

WHITE PAPER

Knowing When Workers Are Present



Why trusted worker-presence records should become a standard work-zone practice

Work zones are dynamic environments. Traffic patterns change, lanes open and close, equipment moves, protective devices are repositioned, and crews enter and leave throughout the day. The level of risk can change dramatically within minutes.

Yet many transportation agencies cannot answer one seemingly simple question with precision:

Exactly when were workers present in the work zone?

In many cases, the answer must be reconstructed after the fact from daily reports, shift schedules, supervisor notes, contractor records, text messages, equipment activity, or personal recollection. These sources may provide useful context, but they were not always designed to establish a precise and independently verifiable timeline.

For routine project administration, that limitation may seem manageable. After a serious crash, a work-zone intrusion, an enforcement challenge, or a claim, it can become a significant problem.

A trusted worker-presence log gives a department of transportation an objective record of when people were working within or near an active roadway environment. It can help agencies improve real-time safety operations, administer contracts, support enforcement, investigate incidents, evaluate exposure, and demonstrate that work-zone procedures were followed.

The concept is straightforward. The operational value is much broader than it first appears.



After a serious crash, a work-zone intrusion, an enforcement challenge, or a claim, it can become a significant problem.

Worker presence is an important work-zone condition

A work zone may exist on paper or remain physically established even when no workers are present. Signs may be installed, barriers may remain in place, lanes may be shifted, and temporary pavement markings may continue to guide traffic. In other situations, crews may enter an area for a short-duration activity while traffic patterns remain largely unchanged.

These different conditions do not create the same level or type of risk.

When workers are present, the consequences of excessive speed, driver distraction, an errant vehicle, or an incorrect traffic movement can become much more severe. Worker presence may also trigger operational requirements such as special warning displays, reduced speeds, enforcement activity, protective vehicles, flagging operations, or additional monitoring.

A reliable presence log allows an agency to distinguish among several important states:

- A work zone exists, but no workers are present.
- Workers are present behind positive protection.
- Workers are present on a shoulder or within a closed lane.
- Workers are operating close to live traffic.
- Workers or inspectors are temporarily entering or leaving the zone.
- The agency cannot currently confirm whether workers are present.

That distinction matters. A system that treats every established work zone as identical may produce misleading safety information, inaccurate exposure measurements, or enforcement records that do not reflect actual field conditions.

A system that treats every established work zone as identical may produce misleading safety information and other issues.



The value becomes clear after an incident

Consider a crash that occurs within the limits of a long-term construction project. The temporary traffic-control plan has been in place for several weeks. The crash happens at 9:47 p.m.

Investigators may need to determine whether workers were present at that moment. If they were, additional questions follow:

Were they actively working? Where were they located? Were they behind a barrier? Had a lane closure recently been installed or removed? Were warning devices operating? Was a work vehicle entering or leaving the site? Had the crew already ended its shift?

Without an automated record, the timeline may depend on a combination of timecards, foreman statements, inspection notes, camera footage, radio traffic, and personal device records. Even when everyone is acting in good faith, memories may differ and recorded times may not align.

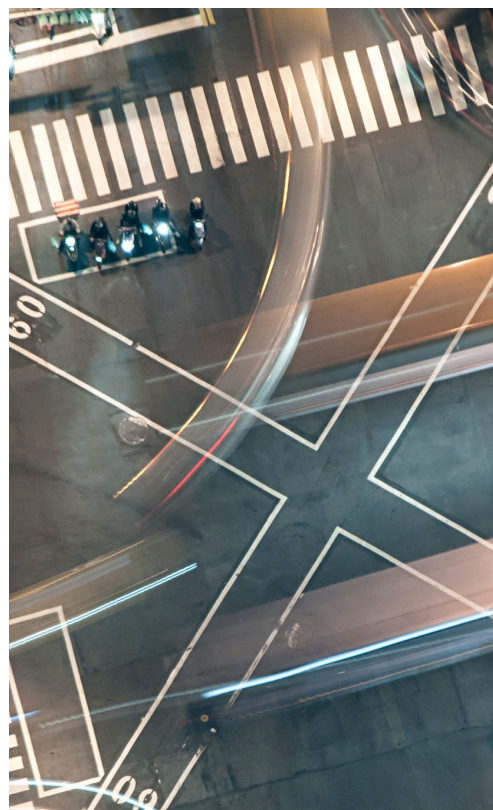
A trusted presence log cannot answer every question about the incident. It can, however, establish a reliable foundation. It may show when worker presence was first confirmed, when it was last observed, what work-zone boundary was in effect, how the presence determination was made, and whether any system exception occurred.

