APPENDIX MATERIAL

for

NCHRP Legal Research Digest 71: Liability of Transportation Entity for the Unintentional Release of Secure Data or the Intentional Release of Monitoring Data on Movements or Activities of the Public

Appendix A: Project Survey Questions, A1–6
Appendix B: Summary of Survey Responses, B1–27
Appendix C: Copies of Policies, Procedures, Regulations, and Contracts on the Collection of Secure Data and Monitoring Data, C1–108
Appendix D: List of Transportation Agencies Responding to the Survey, D1
APPENDIX A

SURVEY QUESTIONS

NCHRP 20-6, Study Topic 21-04, LIABILITY OF TRANSPORTATION ENTITY FOR THE UNINTENTIONAL RELEASE OF SECURE DATA OR THE INTENTIONAL RELEASE OF MONITORING DATA ON MOVEMENTS OR ACTIVITIES OF THE PUBLIC

Agency Name: ____________________________________________

Name of Employee: ____________________________________________

Job Title: ____________________________________________

Contact telephone/ cell phone number: _____________________________

Email address: ____________________________________________

Educational Background: ____________________________________________

Legal Training: YES NO (If “yes” describe)

How many years have you been with the agency? ____________________________

******************************************************

Note: The Report to be prepared for the above topic will focus on two issues: a transportation agency’s liability for the (1) unintentional release of data on motorists, employees, or other individuals that the agency is required to keep secure as required by law and/or agency regulations or policies, hereinafter referred to as “secure data,” and for the (2) intentional release of data collected by monitoring the movements and activities of the traveling public, hereinafter referred to as “monitoring data.”

(If insufficient space is allotted for your responses below, please feel free to place your responses on additional sheets of paper and attach them to the survey.)

1. Does your agency collect and/or maintain:

   (a) Secure data (please circle) YES NO
   (b) Monitoring data (please circle) YES NO

IF YOUR ANSWER IS “YES” TO QUESTION 1(a) AND/OR (b), PLEASE ANSWER THE FOLLOWING QUESTIONS.
2. (a) If your answer to question 1(a) is “Yes”, please describe the kinds of secure data that your agency collects and/or maintains.

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

(b) If your answer to question 1(b) is “Yes”, please describe the kinds of monitoring data that your agency collects and/or maintains.

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

3. Does your agency participate in and/or use Intelligent Transportation Systems (ITS) and/or other methods to collect data? (please circle) YES NO
   If your answer is “YES”, please identify the methods used, the type of data collected, and the purpose or purposes for which the agency uses the data.

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

4. Are there laws, either state or federal, that authorize your agency to collect and/or maintain:
   (a) secure data? (please circle) YES NO
      If your answer is “Yes”, please provide a citation or citations.

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

(b) monitoring data (please circle) YES NO
   If your answer is “Yes”, please provide a citation or citations.

______________________________________________________________________________

______________________________________________________________________________

______________________________________________________________________________

5. Are there any federal laws that limit or prohibit your agency’s collection of data, such as by a certain method or by a certain category of data? (please circle) YES NO
   If your answer is “Yes”, please provide a citation or citations.

______________________________________________________________________________
6. Are there any state laws that limit or prohibit your agency’s collection of data, such as by a certain method or by a certain category of data?  
(please circle) YES NO  
If your answer is “Yes”, please provide a citation or citations.

7. Has your state promulgated any regulations that apply to your agency’s collection or maintenance of:
   (a) secure data?  
      (please circle) YES NO  
      If your answer is “Yes”, please provide a citation or link to the regulations.

   (b) monitoring data?  
      (please circle) YES NO  
      If your answer is “Yes”, please provide a citation or link to the regulations.

8. Does your state have any constitutional or statutory provisions on the privacy or confidentiality of personal data or information in connection with your agency’s collection or maintenance of secure data?  
(please circle) YES NO  
If your answer is “YES”, please provide citations.

9. Does your state have any constitutional or statutory provisions on the privacy or confidentiality of personal data or information in connection with your agency’s collection or maintenance of monitoring data?  
(please circle) YES NO  
If your answer is “YES”, please provide citations.

10. Has your agency adopted any policies that govern your agency’s collection and/or maintenance of:
    (a) secure data?  
        (please circle) YES NO  
        If your answer is “Yes”, please provide a copy of or a link to the policies or procedures.

    (b) monitoring data?  
        (please circle) YES NO  
        If your answer is “Yes”, please provide a copy of or a link to the policies or procedures.
11. Has your agency adopted any procedures that govern your agency’s collection and/or maintenance of:
   (a) secure data? (please circle) YES  NO
   If your answer is “Yes”, please provide a copy of or a link to the policies or procedures.

12. Are there any laws and/or regulations in your state that provide an individual with a cause of action against your agency for the disclosure of:
   (a) secure data? (please circle) YES  NO
   If your answer is “Yes”, please provide a citation to the laws or regulations.

13. Does your agency have immunity under state law (e.g., because of sovereign immunity and/or a provision of a tort claims or governmental immunity act) from claims against your agency for:
   (a) a negligent release or disclosure of data in general or of secure or monitoring data? (please circle) YES  NO
   If your answer is “YES”, please provide citations to applicable statutes and cases.

14. Pursuant to a request made under a Freedom of Information Act or other public records disclosure law has your agency been required to disclose:
   (a) secure data? (please circle) YES  NO
If your answer is “YES”, please provide details regarding the request, the person or entity making the request, whether the data was produced or was not produced for one or more reasons.

______________________________________________________________________________

______________________________________________________________________________

(b) monitoring data? (please circle) YES NO
If your answer is “YES”, please provide details regarding the request, the person or entity making the request, whether the data was produced or was not produced for one or more reasons.

______________________________________________________________________________

______________________________________________________________________________

15. Has your agency received either a discovery request and/or been served with a subpoena for:
   (a) secure data? (please circle) YES NO
   If your answer is “YES”, please provide details regarding the discovery request or subpoena and whether the agency had to comply with the request or subpoena.

______________________________________________________________________________

(b) monitoring data? (please circle) YES NO
If your answer is “YES”, please provide details regarding the discovery request or subpoena and whether the agency had to comply with the request or subpoena.

______________________________________________________________________________

16. Please state whether in the previous five (5) years your agency been sued for a negligent or intentional release or disclosure of:
   (a) secure data? (please circle) YES NO
   (b) monitoring data? (please circle) YES NO
   If your answer is “YES”, please provide details and a citation to any judicial decisions.

______________________________________________________________________________

17. Are there any agreements between the United States Department of Transportation or division thereof and your agency regarding the privacy of information collected by your agency? (please circle) YES NO
If your answer is “YES”, please a link to or a copy of such an agreement.
18. Are there any proposed state law or regulatory changes in your state that could affect your agency’s collection of secure or monitoring data?  
(please circle) YES  NO  
If your answer is “YES”, please provide details.  
______________________________________________________________________________ 
_________

19. Does your agency have contracts with persons or private entities to collect secure or monitoring data?  
(please circle) YES  NO  
If your answer is “YES”, please provide a link to any contracts or copies with your responses to the survey.  
______________________________________________________________________________ 
_________

20. Please include any additional information that you would like to provide that is relevant to the study topic and/or to the survey.  
______________________________________________________________________________ 
_________

******************************************************************************

* Please return your completed survey to:

The Thomas Law Firm  
ATTN: Larry W. Thomas, J.D. Ph.D.  
888 Sixteenth Street, N.W., Suite 800  
Washington, D.C. 20006  
Tel. (202) 248-5402  

E-mail: lwthomas@cox.net
APPENDIX B—SUMMARY OF TRANSPORTATION DEPARTMENTS’ RESPONSES TO THE SURVEY

Seventeen transportation departments, which are identified in Appendix D, responded to the survey conducted for the digest.

1(a). Question 1(a) asked whether the agencies collect or maintain secure data. Fourteen departments reported that they collect or maintain secure data, whereas two departments stated that they do not.

1(b). Question 1(b) asked whether the agencies collect or maintain monitoring data. Thirteen transportation departments reported collecting or maintaining monitoring data, whereas three departments said that they are not doing so.

2(a). For those agencies collecting secure data, question 2(a) requested the agencies to describe the kinds of secure data that they collect and/or maintain.

The Alabama DOT stated that it collected and maintained only employment records. The Arkansas DOT reported having some “protected information,” such as names, addresses, and Social Security numbers that are stored in its Right-of-Way Division. Its Legal Division also maintains similar protected information. The Traffic Safety Division has protected information in connection with the Arkansas State Police and accident reports that include names, addresses, and ages of individuals who were involved in accidents.

The Arizona DOT defined secure data to include information such as Social Security numbers, driver’s license numbers, credit card numbers, financial account data, tax information, and health information.

The Florida DOT’s approach was to identify data that are confidential and exempt from disclosure, including data having, containing, or revealing:

1. The official cost estimate of a proposed project;

2. The identity of persons who have requested or obtained bid packages, plans or specifications pertaining to any project;

3. Financial statements provided by prospective bidders;

---

749 Alabama DOT, Arkansas DOT, Arizona DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

750 District of Columbia DOT and Maine DOT.

751 Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Ohio DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

752 Maine DOT, Montana DOT, and North Dakota DOT.
4. The department’s Bid Analysis and Monitoring System’s documentation, input, computer processes and programs, electronic data files, and output;

5. Information on a contractor’s equipment, past record, experience, financial resources, and personnel;

6. Sealed bids or proposals;

7. Public records prepared by, or at the express direction of, an agency attorney that reflect mental impressions, conclusions, litigation strategy or legal theory of the attorney or agency and that were prepared exclusively for civil or criminal litigation or adversarial administrative proceedings or in anticipation of such proceedings;

8. Security planning pursuant to the Security of Data and Information Resources Management Act;

9. Claim files of the Division of Risk Management, Department of Insurance;

10. Certain personnel records, including Social Security numbers, medical records, and personal information of employees and their families;

11. Complaints and other records relating to complaints or charges of employment discrimination;

12. Plans, blueprints, schematic drawings, and diagrams that depict the internal layout and structural elements of a building or other structure owned or operated by an agency;

13. Records that relate directly to the physical security of a facility or security system plans or portions thereof held by an agency;

14. Appraisals and other reports relating to values and offers and counteroffers in reference to eminent domain matters or proceedings;

15. Bank account numbers and debit, charge, and credit card numbers;

16. Any information that is a trade secret;

17. Certain information and investigatory records of the Inspector General related to active investigations;

18. Crash reports that reveal personal information on the parties who were involved;

19. Personally identifiable information (PII) provided to, acquired by, or in the possession of the Department, a county, or expressway authority for the purpose of using a credit card, charge card, or check for prepayment of electronic toll facilities charges;
20. Questions and answer sheets of examinations administered for the purpose of licensure, certification, or employment; and

21. Toll tag information and license plates.

The Indiana DOT identified secure data to include employee Social Security numbers, medical history and data, personnel and disciplinary records, and protected health information.

The City of Minneapolis–Public Works Department identified names, addresses, and credit card information as its secure data.

The Missouri Highway and Transportation Department (MoDOT) identified crash data and data on employees, including Social Security number, date of birth, medical information, home address, and other information in personnel files.

The Montana DOT identified “sensitive/secure data” as including:
Drug testing information; driver’s records; criminal background checks; Voluntary Employee Benefit Association (VEBA) data; Americans with Disabilities Act records; disciplinary process records, including recommendations for discipline, grievances, settlements, agreements, and disciplinary letters; the FMLA process, including medical notes; the Worker’s Compensation process, including first report of injury, correspondence of the Montana State Fund, medical notes, and early return to work status; recruitment files and folders; personnel files, including performance reviews, training records, I-9 citizenship forms, EEO forms; Social Security numbers; date of birth; credit and debit cards statements; tax returns and W-9s; payments to vendors that include FEIN and Social Security numbers; payroll records; disability medical information; crash reports, including name, Social Security number, date of birth, date of death, tax identification number, and medical information; non-FMLA medical invoices with Social Security numbers and FEINs, financial information, and bank account information; MDT property damage reports, including full name, address, driver’s Social Security number, date of birth, driver’s license numbers, telephone number, age, gender, type of damage, and type of injury (if any); license plate surveys; and MioVision cameras for vehicle classification, traffic volumes, and turning movements (being neither secure nor sensitive).

The North Dakota DOT’s response was that owner information, driver’s license number, and driver’s records are regarded as secure data.

