicable) – *this includes:*

a. History of business regarding AVs
b. Summary of simulation software and or virtual testing and results (if applicable)
c. Summary of off road and on road testing (miles/hours completed, vehicle types, SAE levels, ODDs tested, etc. & results (if applicable)
d. Summary of any previous crash incidents in on or off road testing (damage, injuries, fatalities, was official report filed, etc.)

☐ Photocopies of license(s) of the safety operator(s)

☐ Summary of training provided to designated safety operators listed in Section II

☐ Law Enforcement Interaction Plan – *Please describe the following to the best of your ability; the purpose is to inform law enforcement and first respondents how to safely interact with the autonomous test vehicle in the event of an emergency*

a. Operational Design Domains intended to operate in
b. How to safely immobilize, disable, and tow vehicle in event of crash situations
c. How to recognize if vehicle is being operated in autonomous mode
d. How to disengage autonomous mode in event test operator is unable
e. Any additional safety concerns during operation, crash incident, or autonomous system failure (include those that may impact law enforcement or safety professions)

☐ Proof of Insurance – *Attach a copy of the declarations page relative to an insurance policy, or certificate of self-insurance for* ***each*** *vehicle listed in section II*

VI. Signature / Certification

I certify that I am authorized to make this application on behalf of the above-named entity and that all information is complete and true. I agree and understand that any misstatement in the preceding material may result in the reservation not being issued or delayed. The entity agrees to comply with all terms and conditions set forth herein. I understand the [Insert] may revoke the entity's authority to test vehicles with autonomous technology on the site if there is a failure to comply with terms and conditions set forth, or upon an occurrence that warrants concern of safety as determined by the [Insert].

Entity name:____
Principal Agent, (sign):____
Print Name: ____
Title: ____ Date: _____/______/______

OFFICE USE ONLY
The above entity is approved to test and demonstrate the autonomous vehicles designated in this application. **Approval Date:** _____/_____/_____ ____ (insert associated name here)

__NOTE:__ The contents of this technical note are not to be used for advertising, publication, or promotional purposes. Citation of trade names does not constitute an official endorsement or approval of the use of such products.