That foundation can make every other part of the investigation more effective.

The same information can support:

- Crash reconstruction
- Internal safety reviews
- Insurance and claims analysis
- Workers' compensation matters
- Contractor-performance reviews
- Citation or enforcement proceedings
- Responses to public-records requests
- Legal discovery
- Corrective-action planning

A strong record is not valuable because it automatically favors the agency. It is valuable because it helps establish what actually occurred.



Worker-presence logging is also a preventive safety tool

The value of presence detection should not be limited to post-incident reporting. Its greatest benefit may come from using worker status in real time.

When worker presence changes from unoccupied to occupied, that event can be shared with other systems. Depending on agency policy and local authority, it may be used to update a traffic-management center, activate a warning display, notify approaching vehicles, enable a lower speed indication, begin an enforcement period, or alert a supervisor that a crew has entered an active area.

When the last worker leaves, the same systems can be updated again.

This creates an opportunity to replace manual processes that depend on someone making a phone call, operating a switch, changing a message board, or remembering to notify a control center.

Manual processes remain essential in many work zones, but they are vulnerable to delay and inconsistency. A presence log creates a digital operating state that can be shared across the work-zone ecosystem.

For example, worker presence could be correlated with:

- Arrow board status
- Lane-closure status
- Flashing warning beacons
- Variable speed-limit displays
- Automated enforcement equipment
- Truck-mounted attenuator deployment
- Traffic-management center notifications
- Connected-vehicle warning services
- Vehicle-speed and trajectory data
- Work-zone intrusion sensors

This does not mean that worker presence alone should control every system. It means that presence can become one trusted input in a larger operational decision.



Enforcement programs need a defensible timeline

In some jurisdictions, enhanced work-zone penalties, reduced speed conditions, or automated enforcement depend on whether workers are present, whether actual work is underway, or whether a legally defined active work-zone condition exists.

These requirements vary by state. The exact definition of “workers present” may also vary. Some laws may focus on workers physically within the roadway. Others may include workers adjacent to traffic, inside work vehicles, behind barriers, or performing activities elsewhere within the project limits.

For this reason, a presence-logging program should begin with a clear legal and operational definition.

The agency should be able to explain:

- **Who counts as a worker**
- **What geographic area counts as the relevant work zone**
- **Whether inspectors, law-enforcement officers, utility personnel, and subcontractors are included**
- **Whether a person inside a vehicle counts as present**
- **Whether workers behind concrete barrier count**
- **Whether workers must be actively performing work**
- **What other signs, lights, or devices must be operating**
- **Who is authorized to activate or confirm the condition**
- **What evidence is needed to support a citation or enhanced penalty**

A trustworthy presence log can help establish the authorized time window, but it should be connected to the other conditions required by law. If a warning beacon, regulatory sign, or enforcement camera must also be active, those records should be time-correlated.

The most defensible enforcement record is not a single data point. It is a consistent timeline showing that all required conditions were met.

A better measure of worker exposure

Transportation agencies often track work-zone crashes, injuries, intrusions, speeding events, and complaints. These measures are important, but raw counts do not always provide a fair comparison.

A project with workers present for 20,000 hours creates a different exposure profile than a maintenance operation lasting two hours. A work zone adjacent to high-speed traffic presents different conditions than a fully separated site. Night work creates different visibility and driver-behavior challenges than daytime work.

Worker-presence logs create an exposure denominator.

With reliable presence intervals, an agency can begin evaluating measures such as:

- Crashes per 1,000 worker-hours
- Intrusions per worker-hour
- Near misses during occupied periods
- Speeding events while workers are present
- Exposure hours adjacent to live traffic
- Exposure with and without positive protection
- Exposure by contractor, project type, or roadway class
- Exposure during nighttime or adverse weather
- Changes in risk after a safety countermeasure is introduced

Worker-presence logs create an exposure denominator.



This can improve investment decisions. Instead of asking only how many incidents occurred, the agency can ask how frequently incidents occurred relative to the amount and type of worker exposure.

That distinction can reveal trends that would otherwise remain hidden.