Although not responding directly to the survey question, the Ohio DOT reported that ORC § 149.43 describes data that are secure or confidential data and data that are monitoring data that are generally available to the public. The DOT provided a link to an Executive Order prohibiting executive agencies’ use of off-shore data-services. The department advised that

753 See Executive Order 2011-12K, Governing the Expenditure of Public Funds for Offshore Services, ¶ 1 (2011), available at: http://www.governor.ohio.gov/Portals/0/pdf/executiveOrders/EO%20211-12K.pdf (last accessed November 4, 2015). The Executive Order applies to services in respect to data and states: “No State Cabinet Agency, Board or Commission (‘Executive Agency’) shall enter into any contract which uses any public funds within its control to purchase services which will be provided outside the United States.” The Executive Order applies to all purchases of services
the Ohio Department of Administrative Services (ODAS) has retention schedules that
government entities must follow.754

The Ohio DOT noted also that a “document could contain ‘secure’ data or ‘monitoring’
data as described in [the] questionnaire and could be retained or disposed of in many different
ways subject to the [ODAS] retention schedules.”

The Oklahoma DOT reported that it collects and/or maintains contractor-financial
information, accident information, employee personnel information, and litigation-privileged
information.

The Oregon DOT identified PII, such as bank accounts, credit card accounts, dates of
birth, driver’s license numbers, and tax information. The DOT also collects personal information
on employees as required by the IRS and the Oregon Department of Revenue, the Public
Benefits Board, and the Public Employee Retirement System.

The Oregon DOT also reported that the DMV collects driver’s license or identity card
numbers and telephone numbers, as well as customer information that is considered more secure
than the PII listed above, such as Social Security numbers, photographs, medical information,
and biometric data used to compare DMV photographs during the issuance process.

The Rhode Island DOT has crash data.

The South Carolina DOT identified human rights data, risk management data, and credit
card data.

The Utah DOT identified tolling data associated with the Express Lanes system,
Bluetooth data associated with the reporting of travel times, license plate recognition associated
with commercial vehicle operations, and data collected from law enforcement crash reports.

2(b). For those agencies collecting monitoring data, question 2(b) requested the
agencies to describe the kinds of monitoring data that they collect and/or maintain.

The Alabama DOT stated that it collects and maintains traffic counts and vehicle
speed/traffic flow data.

The Arkansas DOT reported that its research division on occasion will conduct traffic
surveys and obtain motor vehicle data and the license plate numbers of drivers to monitor entry
into and exit from study areas. The DOT noted that the Arkansas Highway Police is
implementing a license plate reader system to allow for simplified review of information on
commercial motor vehicles.

The Arizona DOT defined monitoring data to include information such as Intelligent
Transportation System (ITS) information (e.g., vehicle occupancy, speed, and volume) and
traffic accident information (e.g., location, passengers, and vehicles).

The Washington, D.C. Department of Transportation (District of Columbia DOT)
advised that it collects crash information from the Metropolitan Police Department. The District
DOT’s Traffic Operations Administration collects information on traffic signal locations and

made directly by an Executive Agency and to services provided by subcontractors of those
providing services purchased by an Executive Agency. Id. at ¶¶ 1 and 3(a)(ii)(3).

754 See Ohio General Retention Schedules, available at:
http://apps.das.ohio.gov/rims/General/General.asp (last accessed November 4, 2015). For example, all
bidding documents, requests for proposals or for qualifications or similar documents for sales of goods
are retained for 5 years and for services for 16 years and then destroyed.
configuration, traffic calming devices, streetlights, and parking meters. The District DOT reported that for security purposes the monitoring data are not shared with the public.

The Florida DOT stated that traffic detectors are utilized to collect data on traffic speed, traffic volume, and traffic occupancy for traffic management purposes. For more details, the DOT provided links to an overview of FDOT’s ITS and Central Data Warehouse.

The Indiana DOT stated that it reads Wi-Fi and Bluetooth MAC addresses along interstate routes but that the addresses are “immediately truncated to remove personal information.” The data are then stored for use to calculate travel times. The DOT advised that no personal data are stored. Transponders are used to collect data for toll roads in Indiana, but the information is collected by a private operator.

The City of Minneapolis—Public Works Department reported having a video of movement throughout the City-maintained portions of the Skyway System.

MoDOT reported that it collects standard traffic data in various locations throughout the state; that the vast majority of the data is collected in the Metropolitan areas of St. Louis and Kansas City; and that the data are generally collected via physical detectors along the roadway, such as inductive loops in the pavement or roadside radar units. The data collected include vehicle volumes, vehicle speeds, vehicle classification, and roadway occupancy. The department also collects traffic count and turning movement information at intersections throughout the state. The counts may be collected manually by staff in the field or may be captured using video that is processed later.

MoDOT also monitors traffic using closed-circuit television (CCTV) cameras. Video captured by the cameras is not recorded or stored but is used for the purpose of monitoring live traffic conditions. Video streams are monitored by the state’s Transportation Management Centers and also shared with the public via MoDOT’s website and mobile application.

MoDOT stated that it recently entered into a contract with a company (HERE North America, LLC (HERE)) to receive a live traffic data feed for thousands of roadway miles in Missouri; that the data are collected, processed, and distributed solely by HERE; and that MoDOT is simply a recipient of the data. The data received by MoDOT include the average speed and travel time for pre-defined roadway segments at approximately 60 second intervals. The MoDOT stated that the data have allowed MoDOT to monitor live traffic conditions on thousands of miles of roadways without the need for instrumentation as used in St. Louis and Kansas City.

The Montana DOT referred to its answer to question 2(a).

The Ohio DOT did not respond directly to the question but commented that the department has “video feed facilities across the state that monitor highways” with data being

---


756 Florida DOT, Traffic Engineering and Operations Office, Central Data Warehouse, available at: http://www.dot.state.fl.us/trafficoperations/ITS/RITIS.shtm (last accessed November 4, 2015). The website explains that the DOT “utilizes a wealth of data to help fulfill their traffic operations mission” but that the challenge has been to find a way to make the data available to other users; thus, “a ‘one-stop shop’ for all of Florida’s traffic data has always been part of the Intelligent Transportation Systems Program’s vision.”
The Oregon DOT identified weigh-in-motion data, license plate reader data, and transponder (Green Light) data.

The South Carolina DOT reported having traffic accident reports, vehicle miles traveled (used also to determine vehicle speed), vehicle counts, and toll information, including violations.

The Utah DOT identified real-time images from CCTV cameras (with no recording). The DOT assumes that data such as speed and volume do not come within the category of monitoring data because the data are not attributable to an individual, either in collection or dissemination.

3. **Question 3 asked whether the agencies participate in and/or use Intelligent Transportation Systems (ITS) and/or other methods to collect data.** Although the Arkansas DOT and Maine DOT reported that they do not, fourteen transportation departments reported that they do so.758

The Alabama DOT noted the use of GPS, cameras, and speed monitors.

The Arizona DOT stated that the department uses ITS methods to collect data and that road sensors are used to collect vehicle occupancy (timing), speed, and volume information. The data are used to calculate traffic congestion and speed information.

The District of Columbia DOT reported that it uses approximately 130 sensors in the roadway that monitor the volume of traffic and the number of cars on a road at any particular time. CCTV is used to monitor traffic activity at intersections. The DOT also uses digital sign message boards to alert the public about upcoming traffic and estimated travel time.

The District of Columbia DOT described a subscription that it has to INRIX, which provides a variety of Internet services and mobile applications pertaining to road traffic and driver services. INRIX provides businesses and individuals with historical, real-time traffic information, traffic forecasts, travel times, travel time polygons, and traffic counts. INRIX collects trillions of bytes of information about roadway speeds from over 185 million real-time anonymous mobile phones, connected cars, trucks, delivery vans, and other fleet vehicles equipped with GPS locator devices.

The Florida DOT stated that traffic detectors are utilized to collect data on traffic speed, traffic volume, and traffic occupancy for purposes of traffic management. For more details, the DOT provided a link to an overview of FDOT’s ITS759 and Central Data Warehouse.760

The Indiana DOT referred to its response to question 2(b).

The City of Minneapolis – Public Works Department’s response referred to the detection of vehicles.


758 Alabama DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Ohio DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

759 See Appendix B, n.7.

760 See Appendix B, n.8.
The MoDOT stated that the methods used and the data collected are as stated in response to question 2. The MoDOT uses the data to provide real-time traveler information to the public via the department’s website and mobile application. The data are used also to provide drivers with travel time and delay information on MoDOT’s dynamic message signs (DMS). The data are used to populate performance measures, identify traffic trends, and prioritize the projects on which to focus its limited resources. The data are used as well to provide real-time alerts to staff and customers related to traffic slowdowns, backups, incidents, work zones, or other emergencies. Vehicle counts and vehicle classifications are used to monitor roadway capacity, intersection demand, and traffic patterns. The MoDOT stated that the information helps the department make better decisions related to traffic control, lane usage, the need for capacity, and proposed changes in traffic patterns. The data are helpful also in identifying ideal detour routes to bypass work zones, incidents, or traffic congestion. CCTV cameras are used to monitor live traffic conditions and weather conditions.

The Montana DOT collects RWIS data that include surface and air temperature, precipitation, and wind data for the purpose of evaluating road conditions.

The Oklahoma DOT stated that its ITS uses vehicle detectors to monitor speeds at numerous points along the Interstate system to assist the department and inform the public.

The Oregon DOT identified weigh-in-motion data; transponder (Green Light) data; video data to monitor road conditions; traffic monitoring data; detect/respond to incidents data; MAC addresses (“cryptographically hashed”) via Bluetooth to calculate travel times for system performance monitoring and traveler information; loops/radar sensors/video detection to gather traffic data for planning and operational purposes; and weather data for road condition monitoring, winter maintenance decision-making, and traveler information.

The South Carolina DOT identified traffic volumes, delay, and incident response reports (including location, vehicle type, license tag information, and type of assistance provided).

The Utah DOT stated that it uses radar, inductive loops and video detection to operate traffic signals and to collect speed and volume data; Bluetooth data to generate travel times; and CCTV images to monitor traffic flow and incidents (not recorded and only used in real-time).

4(a). Question 4(a) asked the agencies whether there are laws, either state or federal, that authorize the agency to collect and/or maintain secure data.

Nine departments said there are, whereas five stated that there are not. The departments provided the following additional information:

The Alabama DOT stated that it collects and maintains only employment records and referred to 23 U.S.C. § 409 (2015). The Arizona DOT stated that it uses ITS methods to

---

761 Alabama DOT, Arizona DOT, Florida DOT, Indiana DOT, MoDOT, North Dakota DOT, Oregon DOT, South Carolina DOT, and Utah DOT.

762 Arkansas DOT, City of Minneapolis–Public Works Dept., Montana DOT, Oklahoma DOT, and Rhode Island DOT.

763 Section 409 prohibits the discovery of or the use as evidence of any reports, surveys, schedules, lists, or data compiled or collected for the purpose of identifying evaluating, or planning the safety enhancement of potential accident sites, hazardous roadway conditions, or railway-highway crossings, pursuant to sections 130, 144, and 148 of this title [23 USCS §§ 130, 144, and 148] or for the
collect data and that road sensors are used to collect vehicle occupancy, speed, and volume information.

The Florida DOT identified laws authorizing the collection and maintenance of data: Fla. Stat. § 334.044(20) (2015) (authorizes the department to conduct research studies and to collect data necessary for the improvement of the state transportation system); Fla. Stat. § 334.063 (2015) (mandates that the department shall include in the criteria for the planning, construction, and maintenance of the State Highway System statistical studies of accidents and fatalities as well as traffic count); and Fla. Stat. § 339.177 (2015) (requires the department, in conjunction with metropolitan planning organizations, to develop a state traffic congestion management system).

The Florida DOT also noted the Safe, Accountable, Flexible, Efficient Transportation Equity Act: A Legacy for Users (SAFETEA-LU, 2005), a transportation reauthorization bill that identified reductions in the number of crashes and associated fatalities and injuries as the basis for judging the effectiveness of highway safety programs under the Highway Safety Improvement Program (HSIP). The determination of effectiveness is contingent on each state having good quality traffic safety data and using that data to determine the location, severity, and changes in their traffic safety problems.


The South Carolina DOT identified S.C. Code, title 8, chapter 11 (applicable to state officers and employees).

The Utah DOT identified 23 U.S.C. § 112 (2015) (letting of contracts) and Utah Code § 63G-6a-505 (2015) (“Information submitted to or by a governmental entity in response to a request for information is protected under Section 63 G-2-305.”).

4(b). Question 4(b) asked the agencies whether there are laws, either state or federal, that authorize the agency to collect and/or maintain monitoring data.