A contractor with more reported incidents may actually have a lower incident rate after exposure is considered. A safety treatment that appears expensive may prove highly effective when evaluated against worker-hours protected. A particular type of mobile operation may emerge as a greater risk than a larger construction project.

A trustworthy presence log turns worker exposure into measurable operational data.

Contractor and subcontractor accountability

Most DOT work-zone programs depend heavily on contractors and subcontractors. This creates an additional challenge: the agency needs consistent information across organizations that may use different internal systems, staffing processes, and reporting methods.

Worker-presence logging can become a common project requirement.

The DOT can define the standard, while contractors remain responsible for enrolling their personnel, assigning approved devices or credentials, training users, reviewing exceptions, and ensuring that subcontractors comply.

A contract specification might require that designated personnel participate in the worker-presence system during particular activities. It might also require supervisors to review daily summaries, report device failures, document manual overrides, and certify exceptions.

The goal should not be to create an unnecessary administrative burden. The goal is to establish a consistent record across the project.

A practical program should be:

- Simple enough for field personnel to use
- Applicable to both DOT employees and contractors
- Scalable from small maintenance operations to major projects
- Capable of handling temporary and short-duration work
- Clear about who is responsible for compliance

- Flexible enough to address device or network failures
- Protective of worker privacy
- Auditable when a significant event occurs

The easier the system is to deploy and enforce, the more likely it is to become part of normal work-zone practice rather than a special process used only on high-profile projects.

Trust and integrity matter more than the format of the report

A polished report is useful, but the appearance of a report does not make its contents trustworthy.

The strength of a worker-presence record depends on how the underlying data was created, protected, retained, and verified.

A high-integrity record should answer several questions:

- What device or system created the record?
- Was that device authorized?
- When was the event recorded?
- How accurate was the time source?
- Where was the device located?
- What work-zone boundary was active?
- Could the message have been changed after it was created?
- Can the agency verify its origin?
- Were there gaps, outages, or conflicting observations?
- Can the result be reproduced from the original records?



Digital signatures are particularly valuable in this context.

A digital signature is generated using a private cryptographic key controlled by the originating device or system. The corresponding verification process can determine whether the signed information has changed and whether it was signed using a recognized credential.

If a timestamp, location, work-zone identifier, or other protected field is modified after the message is signed, signature verification will fail.

This creates a strong link from the final report to the source data. A reviewer can move from the summarized presence interval to the underlying records and then verify the original digital signatures.

The signature does not prove every real-world fact by itself. It does not automatically prove that a phone was carried by a particular person, that a positioning sensor was perfectly accurate, or that every worker participated in the system. Those issues must be addressed through enrollment, operating procedures, field validation, and transparent report language.

What the signature does provide is a high level of confidence that a retained message came from the credentialed source and has not been altered since it was signed.

Integrity and Completeness Are Different Requirements

It is important to distinguish record integrity from record completeness.

A valid digital signature can demonstrate that an individual record has not been modified. It does not, by itself, prove that every required record was retained or that no record was deleted.

For that reason, agencies still need normal records-management practices. These may include retention schedules, backups, access controls, system monitoring, export procedures, and legal holds.

These controls do not need to be unnecessarily complex. They simply need to ensure that records remain available and that gaps can be identified.

A strong program should be able to distinguish among:

- Confirmed worker presence
- Confirmed worker absence
- Probable presence
- Unknown status
- Device unavailable
- Network unavailable
- Location quality insufficient
- Manual confirmation
- Manual override

An “unknown” status is often more trustworthy than an unsupported claim that no workers were present.

If a system loses communication at 2:15 p.m., it should not automatically report that all workers left at that time. It should show when presence was last confirmed, when communication was lost, and when reliable observations resumed.

Transparency about uncertainty strengthens the record.

Time Accuracy Is Essential

Worker-presence records are often correlated with other systems. These may include police reports, enforcement cameras, traffic sensors, message signs, lane-closure records, video systems, vehicle data, and contractor logs.

If system clocks are not synchronized, an otherwise useful record may become difficult to interpret.

A reliable program should use a controlled time source and store time in a consistent format. Coordinated Universal Time, or UTC, is typically the best canonical value. Local time can also be displayed for field users, but the underlying record should preserve the UTC time and local offset.