Nine departments responding to the survey said that there are, but six departments said that there are not.

The departments reporting that there are such laws provided additional information.

The Arkansas DOT identified Ark. Code Ann. § 12-12-1803(b)(4) (2015) (stating that an automatic license plate reader (APLR) may be used by the Arkansas Highway Police for the electronic verification of registration, logs, and other compliance data and that an APLR “shall be installed at an entrance ramp at a weigh station facility for the review of a commercial motor vehicle entering the facility”).

The Arizona DOT identified the Arizona Revised Statutes, title 28 (Transportation).

The District of Columbia DOT stated that the District of Columbia Municipal Regulations (DCMR) in 1 DCMR § 1502 (2015) govern “agency records management programs.” In addition, D.C. Code §§ 50-921.03 and 50-921.04 (2015) give the department authority to collect information necessary for various agency functions.

MoDOT stated that there are no laws that specifically authorize the collection of monitoring data but that the authority is implicit in the department’s powers to operate its system efficiently.

The Oklahoma DOT referred to the federal regulations in 23 C.F.R. part 511 (2015) that establish “the provisions and parameters for the Real-Time System Management Information Program.”

The South Carolina DOT identified S.C. Code, title 57, chapter 3 (Department of Transportation).


5. Question 5 asked whether there are federal laws that limit or prohibit the agency’s collection of data, such as by a certain method or by a certain category of data.

---

764 Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Oklahoma DOT, Oregon DOT, South Carolina DOT, and Utah DOT.

765 Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, and Rhode Island DOT.

766 The Alabama DOT stated that there are various federal and state statutes and regulations without identifying them more particularly. The Florida DOT, Oregon DODT, and Indiana DOT referred to their response to question 4(a).
Although six departments said that there are,\textsuperscript{767} nine departments stated that there are no federal laws that limit or prohibit their collection of data, such as by a certain method or by a certain category of data.\textsuperscript{768}

The Alabama DOT identified HIPPA as a federal law that “limits access.”

The Florida DOT identified the Privacy Act of 1974 but also stated:

The federal government has not adopted a set of privacy policies for ITS applications. Both the Federal Highway Administration (FHWA) and the National Highway Traffic Safety Administration (NHTSA), however, have authored reports on connected (automated) vehicles that outline design goals related to privacy. Neither agency references formal laws or regulations in these reports.


The South Carolina DOT referred to the federal Privacy Act, 5 USCS § 552a, \emph{et seq.} (2015) and to the FTC’s Fair Information Practice Principles (FIIPs). The response also noted the Payment Card Industry Data Security Standard (PCI DSS) that applies to the data collected and stored for such cards and payments.

6. \textbf{Question 6 asked whether there are state laws that limit or prohibit the agency’s collection of data, such as by a certain method or by a certain category of data.}

Three departments said that there are state laws that limit or prohibit the department’s collection of data,\textsuperscript{769} such as by a certain method or by a certain category of data, but most departments reported there are none in their state.\textsuperscript{770}


MoDOT cited Mo. Rev. Stat. § 32.091 (2015) (definitions, disclosure of individual motor vehicle records, disclosures prohibited without express consent, disclosure pursuant to United States law, disclosure for purposes of public safety, and certain information not to be collected).

The Florida DOT identified Fla. Stat. § 334.044(20) (2015) that authorizes the department to conduct research studies and collect data necessary for the improvement of the state transportation system.

7(a). \textbf{Question 7(a) asked whether an agency’s state has promulgated any regulations that apply to the agency’s collection or maintenance of secure data.}

\begin{itemize}
\item \textsuperscript{767} Alabama DOT, Arkansas DOT, Florida DOT, Indiana DOT, MoDOT, and South Carolina DOT.
\item \textsuperscript{768} Arizona DOT, District of Columbia DOT, City of Minneapolis–Public Works Dept., Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, and Utah DOT.
\item \textsuperscript{769} Arkansas DOT, MoDOT, and Florida DOT.
\item \textsuperscript{770} Alabama DOT, Arizona DOT, District of Columbia DOT, Indiana DOT, City of Minneapolis–Public Works Dept., Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.
\end{itemize}
Seven departments reported that there are such regulations, whereas seven departments said there are none presently.


The Florida DOT referred to the general records retention schedule GS1-SL and to Fla. Stat. § 119.021 (2015) regarding custodial requirements and the maintenance, preservation, and retention of public records. The department stated that “Florida law regarding record/data maintenance and retention has broad-base application across state agencies.”

MoDOT stated that 7 Missouri Code of State Regulations (CSR) § 10-1.010 (2015) provides that the Commission’s Secretary is responsible for maintaining all records, documents, and papers filed with the Commission and the department, including secure data.

The Montana DOT cited to Mont. Code Ann. § 2-17-505(4)(b) (2015) that states in part that the mitigation of risks is a priority in order to protect individual privacy and acknowledges that “the liabilities stemming from the risk to information technology … have increased.”

The North Dakota DOT referred to N.D. Century Code, ch. 39-33 (Driver and Motor Vehicle Record Privacy).

The Oregon DOT identified ORS § 825.517 (2015) and Oregon Administrative Rules §§ 735-010-0000 to 735-010-0250 (2015) that apply to available motor vehicle records, fees for records, and the authorization needed to obtain records.


7(b). Question 7(b) asked whether an agency’s state has promulgated any regulations that apply to the agency’s collection or maintenance of monitoring data, and, if so, to provide a citation or link to the regulations.

---

771 Arizona DOT, Florida DOT, MoDOT, Montana DOT, North Dakota DOT, Oregon DOT, and South Carolina DOT.

772 Alabama DOT, Arkansas DOT, Indiana DOT, City of Minneapolis–Public Works Dept., Oklahoma DOT, Rhode Island DOT, and Utah DOT.


Four departments reported that their states have promulgated regulations that apply to the department’s collection or maintenance of monitoring data;\textsuperscript{775} eleven departments reported there are no such regulations presently in their state.\textsuperscript{776}


8. **Question 8 asked whether an agency’s state has any constitutional or statutory provisions on the privacy or confidentiality of personal data or information in connection with the agency’s collection or maintenance of secure data, and, if so, to provide citations.**

Ten departments stated that they have such constitutional or statutory provisions,\textsuperscript{777} whereas only four departments reported that they do not have such provisions.\textsuperscript{778}


The Arizona DOT identified the Drivers Privacy Protection Act (18 U.S.C. § 2721, et seq. (2015)).

The Florida DOT referred to the Florida Constitution, art. I, § 23 and the Florida Statutes, ch. 119 (2015), but stated that there are numerous exemptions to the obligation of state entities to provide public records upon request, including for confidential and exempt personal data and information.\textsuperscript{779}

The department also noted that Fla. Stat. § 501.171 (2015) includes provisions on the confidentiality of personal information.

The Indiana DOT identified Ind. Code § 4-1-6 (2015) (compliance with IC 4-1-10-3 by removing or obscuring numbers from records); Ind. Code § 4-1-10 (2015) (negligent disclosure and infraction); Ind. Code § 5-14-3 (2015) (access to public records); and Ind. Code § 8-23-2-6(c)(2) (2015) (Indiana DOT, powers of the department, and confidential information).

\textsuperscript{775} District of Columbia DOT, Florida DOT, MoDOT, and South Carolina DOT. The Florida DOT, MoDOT, and South Carolina DOT referred to their response to question 7(a).

\textsuperscript{776} Alabama DOT, Arkansas DOT, Arizona DOT, Indiana DOT, City of Minneapolis–Public Works Dept., Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, and Utah DOT.

\textsuperscript{777} Arkansas DOT, Arizona DOT, Florida DOT, Indiana DOT, MoDOT, Montana DOT, North Dakota DOT, Oregon DOT, South Carolina DOT, and Utah DOT.

\textsuperscript{778} Alabama DOT, City of Minneapolis–Public Works Dept., Oklahoma DOT, and Rhode Island DOT. The response of the City of Minneapolis–Public Works Department referred to “[p]ublic data information.”

\textsuperscript{779} See, e.g., FLA. STAT. § 119.071(l)(3)(1) (2015) (providing in respect to security that “[b]uilding plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout or structural elements…held by an agency are exempt” from disclosure).

The Montana DOT cited Mont. Code Ann. § 2-17-505(4)(a) (2015) regarding principles for the development of “statewide information technology policies, standards, procedures, and guidelines applicable to all state agencies and other entities using the state network.”


9. Question 9 asked whether an agency’s state has any constitutional or statutory provisions on the privacy or confidentiality of personal data or information in connection with the agency’s collection or maintenance of monitoring data, and, if so, to provide citations.

Departments responding from four states stated that there are constitutional or statutory provisions regarding the privacy or confidentiality of personal data or information in connection with the department’s collection or maintenance of monitoring data. On the other hand, departments from ten states advised that there are no such provisions applicable to their collection or maintenance of monitoring data.


The Florida DOT identified the Florida Constitution, art. I, § 23; Fla. Stat., ch. 119 (2015) that contains numerous exemptions to the obligation of state entities to provide public records upon request, including confidential and exempt personal data and information; Fla. Stat. § 501.171 (2015) that has provisions for the confidentiality of personal information; and Fla. Stat. §§338.155(6) (2015) that is applicable to PII collected by the DOT, a county, a municipality, or an expressway authority for the purpose of paying, prepaying, or collecting tolls and associated administrative charges for the use of toll facilities.


---

780 Arkansas DOT, Florida DOT, South Carolina DOT, and Utah DOT.

781 Alabama DOT, Arizona DOT, District of Columbia DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, and Rhode Island DOT.
10(a). **Question 10(a) asked whether an agency has adopted any policies that govern the agency's collection and/or maintenance of secure data, and, if so, to provide a copy thereof.**

Nine departments reported that they have adopted policies that govern their department’s collection and/or maintenance of secure data, whereas six departments have not done so. The Arizona DOT said that the department adheres to Statewide Policy 8410 on system privacy, the purpose of which “is to provide more detailed guidance for the development of a system privacy notice based on standards, regulations, and best practices.”

The Florida DOT referred to its Security and Use of Information Technology Resources, effective December 5, 2012, as well as to the confidential information policy for My Florida Market Place, a source for centralized procurement activities that streamlines interactions between vendors and state government entities.

The Indiana DOT referred to the policies adopted by State Personnel and the State Auditor.

The City of Minneapolis–Public Works Department referred to the PCI Security Standards that apply to payment card data security.

---

782 Arizona DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oregon DOT, Rhode Island DOT, and South Carolina DOT. Montana DOT did not respond to question 10(a).

783 Alabama DOT, Arkansas DOT, District of Columbia DOT, City of Minneapolis–Public Works Dept., Oklahoma DOT, and Utah DOT.


785 Florida DOT, Policy, Security and Use of Information Technology Resources, http://www.dot.state.fl.us/computersecurity/PDF/Information%20Technology%20Resource%20Security.pdf (last accessed November 4, 2015). DOT’s policy is “to treat information and information technology resources as strategic assets and to protect those assets from misuse, abuse, and loss through the management of a comprehensive information technology resources security program.” Id. at ¶ 1. Paragraph 2.4 requires that “[c]onfidential data or confidential information must be encrypted before being transmitted over a network.”


787 PCI Security Standards Council, PCI SSC Data Security Standards Overview, available at: https://www.pcisecuritystandards.org/security_standards/index.php (last accessed November 4, 2015). As noted on its Web site, the Council provides the PIN Transaction Security (PTS) requirements that contain a single set of requirements for all personal identification number (PIN) terminals, including POS devices,
MoDOT referred to its Open Records Policy (revised April 1, 2015) that begins with the following statements:

It is the policy of the Missouri Department of Transportation (MoDOT) to comply with the provisions of Chapter 610 of the Revised Statutes of Missouri (RSMo), as amended, the Missouri Public Records (Sunshine) law. MoDOT recognizes that it is the public policy of the State of Missouri that all meetings, records, etc., of public governmental bodies are open to public inspection except those that the statutes allow to be closed (Section 610.021 RSMo). MoDOT also recognizes that the law regarding access to such meetings and records is to be liberally construed.

This policy is adopted by MoDOT pursuant to Section 610.028.2 RSMo, as amended. MoDOT has appointed the Secretary to the Commission as the custodian of such records as required by Section 610.023, as amended.

MoDOT hereby adopts and implements this Public Records Policy and Procedure to respond to requests for access to such records. The adoption of this policy and procedure repeals and replaces all earlier policies and/or procedures.

The Oregon DOT provided a copy of the Oregon Transportation Commission Data Privacy Policy, as well as of a copy of its DMV policies. See Appendix C.4 to the Report.

The South Carolina DOT provided a link to an overview of the South Carolina Department of Administration’s Division of Technology.

10(b). Question 10(b) asked whether an agency has adopted any policies that govern the agency’s collection and/or maintenance of monitoring data, and, if so, to provide a copy thereof.

Ten departments stated that they have adopted policies that govern their department’s collection and/or maintenance of monitoring data. Five departments reported having no such policies.

encrypting PIN pads, and unattended payment terminals. PCI Standards and Documents are available at: https://www.pcisecuritystandards.org/security_standards/documents.php (last accessed November 4, 2015).

788 South Carolina Department of Administration, Division of Technology, available at: http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx#Information%20Security%20Policies (last accessed November 4, 2015). The technology division facilitates the “delivery of technology, security and privacy-related services and solutions to governmental entities throughout the state.” Id. at: http://www.admin.sc.gov/technology/about (last accessed November 4, 2015). The Division of Information Security is “responsible for a variety of statewide policies, standards, programs and services relating to cyber security and information systems.” Id. at: http://www.admin.sc.gov/technology/information-security (last accessed November 4, 2015).

789 Arizona DOT, Florida DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, and South Carolina DOT.

790 Alabama DOT, Arkansas DOT, District of Columbia DOT, Indiana DOT, and Utah DOT.
The departments having policies reported as follows:

The Arizona DOT identified Statewide Policy 8410.791

The Florida DOT referred to FHWA’s Traffic Monitoring Guide (TMG). 792 The TMG is “the most up to date guidance to State highway agencies in the policies, standards, procedures, and equipment typically used in a traffic monitoring program.” 793 The DOT also referred to federal regulations applicable to the Real-Time System Management Information Program794 and to transportation funding for ITS authorized by the Moving Ahead for Progress in the 21st Century Act, P. L. 112-141 (2012) (MAP-21).795

The City of Minneapolis-Public Works Department referred to the PCI Security Standards that apply to payment card data security.796

MoDOT provided a link to a description of its use of ITS.797 The department also provided a link to frequently asked questions on video cameras at signalized intersections.798

791 See Appendix B, footnote 36.


795 See FHWA, Moving Ahead for Progress in the 21st Century (MAP-21), A Summary of Highway Provisions, available at: http://www.fhwa.dot.gov/map21/summaryinfo.cfm (last accessed November 4, 2015). The summary explains, for example, that the Highway Safety Improvement Program (HSIP) remains USDOT’s number one priority. The HSIP emphasizes a data-driven, strategic approach for which the foundation is a safety data system that each state must have.

796 See Appendix B, n.39.

The North Dakota DOT provided a link to its privacy and security policy. 799

The Oklahoma DOT stated that there are no written policies or procedures for the data collected and that the current CCTV camera system does not record or archive data.

The Oregon DOT provided a copy of the Oregon Transportation Commission Data Privacy Policy and a copy of its Policy ADM 08-01 on passive electronic data collection. See Appendix C. 4 to the Report.

The South Carolina DOT provided a link to an overview of the South Carolina Department of Administration, Division of Technology. 800

11(a). Question 11(a) asked whether an agency has adopted any procedures that govern the agency’s collection and/or maintenance of secure data, and, if so, to provide a copy thereof.

Nine departments reported that they have adopted procedures, 801 in contrast to five departments that have not done so. 802

The Arizona DOT reported that agency business units maintain internal procedures relative to secure data collection.

The Florida DOT provided a link to information on its collection of crash data and its procedures governing the release of such data. 803 The DOT also provided a link to the state’s Distribution of Exempt Documents Concerning Department Structures and Confidential and Exempt Security System Plans. 804

The City of Minneapolis–Public Works Department referred to the PCI Security Standards that apply to payment card data security. 805

---


800 See Appendix B, n.40.

801 Arizona DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Indiana DOT referred to its response to question 10(a). The Montana DOT and Oklahoma DOT referred to their responses to question 10(b).

802 Alabama DOT, Arkansas DOT, North Dakota DOT, and Oklahoma DOT.


805 See Appendix B, n.39.
The Oregon DOT said that the “DMV has hundreds of employees in various work units that deal with secure data on a daily basis. There are numerous procedures which in many cases describe internal security measures … [that] are not shared externally.”

The South Carolina DOT provided a link to an overview of the South Carolina Department of Administration, Division of Technology.806

The Utah DOT provided a copy of its requirements for the handling of Bluetooth data.

11(b). Question 11(b) asked whether an agency has adopted any procedures that govern the agency’s collection and/or maintenance of monitoring data, and, if so, to provide a copy thereof.

Eleven departments reported that they have adopted procedures,807 but three departments stated that they have not.808

The Arizona DOT stated that agency business units maintain internal procedures relative to monitoring data collection.

The District of Columbia DOT said that individual offices within the agency have retention policies for records.

The Florida DOT referred to FHWA’s Traffic Monitoring Guide (TMG).809

The City of Minneapolis–Public Works Department referred to the PCI Security Standards that apply to payment card data security.

MoDOT referred to its response to question 10(b) concerning its use of CCTV cameras.

The North Dakota DOT provided a link to its privacy and security policy.

The Rhode Island DOT advised that all vendors doing business with the DOT have to adhere to its privacy policies.

The South Carolina DOT stated that “[w]hen SCDOT monitoring data contains PII, it is collected and protected in the same manner as secure data” and provided a link to an overview of the South Carolina Department of Administration, Division of Technology.812

The Utah DOT provided a copy of its procedures for the use of CCTV camera images. See Appendix C.5 to the Report.

806 See Appendix B, n.40.

807 Arizona DOT, District of Columbia DOT, Florida DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Oklahoma DOT referred to its response to question 10(b).

808 Alabama DOT, Arkansas DOT, Indiana DOT. The Montana DOT did not respond to question 11(b).

809 See Appendix B, n.44.

810 See Appendix B, n.39.


812 See Appendix B, n.40.
12(a). **Question 12(a)** inquired whether there are any laws and/or regulations in an agency’s state that provide an individual with a cause of action against the agency for the disclosure of secure data, and, if so, to provide a copy of the laws or regulations.

Nine departments advised that there are laws and/or regulations in their state that provide an individual with a cause of action against the department for the disclosure of secure data. 813 Seven departments stated that there are no such laws or regulations in their state. 814


The District of Columbia DOT stated that “1 DCMR §1500 states in part that individuals that misuse or destroy public records are subject to penalty.”


The Oregon DOT identified ORS § 802.191 (2015). Subsection (1) provides that “[a] person aggrieved by an intentional violation of ORS 802.175 to 802.187 may bring an action at law against a person who has knowingly obtained or used personal information about the aggrieved person in violation of ORS 802.175 to 802.187. The action shall be for actual damages or $2,500, whichever is greater, plus attorney fees and court costs reasonably incurred in the action.”

The South Carolina DOT referred to S.C. Code § 39-1-90 (2015) that requires that a notification be given whenever there is a breach of the security of data and authorizes a cause of action for actual damages caused by a breach. 815

12(b). **Question 12(b)** inquired whether there are any laws and/or regulations in an agency’s state that provide an individual with a cause of action against the agency for the disclosure of monitoring data, and, if so, to provide a copy of the laws or regulations.

---

813 Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Florida DOT, North Dakota DOT, Oregon DOT, South Carolina DOT, and Utah DOT. The North Dakota DOT stated “risk management” in response to the question. The Utah DOT attached a copy of its requirements for the handling of Bluetooth data.

814 Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT (not aware of any); Oklahoma DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Montana DOT’s response was “none known.”

815 Based on the definitions of the terms “person” and “organization” in the statutes, it appears that the data breach statute may apply to governmental units as well as to business entities and natural persons. See S.C. Code Ann. §§ 39-1-90(D)(2) (2015), 37-20-110(10) (2015), and 37-1-301(18) and (20) (2015). S.C. Code § 39-1-90(G)(1) (2015) authorizes a civil action for damages for a willful and knowing violation, but damages are limited to actual damages for a negligent violation of the statute.
Six departments reported that there are laws and/or regulations in their state that provide an individual with a cause of action against the department for the disclosure of monitoring data.\textsuperscript{816} Nine departments reported that there are no such laws or regulations authorizing a cause of action for a disclosure of monitoring data.\textsuperscript{817}


The District of Columbia DOT said that “1 DCMR §1500 states in part that individuals that misuse or destroy public records are subject to penalty.”

The City of Minneapolis–Public Works Department referred to its state’s Data Practices Act and its response to question 14.

The South Carolina DOT, referring to monitoring data that contain PII, referred to S.C. Code § 39-1-90 (2015) (breach of security of business data, notification, definitions, penalties, exception as to certain banks and financial institutions, and notice to the Consumer Protection Division).

The Utah DOT referred to its requirements regarding the use of CCTV camera images.

13(a). \textit{Question 13(a) asked whether the agencies have immunity under state law (e.g., because of sovereign immunity and/or a provision of a tort claims or governmental immunity act) from claims against the agency for a negligent release or disclosure of data in general or of secure or monitoring data, and, if so, to provide citations to applicable statutes and cases.}

Seven departments advised that they have immunity from such a claim;\textsuperscript{818} however, seven departments reported that they do not have immunity.\textsuperscript{819} Some of the departments reporting that they have immunity stated as follows:


The Florida DOT identified Fla. Stat. § 768.28 (2015) (waiver of sovereign immunity in tort actions, recovery limits, limitation on attorney fees, statute of limitations, exclusions, indemnification, and risk management programs).


The Oregon DOT stated that there is an indemnification provision in “Oregon’s Privacy Law for the agency concerning a person who discloses personal information in violation of the

---

\textsuperscript{816} Arkansas DOT, District of Columbia DOT, Florida DOT, City of Minneapolis–Public Works Dept., South Carolina DOT, and Utah DOT. The Florida DOT referred to its response to question 12(a).

\textsuperscript{817} Alabama DOT, Arizona DOT, Indiana DOT, MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, and Utah DOT. The Montana DOT’s response was “none known.”

\textsuperscript{818} Alabama DOT \textit{(citing ALA. CONST. (1901), art. I, § 14); Arkansas DOT, Florida DOT, Indiana DOT \textit{(citing IND. CODE § 34-13-3 (2015)), MoDOT, Oregon DOT, and Rhode Island DOT. Montana DOT’s response was “none known.” The Maine DOT and Ohio DOT did not respond to the question.}

\textsuperscript{819} Arizona DOT, District of Columbia DOT, City of Minneapolis–Public Works Dept., North Dakota DOT, Oklahoma DOT, South Carolina DOT, and Utah DOT. Although the South Carolina DOT answered no to the question, the department referred to the South Carolina Tort Claims Act, tit. 15, Civil Remedies and Procedures, ch. 78. Montana DOT’s response was “none known.” The Maine DOT and Ohio DOT did not respond to the question.
law” and cited ORS § 802.191(3) (2015) (“Any person whose use or obtaining of personal information in violation of ORS 802.175 to 802.187 subjects the State of Oregon to any liability or claim shall indemnify and hold harmless this state from all such liability and any claims, including attorney fees and court costs, incurred in any proceeding arising under ORS 802.175 to 802.187.”)

The Rhode Island DOT stated that a breach must be willful.

13(b). Question 13(b) asked whether the agencies have immunity under state law (e.g., because of sovereign immunity and/or a provision of a tort claims or governmental immunity act) from claims against the agency for an intentional release or disclosure of data in general or of secure or monitoring data, and, if so, to provide citations to applicable statutes and cases.

Five departments reported that they would have immunity; eight departments stated that they would not have immunity.

The Florida DOT stated that its answer was “Yes, if judicially determined that the conduct was committed in ‘bad faith’ or for a ‘malicious purpose.’” The department quoted Fla. Stat. § 768.28(9) (2015):

The state or its subdivisions shall not be liable in tort for the acts or omissions of an officer, employee, or agent committed while acting outside the course and scope of her or his employment or committed in bad faith or with malicious purpose or in a manner exhibiting wanton and willful disregard of human rights, safety, or property.

14(a). Question 14(a) asked whether the agencies have been required to disclose secure data pursuant to a request made under a Freedom of Information Act or other public records disclosure law, and, if so, to provide details regarding the request and the person or entity making the request and to state whether the data were produced or were not produced for one or more reasons.

Four departments said that they have received requests, but nine departments stated that they have not received any requests.