The record should also document relevant timing quality, including:

- Device event time
- Server receipt time
- Time source
- Last successful synchronization
- Estimated clock offset
- Maximum expected uncertainty
- Periods of clock or synchronization failure

This may appear highly technical, but its practical purpose is simple: an agency should be able to compare records from multiple systems and understand whether events occurred seconds apart or several minutes apart.

Location and Boundary Quality Must Be Managed

Worker-presence detection normally depends on a geographic boundary. That boundary may represent an entire project, an active closure, a protected work area, or a smaller enforcement zone.

A trustworthy report should identify which boundary was used and which version was active at the time.

Work zones change frequently. Lanes are shifted, closures are moved, phases change, and temporary operations may extend beyond the original limits. If the digital boundary is not updated, the presence result may be technically accurate but operationally misleading.

The agency should define:

- Who can create or modify a boundary
- Who must approve a change
- When a new version becomes effective
- How prior versions are retained

- How boundary changes are communicated
- How temporary or mobile operations are handled

Location accuracy also varies. Smartphones, wearables, vehicles, and roadside sensors may perform differently depending on terrain, buildings, foliage, tunnels, weather, and satellite visibility.

The system should use reasonable thresholds and avoid presenting location estimates as more precise than they are.

For example, a worker near the edge of a boundary may move in and out of the zone because of normal positioning variation. The system may need entry and exit rules, minimum observation periods, or a small buffer to avoid generating repeated false transitions.

These rules should be documented and consistently applied.

Identity, Authorization, and Privacy

Worker-presence logging is most trustworthy when the system can establish that the source was authorized to represent a worker on the project.

This does not mean that every operational report must identify every person by name.

A privacy-conscious program can separate authorization from routine reporting. The system may confirm that an approved worker credential was present without displaying the individual's identity in a daily summary.



A privacy-conscious program can separate authorization from routine reporting.

More detailed identity information may be restricted to authorized users and accessed only for a safety investigation, contract issue, legal requirement, or other approved purpose.

Agencies should also avoid turning work-zone safety technology into unrestricted employee tracking.

Appropriate protections may include:

- Limiting collection to active work zones
- Limiting collection to work hours
- Disabling presence reporting outside the project area
- Reporting aggregate presence when individual identity is unnecessary
- Restricting access to identity mappings
- Establishing clear retention periods
- Informing workers about what is collected and why
- Auditing access to sensitive records

A program that is transparent and narrowly focused on safety is more likely to earn acceptance from workers, contractors, and labor representatives.

Corroboration Strengthens High-Stakes Uses

For many operational purposes, a single authorized mobile-device observation may provide sufficient evidence that one or more workers were present.

Higher-stakes uses may justify corroboration.

An agency may combine presence records with:

- Supervisor check-in
- Wearable-device status
- Contractor roster

- Maintenance-vehicle location
- Arrow board or attenuator status
- Camera or roadside sensor observation
- Work-order activity
- Traffic-management center confirmation
- Sign or beacon activation records

The appropriate level of corroboration depends on the consequence of the decision.

A real-time driver warning may need rapid, automated detection. A criminal or civil enforcement action may require a more complete evidentiary package. A routine exposure report may use aggregated presence intervals. A major crash investigation may require the underlying signed records, device authorization history, boundary version, time-quality information, and system exception logs.

The program should support these different needs without making routine operations unnecessarily difficult.

The Report Should Communicate Facts, Not Overstate Conclusions

A good worker-presence report should be understandable to a project manager, investigator, attorney, contractor, and technical reviewer.

It should explain what was observed, how it was observed, and what limitations applied.

A useful report may include:

- Agency, project, and contract identifiers
- Roadway and jurisdiction
- Work-zone boundary and version
- Presence start and end times
- UTC and local time

- Number of authorized worker devices observed
- Detection method
- Confidence or quality indicator
- Relevant traffic-control status
- System outages or exceptions
- Manual confirmations or overrides
- Digital-signature verification status
- References to the underlying records

The report should use careful language.

"An authorized worker device was detected inside the work-zone boundary" is a specific technical conclusion.

"One or more authorized workers were present" may be a reasonable operational conclusion when enrollment and device-assignment procedures are strong.

"Workers were exposed to live traffic" is a different conclusion that may require lane geometry, barrier status, or other contextual information.

"The legal workers-present condition was satisfied" may require additional statutory elements.