---

820 Alabama DOT (citing ALA. CONST. (1901), art. I, § 14), Arkansas DOT, Florida DOT, MoDOT, and Indiana DOT (citing IND. CODE § 34-13-3 (2015)). The MoDOT referred to its answer to question 13(a).

821 Arizona DOT, District of Columbia DOT, City of Minneapolis–Public Works Dept., North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Montana DOT did not respond to question 13(b). Although the District of Columbia DOT responded in the negative to the question, the department also said “1 DCMR §1500 does not specifically disclose immunity under state law from claims against the agency.” Although the South Carolina DOT also answered no, the DOT referred to the South Carolina Tort Claims Act, tit. 15, Civil Remedies and Procedures, ch. 78.

822 Arkansas DOT, Florida DOT, Indiana DOT, and City of Minneapolis–Public Works Dept. The Indiana DOT said that the details of such requests were not available. The Florida DOT stated that it was not possible to recount or paraphrase the details of the handling and response to each of those requests in response to the question. The Maine DOT and Ohio DOT did not respond to the question.

823 Alabama DOT, Arizona DOT, MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. Montana DOT’s response was “not known.”
The Arkansas DOT reported that under the Arkansas Freedom of Information Act of 1967 it is required to release public information retained or in the custody of the department that is not exempt and that a public record includes, films, tapes, sound tape, and electronic or computer based information or data compilations in any medium.

The City of Minneapolis–Public Works Department reported that “[a] county sheriff requested information on the location of a customer requesting data related to the credit card number he provided. We supplied the times that the person entered the facility and exited.”

Although answering the question in the negative, the Oregon DOT added that unless a requestor is qualified to receive it “Oregon’s Privacy Law (ORS 802.175-802.191) protects personally identifiable customer information from being disclosed unless to the person whose record it refers to or to qualified entities listed in the law for specific purposes.”

14(b). **Question 14(b) asked whether the agencies have been required to disclose monitoring data pursuant to a request made under a Freedom of Information Act or other public records disclosure law, and, if so, to provide details regarding the request and the person or entity making the request and to state whether the data were produced or were not produced for one or more reasons.**

Five departments reported having such requests. Eight departments stated that they have not received any requests.

The Arkansas DOT advised that data are produced with appropriate redactions of information that are not subject to release under Arkansas or federal law.

The District of Columbia DOT stated:
Under the Freedom of Information Act (FOIA) the agency provides information that includes monitoring data (i.e., traffic light synchronicity data, bicycle rental, traffic patterns on city streets, reports of damaged trees on public space, potholes, bridge repairs, and construction, etc.). The requests are submitted by legal offices on behalf of constituents, residents, print and electronic media, and by academic researchers from local and out of state schools and universities.

The City of Minneapolis – Public Works Department stated that it has provided video to various law enforcement agencies requesting such data for investigations and active pursuits.

MoDOT stated that it has received requests only for daily traffic counts.

The Ohio DOT advised in part that the department responds to records requests occasionally regarding federally funded issues and federal partners but does so primarily under the Ohio Public Records laws in Ohio Revised Code, ch. 149.

15(a). **Question 15(a) asked whether the agency has received either a discovery request and/or been served with a subpoena for secure data, and, if so, to provide details**

---

824 Arkansas DOT, Arizona DOT, District of Columbia DOT, City of Minneapolis–Public Works Dept., Florida DOT, Ohio DOT, and MoDOT. The Arizona DOT advised that “[a] public records report that provides request details is not available.” The Florida DOT stated that it was not possible to recount or paraphrase the details of the handling and response to each of those requests in response to the question.

825 Alabama DOT, Indiana DOT (stating that details are not available), North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Montana DOT’s response was “none known.”
Regarding the discovery request or subpoena and to state whether the agency had to comply with the request or subpoena.

Nine departments reported receiving discovery requests and subpoenas for secure data. Two departments reported that they have not received such requests and subpoenas. The Alabama DOT stated that it has received numerous requests for crash data. The Indiana DOT stated that it was not sure about INDOT but that “State Personnel has revealed secure data in litigation cases, subject to protective orders. INDOT also receives requests for the State’s appraisal in condemnation proceedings, which we deny.” MoDOT stated that employee data are “sometimes an issue in employment claims and other litigation.” The department stated that it has received subpoenas from private parties regarding secure employee data which MoDOT will release when the employee (or former employee) provides a waiver via a notarized written request signed and dated by the employee (or former employee) specifically stating the employee’s full name, the last four digits of his/her social security number, what information is to be released, and to whom it is to be released. MoDOT has also received subpoenas from governmental agencies with subpoena power and has released certain secure employee data pursuant to such lawful subpoenas.

The Oklahoma DOT responded affirmatively but stated, “we have no secure data.” The Oregon DOT said that the “Oregon DMV receives approximately 1600 subpoenas per year for records information. However, the subpoena requestor must still qualify under Oregon law to receive secure data. A subpoena by a nonqualified entity is not valid to receive secure data.”

The Rhode Island DOT advised that it receives many requests for video footage but that the department does not maintain such footage.

15(b). Question 15(b) asked whether the agency has received either a discovery request and/or been served with a subpoena for monitoring data, and, if so, to provide details regarding the discovery request or subpoena and to state whether the agency had to comply with the request or subpoena.

Seven departments reported receiving discovery requests and subpoenas for monitoring data. However, five agencies have not received such discovery requests and subpoenas.

---

826 Alabama DOT, Arizona DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, and Rhode Island DOT. The Arizona DOT reported that “[a] public records report that provides request details is not available.” The District of Columbia DOT and the Florida DOT reported that the requested information is not available. Although not responding directly to questions 15(a) or (b) that distinguish between secure data and monitoring data, the Ohio DOT stated that the department responds to public records requests and discovery requests and subpoenas on a daily basis.

827 Arkansas DOT and South Carolina DOT. Montana DOT’s and Utah DOT’s responses were “not known.”

828 Alabama DOT, Arizona DOT, City of Minneapolis–Public Works Dept., MoDOT, Oklahoma DOT, Oregon DOT, and Rhode Island DOT. The Arizona DOT and Florida DOT reported that the information requested is not available.
The Alabama DOT reported that it has received numerous requests for traffic data and non-protected employee records. The Oklahoma DOT answered affirmatively but stated that “we have no archived monitoring data.” The Oregon DOT stated that it receives numerous requests for video data but that it does not keep a record of video data.

16(a). Question 16(a) asked whether in the previous five (5) years an agency has been sued for a negligent or intentional release or disclosure of secure data, and, if so, to provide details and a citation to any judicial decisions. No transportation departments responding to the survey reported having had any claims.830

16(b). Question 16(b) asked whether in the previous five (5) years an agency has been sued for a negligent or intentional release or disclosure of monitoring data, and, if so, to provide details and a citation to any judicial decisions. No transportation departments responding to the survey reported having had any claims.831

17. Question 17 asked whether there are any agreements between the United States Department of Transportation or a division thereof and an agency regarding the privacy of information collected by the agency, and, if so, to provide a copy of any agreements. All departments responding to the survey reported that they do not have an agreement with the United States Department of Transportation or a division thereof regarding the privacy of information collected by the department.832

The Florida DOT added that, although the department complies with all applicable federal laws and regulations regarding the privacy of information collected by the department, there are no separate, individual agreements applicable specifically to the department.

829 Arkansas DOT, District of Columbia DOT, Indiana DOT, North Dakota DOT, and South Carolina DOT. The Montana DOT’s and the Utah DOT’s responses were “not known.” The Maine DOT and Ohio DOT did not respond to the question.

830 Alabama DOT, Arkansas DOT, Arizona DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Maine DOT, Montana DOT, and Ohio DOT did not respond to the question. The District of Columbia DOT and Florida DOT stated that information was not available on any claims made with respect to disclosure of secure data.

831 Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oklahoma DOT, Oregon DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT. The Florida DOT stated that information was not available on any claims made with respect to the disclosure of monitoring data. The Maine DOT, Montana DOT, and Ohio DOT did not respond to the question.

18. **Question 18 asked whether there were proposed state law or regulatory changes in an agency’s state that could affect the agency’s collection of secure or monitoring data, and, if so, to provide details.**

With one exception, the departments responding to the survey reported that there are no proposed changes in state law or regulations that would affect their collection of secure or monitoring data.833

The Oregon DOT reported that the Oregon Legislature was still in session at the time of responding to the survey but there were numerous items of proposed legislation, which the department identified as HB 2919, HB 2356, HB 2596, HB 3142, HB 3154, SB 316, SB 377, SB 514, SB 601, SB 639, SB 640, SB 641, SB 711, and SB 904. The legislature was scheduled to end its session by early July, 2015.

19. **Question 19 asked whether the agencies have contracts with persons or private entities to collect secure or monitoring data, and, if so, to provide copies thereof.**

Nine departments stated that they have such contracts for the collection of secure or monitoring data.834 The other departments reported that they do not have such contracts.

The Arizona DOT provided a copy of a Database Access Agreement. See Appendix C.1 to the Report.

The Florida DOT identified its CCTV AGREEMENT (001013), an ATIS AGREEMENT (Code Pending - 021002) for Third Party Data Feed for Traffic Information, the Florida 511 Travel Information System,835 and WAZE,836 the latter being an “app” that may be downloaded to obtain real-time traffic information.

The Indiana DOT reported that State Personnel has data contracts and that the DOT has contracts with outside appraisers for condemnation proceedings and land acquisitions.

---

833 Alabama DOT, Arkansas DOT, Arizona DOT, District of Columbia DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, Montana DOT, North Dakota DOT, Oklahoma DOT, Rhode Island DOT, South Carolina DOT, and Utah DOT.

834 Arizona DOT, Florida DOT, Indiana DOT, City of Minneapolis–Public Works Dept., MoDOT, North Dakota DOT, Oregon DOT, Rhode Island DOT, and Utah DOT.


the safety and mobility of people and goods, economic competitiveness, and the quality of our environment and communities by serving commuters, tourists, commercial vehicle operators, and evacuees. FL511 is fully bilingual, offering users information in English and Spanish via the phone, text, e-mail, and the FL511.com web site allowing Florida’s diverse population to better receive travel information.


The City of Minneapolis—Public Works Department identified the Ampco System Parking with a sub-contract to ABM Security.

MoDOT reported that it has numerous contracts with private entities for the collection of secure employee data but that it would be overly burdensome for the department to provide copies of the contracts. The MoDOT stated that it has an agreement with HERE for the collection of traffic data pursuant to which HERE collects, analyzes, and distributes the data directly to MoDOT. See Appendix C.3 to the Report.

The North Dakota DOT reported that it has contracts with RL Polk, Experian, Complus Data Innovations, Inc., Dominion Enterprises, Duncan Solutions, and HELP, Inc.

The Oregon DOT stated:
DMV has data brokers that provide the information to other qualified entities. There are Disseminator contracts for records access per ORS 802.179(13). …

ITS does not have current contracts, but has had a previous contract with Inrix to provide travel time data based on probe data. No personally identifiable information is included in this data. An RFP for a new contract is underway.

Although it answered the question in the negative, the South Carolina DOT stated that the department obtains some monitoring data as a member of “The I-95 Corridor Coalition.”837

The Utah DOT identified toll collection with ETCC and Bluetooth data collection with Digiwest. See Appendix C.7 to the Report.

20. Question 20 asked agencies responding to the survey to include any additional information that the agency would like to provide that is relevant to the study topic and/or to the survey.

The District of Columbia DOT stated:
Although this is not directly relevant to the survey, DDOT used NextBus, a vehicle tracking system that uses global positioning satellite information to predict when the next bus will arrive at any given bus stop. The agency replaced NextBus with smart phone data to collect real time bus location. DDOT also adopted the initiative Vision Zero, which is a multi-national road traffic safety project that aims to achieve a highway system with no fatalities or serious injuries in road traffic. The agency monitors oversized and overweight vehicles to track entrance and exits routes from the District, and DDOT offers suggested routes to truck drivers passing thorough and operating within the District.

The Oregon DOT supplied the following additional information:
The majority of DMV records is considered public record and is available by making a request and paying a fee. However, the personally identifiable customer information contained in the record is protected unless a requestor is ordering their own record information or is a qualified entity under Oregon’s Record Privacy Law. (ORS 802.175–802.191). This law is based on the federal Driver Protection Act which requires states to have a version of the federal law. Oregon law is more restrictive than the federal law in certain areas. Likewise, Oregon law

837 Information on the Coalition is available at: http://www.i95coalition.org/ (last accessed November 4, 2015).
already had protections in place for certain sensitive information and limits the access more than federal law requires.