Clear language protects the credibility of the program.

The report should explain what was observed, how it was observed, and what limitations applied.



Building a Program That Can Be Trusted

A DOT does not need to deploy a statewide system all at once.

A focused pilot can establish value and identify the operating rules needed for broader adoption.

The agency should begin by selecting a clear use case. Good candidates include worker-exposure measurement, contractor compliance, automated warning activation, incident reporting, or support for an enforcement program.

The pilot should include a mix of field conditions. A long-term project, a short-duration maintenance activity, a nighttime closure, and a contractor-operated work zone may reveal different operational needs.

During the pilot, the agency should compare the recorded presence intervals with direct field observation. It should intentionally test difficult scenarios:

- A device left in a truck
- A worker without a functioning device
- Poor satellite reception
- Lost cellular connectivity
- A worker near the boundary
- A shift change
- A temporary boundary modification
- A device assigned to the wrong user
- A manual override
- A communication outage during an incident

The objective is not merely to show that the technology works under ideal conditions. The objective is to understand how it behaves when field conditions are imperfect.

A successful pilot should produce more than a demonstration. It should produce a repeatable operating model, including:

- A definition of worker presence
- Enrollment and authorization procedures
- Boundary-management procedures
- Contractor requirements
- Exception-handling rules
- Privacy controls
- Report formats
- Retention requirements
- Validation results
- Training materials
- Responsibilities for system administration

A Call to Action for Work-Zone Leaders

Worker-presence information is too important to remain an assumption.

DOT employees responsible for work zones should begin asking several questions:

1. **Can we determine precisely when workers were present on a project?**
2. **Can we distinguish between occupied and unoccupied periods?**
3. **Can we correlate worker presence with signs, lane closures, enforcement systems, and traffic conditions?**
4. **Can we verify that the underlying records were not altered?**
5. **Can we identify gaps and uncertainty rather than hiding them?**
6. **Can contractors and subcontractors comply without specialized or burdensome equipment?**
7. **Can we use the information to measure worker exposure and improve future projects?**

If the answer to these questions is no, the agency has an opportunity to strengthen both safety and accountability.

The first step does not need to be a major procurement. It can begin with a cross-functional discussion involving work-zone operations, construction, maintenance, traffic engineering, legal counsel, records management, information technology, safety personnel, contractors, and law enforcement.

That group can identify the most valuable initial use case and define what a trustworthy record should mean for the agency.

The next step is a field pilot with measurable objectives.

The final step is to convert the lessons learned into standard practice—through policies, contract language, reporting procedures, and integration with the systems that already manage work-zone operations.

Conclusion

A work-zone program is strongest when it can accurately describe not only where a work zone was established, but also when workers were actually present and exposed to roadway risk.

A trusted worker-presence log can support real-time warnings, contract oversight, enforcement, crash investigation, claims analysis, performance measurement, and long-term safety improvement.

The value depends on more than collecting location data. The record must have a clear operational meaning, a reliable time source, an approved work-zone boundary, authorized data sources, transparent exception handling, appropriate privacy controls, and a verifiable connection to the underlying evidence.

Digitally signed records can provide a high level of integrity by making later alteration detectable and by linking each message to an authorized source. Combined with sound records management and field procedures, they can create an evidence trail that is substantially stronger than a manually reconstructed timeline.

For DOT work-zone leaders, the call to action is clear:

Make worker presence a defined, measurable, and trustworthy work-zone operating condition.

Doing so will help agencies protect workers, improve decisions, strengthen accountability, and better understand when and where work-zone risk is truly present.

About TrafficAuth

TrafficAuth, powered by OmniTrust, secures connected mobility and traffic management networks by establishing trusted identity, authentication, and authorization across vehicles, devices, and traffic systems. Built on the OmniTrust Trust Lifecycle Management platform, TrafficAuth enables verifiable, enforceable trust for the full lifecycle of safety critical traffic infrastructure equipment. Global customers rely on TrafficAuth to secure large-scale networks, including connected vehicles, roadside infrastructure, and sensor networks, ensuring trusted communication, authenticated access, and lifecycle governance across millions of devices. TrafficAuth combines hardware-rooted identity, scalable PKI infrastructure, and policy-driven lifecycle enforcement to support safety-critical transportation, smart infrastructure, and regulated mobility environments. Learn more at trafficauth.com.