ODOT ITS does not gather or store any data that includes personal information. The monitoring data are not stored or encrypted in a way that recovery of any personal or sensitive information is not possible.

The South Carolina DOT stated that the department is currently implementing security controls and policies dictated by the South Carolina Budge and Control Board for state agencies as ordered by Legislative Proviso 117.132 as part of general provisions of the 2014-2015 Appropriation Act…. The policies that are being implemented are based on controls such as FISMA, FIPS pub 199 & 200, and the NIST 800 series. While these are not laws, but controls for federal information systems, they are the industry standards used for controls and compliance.

The South Carolina DOT provided a link to information technology and information security plans that are required of all state agencies.838

APPENDIX C—COPIES OF POLICIES, PROCEDURES, REGULATIONS, AND CONTRACTS ON THE COLLECTION OF SECURE DATA AND MONITORING DATA

**Arizona DOT**
Database Access Agreement  
**APPENDIX C.1**

**Rhode Island DOT**
Traffic Management Policy for the Design and Operation of Closed-Circuit Television (CCTV) in Advanced Management Systems  
**APPENDIX C.2**

**MoDOT**
Agreement between MoDOT and HERE North America LLC  
**APPENDIX C.3**

**Oregon DOT**
Data Privacy Policy and of Policy ADM 08-01 on Passive Electronic Data Collection  
**APPENDIX C.4**

**Utah DOT**
Traffic Operations Center Control Room, CCTV Etiquette  
**APPENDIX C.5**
Privacy Protection Plan for Bluetooth/Wi-Fi Travel Times  
**APPENDIX C.6**
Agreement between Utah DOT and Digiwest LLC  
**APPENDIX C.7**

LINKS TO POLICIES, PROCEDURES, REGULATIONS, AND CONTRACTS ON THE COLLECTION OF SECURE DATA AND MONITORING DATA

**Federal Highway Administration**

**State Transportation Agency Policies—Secure Data**

**Arizona DOT**

**Florida DOT**


**City of Minneapolis—Public Works Department**

PCI Standards and Documents are accessible at: https://www.pcisecuritystandards.org/security_standards/documents.php (last accessed November 4, 2015).

**South Carolina DOT**

**State Transportation Agency Policies—Monitoring Data**

**Arizona DOT**

**City of Minneapolis—Public Works Department**
PCI Standards and Documents are accessible at: https://www.pcisecuritystandards.org/security_standards/documents.php (last accessed November 4, 2015).

**North Dakota DOT**

**South Carolina DOT**
**State Transportation Department Procedures—Secure Data**

**Florida DOT**


**City of Minneapolis–Public Works Department**

**South Carolina DOT**

**Transportation Department Procedures—Monitoring Data**

**Florida DOT**

**City of Minneapolis–Public Works Department**

**North Dakota DOT**

**South Carolina DOT**
**Transportation Department Regulations—Secure Data or Monitoring Data**

**Arizona DOT**

**Florida DOT**

**South Carolina DOT**

**Contracts for the Collection of Secure Data or Monitoring Data**

**Florida DOT**


APPENDIX C.1

ARIZONA DEPARTMENT OF TRANSPORTATION

DATABASE ACCESS AGREEMENT
DATABASE ACCESS AGREEMENT – Government AZ State

The Department (as defined below) hereby requests authorization for connectivity to the records database(s) of the Arizona Department of Transportation, Motor Vehicle Division (MVD). The Department’s specific access capabilities are set forth and further described in the attached Addendum, which shall be considered a part of this Agreement between the Department and MVD.

The Department understands and agrees that it shall only access MVD’s database(s) in accordance with the terms and conditions set forth herein. If at any time MVD believes the Department is using such access in an unauthorized or unlawful manner, MVD reserves the right, in its sole discretion, to immediately terminate this Agreement.

Definitions

“ADOT” means the Arizona Department of Transportation.

“Arizona @ Your Service Web Portal” or “Portal” means the single entry point through which the Company may access MVD’s database(s) under this Agreement.

“Authorized users” mean those persons who are employed or contracted by the Department to perform the activities authorized hereunder.

“Confidential information” means all information used by and proprietary to MVD which is not generally known by non-MVD personnel. This includes, but is not limited to, the following types of information (whether or not reduced to writing or designated as confidential):

- Viewed or printed information resulting from or related to the access provided under this Agreement;
- All computer software and accompanying documentation (i.e., operating systems, user’s guide, etc.) provided by MVD, its agents, vendors or other contractors;
- MVD’s personnel, financial, marketing and other internal business information, including the manner and method of conducting business;
- MVD’s strategic, operations and other business plans, measurements and forecasts; and
- Information regarding MVD’s employees, electronic data access customers, vendors and other contractors.

“Connectivity” means to make and/or maintain a computer connection with MVD, through the Arizona @ Your Service Web Portal, for the purpose of performing the activities authorized under this Agreement.

“Data Access Security Level” means the level of access privileges granted to the Department’s authorized users to retrieve and/or modify MVD data based upon the Department’s stated eligibility for such data, as provided in Sections II and III of the Agreement Addendum.

“Department” means the government entity identified and referred to in Section I of the Agreement Addendum.
"Encrypted," means the scrambling of computerized information in order to secure data by using special algorithms for transmission or other purposes.

"MVD" means the Arizona Department of Transportation, Motor Vehicle Division.

"Motor Vehicle Record Request System or "MVRRS" means the system used by the Portal provider to facilitate the Department's electronic access to MVD record information through the Arizona @ Your Service Web Portal.

"Personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

"Portal provider" means the private entity to which the State of Arizona has awarded a statewide contract to provide for the transmission of MVD's record information to its pre-approved electronic data access customers via the Portal's MVRRS.

"Secure location" means an area designated specifically for the Department's authorized users to access MVD's database(s) pursuant to this Agreement and to which all unauthorized individuals shall be prohibited from accessing or viewing MVD data. The designated secure location does not necessarily need to be a segregated or separately enclosed area within the Department's place of business. However, reasonable measures must be undertaken at all times to ensure that the computers used to access MVD's database(s) are accessibly only to Department personnel with assigned user IDs and passwords and are, therefore, shielded from the view of the public and/or any unauthorized individuals.

Records Access

The Department understands that its exclusive access to MVD records pursuant to this Agreement is through the Portal provider's MVRRS application. Upon execution of this Agreement between the Department and MVD, the Department's authorized users will be assigned user identifications (user IDs) and passwords based on the Department's approved data access security level to receive such records under federal and state law.

The Department will have three (3) access options under MVRRS, as described below:

- Via a web browser over the Internet;
- Via file (request / reply) transfers using file transfer protocol (FTP) over a dedicated and secured line; or
- Via sockets-based messaging over a dedicated and secured line.

Location of Activities

The Department may conduct authorized activities only at those locations which have been pre-approved by MVD. Any disapproval of location by MVD must be based on reasonable cause.
Equipment

The Department shall obtain computer equipment and software that is compatible with the information systems and connectivity requirements of the Portal provider and MVD, and which will allow access only to the specific database(s) listed in the Addendum to this Agreement.

Data Security

The Department shall provide a secure location for all computer equipment used to access MVD's database(s).

The Department shall provide access to MVD's database(s) only to Department personnel or contractors who are authorized users, and to no one else. If at any time MVD believes that an authorized user is utilizing such access in an unauthorized or unlawful manner, MVD reserves the right to immediately suspend or revoke that user's database access and/or to terminate the Department's authorization under this Agreement.

The Department shall comply with all policies, procedures and directives regarding security and database access made available to the Department by MVD during the course of this Agreement, including any future amendments thereto. All subcontractors utilized to perform the activities authorized by this Agreement must abide by the same security and access requirements as the Department.

Upon request by MVD, the Department must disclose any existing strategic alliances, partnerships, or subcontracting arrangements that the Department has which involve the processing and/or use of MVD data acquired pursuant to this Agreement.

Both during the term of this Agreement and subsequent to any termination of this Agreement, the Department, its officers, agents, employees, contractors and representatives shall not, without the prior written approval of MVD, disclose, distribute, or utilize in any manner not expressly authorized under this Agreement, any confidential and/or personal information which is connected or otherwise associated with this Agreement.

The Department shall maintain all hard copy information and electronic data related to this Agreement in a secure location at all times.

Data Privacy

The Department understands that both the manner in which MVD may release information from the records contained in its databases and the manner in which the Department may access and/or utilize such information are regulated by the Federal Driver's Privacy Protection Act (DPPA), 18 U.S.C. §§ 2721-2725, as well as Title 28, Chapter 2, Article 5 of the Arizona Revised Statutes. It is the responsibility of the Department, and any authorized user acting on the Department's behalf, to gain knowledge of all laws and applicable MVD policies and procedures which govern access to and use of MVD records, and to determine whether the Department is legally eligible to obtain such records from MVD.

MVD is not an agent of the Department or its subcontractors, and is in no way responsible or liable for the decisions or interpretations made by the Department or its officers, agents, employees, contractors and representatives, unless the contrary is specifically stated in writing by the MVD Director.

Anyone who knowingly obtains, uses or otherwise discloses personal information from an MVD record for a use not permitted under 18 U.S.C. § 2721, and anyone requesting the disclosure of personal information who
misrepresents his/her identity or makes a false statement in connection thereto, with the intent to obtain such information in a manner not authorized by law, is subject to civil and/or criminal penalties. A violation of the DPPA or any other applicable federal or state law will cause the immediate termination of this Agreement.

In reference to motor vehicle records access, the Department shall not utilize its connectivity to MVD’s records database(s) under this Agreement for any purpose other than the purpose(s) specified in the Addendum to this Agreement. If the Department seeks access to or information from MVD’s database(s) for a reason other than that specifically authorized by this Agreement, the Department must submit a completed hard copy of the Motor Vehicle Record Request form to the appropriate MVD Unit.

Network Security

The Department understands and agrees that any and all MVD information that it sends over external or public computer networks, such as the Internet, must be encrypted.

The Department further understands and agrees that all computers which are permanently or intermittently connected to the Department’s internal computer network(s) must employ a pre-approved rule and/or privilege-based access control system that, in MVD’s sole judgment, will serve to identify and authenticate each user in a manner which adequately protects MVD data from unauthorized access, disclosure and/or dissemination.

Scrutinized Business Operations

Pursuant to A.R.S. §§ 35-391.06 and 35-393.06, the DEPARTMENT (or private contractor) certifies that it does not have a scrutinized business operation in Sudan or Iran. For purposes of this Agreement, the term “scrutinized business operations” shall have the meanings set forth in A.R.S. § 35-391 and/or § 35-393, as applicable. If ADOT/MVD determines that the DEPARTMENT (or private contractor) submitted a false certification, ADOT may impose remedies as provided by law, including the cancellation or termination of this Agreement.

Personnel

The Department shall notify MVD in writing within two business days of any change in its list of authorized users, including, but not limited to, any subtractions from this list which may occur as a result of the termination of an authorized user’s employment, a job transfer, or any other change in status which establishes that the individual no longer requires access to MVD data.

The Department shall also respond immediately to all MVD inquiries concerning its list of authorized users.

Non-exclusivity

This Agreement shall not preclude MVD from entering into the same or similar Agreement with other public or private entities, including those performing identical or similar functions as the Department.
Notification

The Department shall assign a contact person who possesses, at a minimum, the authority to communicate on behalf of and to answer for the Department with respect to this Agreement. The contact person will sign individual user access agreements, receive and distribute user IDs within the Department and will maintain responsibility for record retention, problem resolution and notification of procedural changes.

The Department shall provide MVD in writing a description of the contact person's scope of authority regarding department operations in general and the activities to be performed under this Agreement in particular. The Department shall advise MVD within two business days of any change in its designated contact person and provide a statement as to that person's scope of authority. All notices to or demands upon MVD shall be in writing and shall be delivered in person, by fax, by email, or by U.S. mail addressed as follows:

Motor Vehicle Division  
Commercial Licensing and Specialty Services  
Electronic Data Services  
P.O. Box 2100, Mail Drop 502M  
Phoenix, AZ 85001  
Fax: (602) 712-3145  
Email: eds@azdpts.gov

All notices to or demands upon the Department by MVD will be addressed as specified in Section VI of the Agreement Addendum.

Records

The Department shall maintain a log or register of all MVD records it requests and all MVD records it obtains by virtue of the access provided herein. The Department shall retain this log or register either manually or electronically, along with all other books, papers, records, data, and accounting records relating to this Agreement, for a period of five (5) years; or such greater or lesser time as may be required by federal or state law, rule, or the ADOT Records Retention Schedule.

It is further agreed that ownership of all records relating to this Agreement resides exclusively with MVD.

Audit and inspection

The Department understands and agrees that all records described in the preceding section shall be subject to audit and inspection by authorized representatives of MVD or by any law enforcement agency at all times during the term of this Agreement, and for a period of five (5) years thereafter. If MVD determines that an on-site audit or inspection of the Department outside of Arizona is necessary, the Department shall pay for the auditors' travel expenses in an amount equal to the Arizona Department of Administration (ADOA) reimbursement rate for out-of-state travel as authorized by A.R.S. Title 38, Chapter 4, Article 2 and Section B of the Arizona Accounting Manual prepared by ADOA.

At MVD's sole discretion, the Department shall be required to retain a pre-approved independent professional organization to audit or assess the adequacy of the Department's information technology security procedures, including the methods and practices employed in the processing and use of MVD data. A written report of the results of each audit or assessment shall be provided to MVD within thirty (30) days of its completion. The Department shall have an audit or assessment performed based on a frequency specified by MVD and shall
not, without the express written approval of MVD, discontinue or modify this schedule. The Department shall also pay any and all costs associated with such security audits or assessments.

If any security and/or control deficiencies are identified as a result of an audit report, the Department understands and agrees that it must immediately take any and all corrective measures necessary to resolve those deficiencies. Within thirty (30) days of the issuance of the audit report, the Department shall also provide MVD with a written corrective action plan which, in MVD’s sole judgment, adequately describes the steps the Department has taken (or will take) in order to fully resolve each and every deficiency identified in a security audit.

Compliance

The Department shall comply with all of the terms set forth in this Agreement, together with all applicable federal and state statutes, rules, and regulations. The Department shall also comply with all relevant policies, procedures and directives made available to the Department by MVD during the course of this Agreement.

All Department subcontractors are held to the same compliance standards, and any failure to comply on the part of the subcontractor will be deemed a failure on the part of the Department.

Non-Compliance

If the Department fails to comply as provided above, MVD reserves the right to take any remedial action that it deems necessary and appropriate, including the revocation of the department’s account and termination of this Agreement in its entirety. In case of a violation of law, the Agreement shall be subject to immediate termination by MVD.

Cancellation

Either party may cancel this Agreement for cause or convenience upon thirty (30) days prior written notice to the other party. MVD reserves the right to cancel this Agreement at any time, without prior notice, if it determines that the public interest so requires, and the exercise of such right shall be without penalty and without recourse against MVD by the Department or any of its subcontractors.

This Agreement is also subject to cancellation by the Governor of Arizona pursuant to A.R.S. §38-511.

Except as otherwise directed by MVD, upon receipt of a notice of cancellation or termination (and to the extent specified in such notice) the Department shall:

1. Immediately cease any and all activities previously authorized under this Agreement;
2. Place no further requests for records pursuant to this Agreement;
3. Remit any outstanding monies owed to MVD and/or the Portal provider within forty-eight (48) hours; and
4. Ensure that its continued use of any records obtained prior to the effective date of cancellation or termination is restricted solely to the use(s) authorized by this Agreement.
Duration

This Agreement shall commence upon approval by the Motor Vehicle Division Director and execution by both parties, and shall thereafter continue in effect for a term of three (3) years, unless previously canceled or terminated as provided herein. Upon expiration of this three-year period, the parties may mutually agree to extend the term of the Agreement for another three (or fewer) year by entering into a "Joint Letter of Renewal."

Amendment and Modification of Agreement

The Department shall accept any modification of the Agreement for reasonable cause, if set forth in writing and deemed necessary by MVD. Upon the amendment of any applicable law, rule or regulation, the Agreement shall automatically be modified to reflect such amendment. Any modification of the Agreement shall be incorporated herein and shall be subject to all other provisions of this Agreement.

Non-Assignability

Unless the Department obtains the express written consent of MVD, this Agreement is not assignable to any other entity, in whole or in part.

Waiver/Severability

The Department agrees that a waiver of any provision of this Agreement shall not act as a waiver of any other provision of this Agreement. If a provision of this Agreement is for any reason declared invalid, illegal, or unenforceable, that declaration shall not affect the remainder of the provisions of the Agreement.

Liability

Each party (as "indemnitor") agrees to indemnify, defend and hold harmless the other party (as "indemnitee") from and against any and all claims, losses, liability, costs or expenses (including reasonable attorney's fees) (hereinafter collectively referred to as "claims") arising out of bodily injury of any person (including death) or property damage, but only to the extent that such claims which result in vicarious/derivative liability to the indemnitee are caused by the act, omission, negligence, misconduct, or other fault of the indemnitor, its officers, officials, agents, employees, or volunteers.
APPENDIX C.2

MISSOURI HIGHWAYS AND TRANSPORTATION COMMISSION

CONTRACT SERVICES AGREEMENT
MISSOURI HIGHWAYS AND TRANSPORTATION COMMISSION
CONTRACT SERVICES AGREEMENT

THIS AGREEMENT is entered into by HERE North America, LLC (hereinafter, "Contractor") and the Missouri Highways and Transportation Commission (hereinafter, "Commission").

WITNESSETH:

WHEREAS, the Commission has selected the Contractor to perform professional services in the nature of Real-Time and Historical Traffic Data Services; and

WHEREAS, the Contractor represents that it is qualified in its field of expertise to competently provide such services.

NOW, THEREFORE, in consideration of the mutual promises, covenants, and representations contained herein, the parties agree as follows:

(1) **SCOPE OF SERVICES.**

(A) The services covered by this Agreement shall include furnishing all personnel and the equipment, material and all other things necessary for the provision of Real-Time and Historical Traffic Data Services. The Contractor's provision of Real-Time and Historical Data is subject to the Contractor's license terms for the use of such data, as set forth in Exhibit III of the Agreement, titled "Licensing Terms".

(B) The specific services to be provided by the Contractor are set forth in Exhibit I to this Agreement, titled "Scope of Work," which is attached hereto and made a part of this Agreement, and which is also referenced in RFP # 6-131028BR.

(2) **ADDITIONAL SERVICES:** The Commission reserves the right to direct additional services not described in Exhibit I as changed or unforeseen conditions may require. Such direction by the Commission shall not be a breach of this Agreement. In this event, a supplemental agreement will be negotiated.
and executed prior to the Contractor performing the additional or changed services, or incurring any additional cost therefore.

(3) **NON SOLICITATION**: The Contractor warrants that it has not employed or retained any company or person, other than a bona fide employee working for the Contractor, to solicit or secure this Agreement, and that it has not paid or agreed to pay any company or person, other than a bona fide employee, any fee, commission, percentage, brokerage fee, gift, or any other consideration, contingent upon or resulting from the award or making of this Agreement. For breach or violation of this warranty, the Commission shall have the right to annul this Agreement without liability, or in its discretion, to deduct from this Agreement price or consideration, or otherwise recover, the full amount of such fee, commission, percentage, brokerage fee, gift, or contingent fee.

(4) **FEES**: The amount to be paid to the Contractor by the Commission as full remuneration for the performance of all services called for in connection with Option 1 of the Scope of Work, attached hereto as Exhibit I, is three-hundred seventy-eight thousand five-hundred dollars ($378,500.00), which is shown in Exhibit II, "Pricing Pages", Option 1, No. 5, Data for the entire state, attached hereto and made a part of this Agreement. For clarity, the fees shown in Exhibit II do not include fees for any Additional Services that may be requested by the Commission pursuant to Section 2 above.

(5) **NONDISCRIMINATION CLAUSE**: The Contractor shall comply with all state and federal statutes applicable to the Contractor relating to nondiscrimination, including, but not limited to, Chapter 213, RSMo; Title VI and Title VII of the Civil Rights Act of 1964 as amended (42 U.S.C. Sections 2000d and 2000e, et seq.); and with any provision of the "Americans with Disabilities Act" (42 U.S.C. Section 12101, et seq.).

(6) **EXECUTIVE ORDER**: The Contractor shall comply with all the provisions of Executive Order 07-13, issued by the Honorable Matt Blunt, Governor of Missouri, on the sixth (6th) day of March, 2007. This Executive Order, which promulgates the State of Missouri's position to not tolerate persons who contract with the state engaging in or supporting illegal activities of employing individuals who are not eligible to work in the United States, is incorporated herein by reference and made a part of this Agreement.

(A) By signing this Agreement, the Contractor hereby certifies that any employee of the Contractor assigned to perform services under the contract is eligible and authorized to work in the United States in compliance with federal law.
(B) In the event the Contractor fails to comply with the provisions of the Executive Order 07-13, or in the event the Commission has reasonable cause to believe that the Contractor has knowingly employed individuals who are not eligible to work in the United States in violation of federal law, the Commission reserves the right to impose such contract sanctions as it may determine to be appropriate, including but not limited to contract cancellation, termination or suspension in whole or in part or both.

(7) INCORPORATION OF PROVISIONS: The Contractor shall include the provisions of paragraph 6 of this Agreement in every subcontract. The Contractor shall take such action with respect to any subcontract as the Commission may direct as a means of enforcing such provisions, including sanctions for noncompliance.

(8) DISPUTES UNDER THIS AGREEMENT: The Commission's representative will decide all questions which may arise as to the quality, quantity, and acceptability of services performed by the Contractor and as to the rate of progress of the services; all questions which may arise as to the interpretation of the plans and specifications; all questions as to the acceptable fulfillment of the Agreement on the part of the Contractor; the proper compensation for performance or breach of the Agreement; and all claims of any character whatsoever in connection with or growing out of the services of the Contractor whether claims under this Agreement or otherwise. The Commission representative's decisions shall be conclusive, binding and incontestable.

(6) SUCCESSORS AND ASSIGNS: The Commission and the Contractor agree that this Agreement and all agreements entered into under the provisions of this Agreement shall be binding upon the parties hereto and their successors and assigns.

(10) INDEMNIFICATION: The Contractor shall defend, indemnify and hold harmless the Commission, including its members and department employees, from any claim or liability whether based on a claim for damages to real or personal property or to a person for any matter relating to or arising out of the Contractor's performance of its obligations under this Agreement.

(11) VENUE: It is agreed by the parties that any action at law, suit in equity, or other judicial proceeding to enforce or construe this Agreement, or regarding its alleged breach, shall be instituted only in the Circuit Court of Cole County, Missouri.

(12) AUDIT OF RECORDS: The Contractor must maintain all records relating to this Agreement, including but not limited to invoices, payrolls, etc. These records
must be available at all reasonable times at no charge to the Commission and/or its designees or representatives during the period of this Agreement and any extension thereof, and for three (3) years from the date of final payment made under this Agreement.

(13) **WORK PRODUCT:** All documents, reports, exhibits, etc. produced by the Contractor at the direction of the Commission and information supplied by the Commission shall remain the property of the Commission.

(14) **CONFIDENTIALITY:** The Contractor shall not disclose to third parties confidential factual matter provided by the Commission except as may be required by statute, ordinance, or order of court, or as authorized by the Commission. The Contractor shall notify the Commission immediately of any request for such information.

(15) **SOLE BENEFICIARY:** This Agreement is made for the sole benefit of the parties hereto and nothing in this Agreement shall be construed to give any rights or benefits to anyone other than the Commission and the Contractor.

(16) **AMENDMENTS:** Any change in this Agreement, whether by modification or supplementation, must be accomplished by a formal contract amendment signed and approved by the duly authorized representative of the Contractor and the Commission.

(17) **ASSIGNMENT:** The Contractor shall not assign, transfer or delegate any interest in this Agreement without the prior written consent of the Commission.

(18) **BANKRUPTCY:** Upon filing for any bankruptcy or insolvency proceeding by or against the Contractor, whether voluntarily, or upon the appointment of a receiver, trustee, or assignee, for the benefit of creditors, the Commission reserves the right and sole discretion to either cancel this Agreement or affirm this Agreement and hold the Contractor responsible for damages.

(19) **CANCELLATION:** The Commission may cancel this Agreement at any time for a material breach of contractual obligations or for convenience by providing the Contractor with written notice of cancellation. Upon cancellation, HERE shall be entitled to all fees incurred or payable through the date of cancellation. Should the Commission exercise its right to cancel the contract for such reasons, cancellation will become effective upon the date specified in the notice of cancellation sent to the Contractor.

(20) **COMMISSION REPRESENTATIVE:** The Commission's Authorized Representatives, MoDOT's State Traffic and Highway Safety Engineer or Traffic Management and Operations Engineer, are designated as the Commission's
representatives for the purpose of administering the provisions of this Agreement. The Commission's representatives may designate by written notice other persons having the authority to act on behalf of the Commission in furtherance of the performance of this Agreement.

(21) **SECTION HEADINGS:** All section headings contained in this Agreement are for the convenience of reference only and are not intended to define or limit the scope of any provision of this Agreement.

(22) **LAW OF MISSOURI TO GOVERN:** This Agreement shall be construed according to the laws of the state of Missouri. The Contractor shall comply with all local, state and federal laws and regulations relating to the performance of this Agreement.

(23) **CONTRACT PERIOD:** The initial contract period is from Notice of Award through one (1) year.

(24) **RENEWAL INFORMATION:** The contract shall not bind, nor purport to bind, the Commission for any contractual commitment in excess of the original contract period. The Commission shall have the right, at its sole option, to extend the contract for four (4) additional one-year periods, or any portion thereof. In the event that the Commission exercises its options to extend the contract, such extension must be accomplished by a formal contract amendment signed and approved by the duly authorized representative of the Contractor and the Commission.

[Remainder of Page Intentionally Left Blank.]
IN WITNESS WHEREOF, the parties have entered into this Agreement on the date last written below:

Executed by the Contractor the 25th day of February 2014.
Executed by the Commission the 27th day of February 2014.

MISSOURI HIGHWAYS AND TRANSPORTATION COMMISSION
By
Title: Chief Financial Officer

HERE North America, LLC
By
Title: Director

HERE North America, LLC
By
Title: General Legal Counsel

ATTEST:

Secretary to the Commission

ATTEST:

Title: Sales Support Specialist

ATTEST:

Title: Sales Support Specialist

APPROVED AS TO FORM:

Commission Counsel

APPROVED AS TO FORM:

Title:
EXHIBIT I
SCOPe OF WORK

(A) **Services:** The Offeror shall provide the following professional services: Real-time and/or historical traffic flow data.

(B) **Specific Requirements:** The Offeror will provide to the General Services Procurement Unit one (1) original, five (5) copies, and an electronic version of a program proposal which will include the following:

**Dual Option Proposal**

As described in Section (1), each proposal shall include **two separate options for providing the data:**

- Option 1 for providing recurring real-time data;
- Option 2 for providing recurring historical data.

Any real-time data purchased by MoDOT under Option 1 shall include the right to indefinitely archive such data going forward. In addition, any real-time data purchased for a roadway segment under Option 1 shall include access to archived traffic flow data for that particular segment as far back, and including, the entire 2012 calendar year. In other words, if real-time data is bought for a particular roadway segment, there is no need for MoDOT to purchase separate historical or archived data for that same segment. Pricing for real-time data purchased under Option 1 shall be provided in the form of a startup cost, if applicable, and a recurring subscription rate (i.e., X dollars for startup, if applicable, and Y dollars per centerline mile per month).

Option 2 of the proposal shall allow for the purchase of recurring historical data for a particular roadway segment or a group of roadway segments as it is archived. Any historical data purchased for a roadway segment under Option 2 shall include access to archived traffic flow data for that particular segment as far back, and including, the entire 2012 calendar year. Pricing for historical data shall be provided in the form of a startup cost, if applicable, and a recurring subscription rate (i.e., X dollars for startup, if applicable, and Y dollars per centerline mile per month).

For consistency, proposals shall utilize the pricing structure found in Section (5) of this RFP to provide the minimum required pricing information.
Option 1 – Real-Time Traffic Flow Data

Where possible, MoDOT will seek to purchase real-time traffic flow data for prioritized roadway segments throughout the state. Tables 1 and 2 are intended to outline MoDOT’s desired coverage area for real-time data and are prioritized to show which segments are viewed as most critical for coverage. Both the ability and the costs to provide the desired coverage identified in the tables below will be evaluated as part of the selection process. For consistent evaluation purposes, pricing shall be in accordance with the pricing page in Section (5) and shall include:

- Pricing for defined data packages including startup costs, if applicable, and the recurring subscription rate per month; and
- Pricing on a per-mile basis including startup costs, if applicable, and the recurring subscription rate per month based on the total centerline miles subscribed to.

Where practical, MoDOT anticipates purchasing data based on the defined data packages shown in Section (5). However, this may not always be feasible based on the available budget, and MoDOT may choose to purchase only portions of segments identified in Tables 1 and 2. The decision to purchase real-time data under Option 1 in whole or in part shall be at the sole discretion of MoDOT throughout the contract duration including any renewal periods.

Recurring subscription rates for data purchased apart from the defined data packages shall be based on the cumulative total centerline miles of data subscribed to at any one time. For example, one rate may be provided for a subscription to 0-100 centerline miles, while another rate might be provided for a subscription to 100-200 centerline miles. At any time during the contract, the subscription rate for any roadway segments purchased apart from a defined data package shall be based on the total centerline miles subscribed to at the current time. For example, if MoDOT elects to purchase Data Set A (134.2 miles) at the onset of the contract and later elects to subscribe to a portion of segments from Data Sets B and C, the subscription rate for the new segments would be based on the “total centerline miles subscribed to”, which would include the 108.2 miles from Data Set A and the mileage of the new segments to be purchased from Data Sets B and C.
Table 1 represents the minimum roadway segments for which MoDOT intends to obtain real-time data. Any variations or limitations between the segments identified below and those actually available should be clearly noted in the proposal. Proposals shall also indicate any segments for which data is typically only available at periodic times throughout the day.

Table 1 – Minimum Required Coverage – Real-Time Data (Option 1)

<table>
<thead>
<tr>
<th>Roadway</th>
<th>Length (miles)</th>
<th>Start</th>
<th>End</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-29</td>
<td>14.2</td>
<td>I-435 (Platte City)</td>
<td>Buchanan County line (MP 31)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-35</td>
<td>19.8</td>
<td>I-435 (Liberty)</td>
<td>Clinton County line (MP 33)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-44</td>
<td>34.0</td>
<td>Franklin County line (MP 223.8)</td>
<td>MP 257.8</td>
<td>Western Franklin County</td>
</tr>
<tr>
<td>I-49</td>
<td>29.8</td>
<td>Bates County line (Archie)</td>
<td>Jackson County line (Belton)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-55</td>
<td>20.0</td>
<td>RT M (MP 185.2)</td>
<td>Jefferson County line (MP 165.2)</td>
<td>Southern Jefferson County</td>
</tr>
<tr>
<td>I-70</td>
<td>5.0</td>
<td>US 40 (Grain Valley)</td>
<td>Lafayette County line (e/o Oak Grove)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-435</td>
<td>11.4</td>
<td>Kansas state line (MO River)</td>
<td>I-29 (Platte City)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>134.2</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 2 represents segments for which real-time data is highly desirable. Any variations or limitations between the segments identified below and those available should be clearly noted in the proposal. Proposals shall also indicate any segments for which data is typically only available at periodic times throughout the day. For pricing purposes, segments have been grouped into smaller data packages.

**Table 2 – Highly Desirable Coverage – Real-Time Data (Option 1)**

<table>
<thead>
<tr>
<th>Roadway</th>
<th>Length (miles)</th>
<th>Start</th>
<th>End</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-70</td>
<td>91.8</td>
<td>Lafayette County line (e/o Oak Grove)</td>
<td>MP 121.0</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-70</td>
<td>12.0</td>
<td>MP 121.0</td>
<td>MP 133.0</td>
<td>Columbia area</td>
</tr>
<tr>
<td>I-70</td>
<td>71.0</td>
<td>MP 133.0</td>
<td>MP 204.0</td>
<td>Rural interstate</td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td><strong>174.8</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>I-44</td>
<td>69.0</td>
<td>Oklahoma State line</td>
<td>MP 69.0</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-44</td>
<td>16.0</td>
<td>MP 69.0</td>
<td>MP 85.0</td>
<td>Springfield area</td>
</tr>
<tr>
<td>I-44</td>
<td>138.8</td>
<td>MP 85.0</td>
<td>Franklin County line (MP 223.8)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td><strong>223.8</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US 50</td>
<td>18.2</td>
<td>I-470</td>
<td>Johnson County line</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>US 60</td>
<td>12.4</td>
<td>MO 360</td>
<td>RT J</td>
<td>Springfield</td>
</tr>
<tr>
<td>US 61</td>
<td>7.4</td>
<td>I-70</td>
<td>St. Charles County line (northern border)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>US 63</td>
<td>5.5</td>
<td>RT AC</td>
<td>RT D</td>
<td>Columbia</td>
</tr>
<tr>
<td>US 65</td>
<td>15.8</td>
<td>I-44</td>
<td>MO 14</td>
<td>Springfield</td>
</tr>
<tr>
<td>US 67</td>
<td>15.2</td>
<td>Jefferson County line (southern border)</td>
<td>RT A (Crystal City)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>MO 21</td>
<td>20.0</td>
<td>MO 14</td>
<td>RT D</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>MO 30</td>
<td>13.3</td>
<td>RT W/RT MM</td>
<td>I-270</td>
<td>St. Louis area</td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td><strong>107.8</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>506.4</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition to the segments in Tables 1 and 2, proposals may include a list of additional roadway segments for which real-time data would be made available.
Option 2 – Historical Data Only

Where purchasing real-time data is not feasible, MoDOT may seek to purchase historical data for prioritized roadway segments throughout the state. Such data will also be considered for purchase where MoDOT already collects real-time traffic flow data via its own sensors and detectors.

Historical data provided under Option 2 shall meet the following requirements:

- Historical data for each month shall be made available to MoDOT for full use within ten (10) business days from the end of said month; five (5) business days is desired; see Table 5.
- MoDOT shall have indefinite access and rights to any historical data for a particular roadway segment, once purchased.
- Historical data purchased for any given segment shall include archived data from all prior months as far back and including the entire 2012 calendar year.
- Historical data shall be provided, at a minimum, in 5-minute intervals.
- Historical data shall meet the requirements specified in Table 5 of Section (2).

Tables 3 and 4 are intended to outline MoDOT’s desired coverage area for historical data and are prioritized to show which segments are viewed as most critical for coverage. Both the ability and the costs to provide the desired coverage identified in the tables below will be evaluated as part of the selection process. For consistent evaluation purposes, pricing shall be in accordance with the pricing page in Section (5) and shall include:

- Pricing for defined data packages including startup costs, if applicable, and the recurring subscription rate per month.
- Pricing on a per mile basis including startup costs, if applicable, and the recurring subscription rate per month based on the total centerline miles subscribed to.

Where practical, MoDOT anticipates purchasing data based on the defined data packages shown in Section (5). However, this may not always be feasible based on the available budget, and MoDOT may choose to purchase only portions of segments identified in Tables 3 and 4. The decision to purchase historical data under Option 2 in whole or in part shall be at the sole discretion of MoDOT throughout the contract duration including any renewal periods.

Recurring subscription rates for data purchased apart from the defined data packages shall be based on the cumulative total centerline miles of data subscribed to at any one time. For example, one rate may be provided for a subscription to 0-100 centerline miles, while another rate might be provided for a subscription to 100-200 centerline miles. At any time during the contract, the subscription rate for any roadway segments purchased apart from a defined data package shall be based on the total centerline miles subscribed to at the current time. For example, if MoDOT elects to purchase Data Set E at the onset of the contract and later elects to subscribe to a portion of segments from Data Set F, the subscription rate for the new segments would be based on the "total centerline miles subscribed to", which:
would include the 737.3 miles from Data Set E and the mileage for the new segments to be purchased from Data Set F.

Table 3 represents the roadway segments for which MoDOT most desires historical data. Any variations or limitations between the segments identified below and those available should be clearly noted in the proposal.

Table 3 – Minimum Desired Coverage – Historical Data Only (Option 2)

<table>
<thead>
<tr>
<th>Roadway</th>
<th>Length (miles)</th>
<th>Start (mile marker)</th>
<th>End (mile marker)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-44</td>
<td>56.6</td>
<td>Franklin County line (MP 223.8)</td>
<td>I-55 (MP 290.4)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-55</td>
<td>44.6</td>
<td>Jefferson County line (MP 165.2)</td>
<td>Miss. River (MP 200.8)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-64</td>
<td>40.8</td>
<td>I-70 (MP 0.0)</td>
<td>Miss. River (MP 40.8)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-70</td>
<td>47.6</td>
<td>MP 204.0</td>
<td>Miss. River (MP 251.6)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-170</td>
<td>11.2</td>
<td>I-64 (MP 0.0)</td>
<td>I-270 (MP 11.2)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-255</td>
<td>4.0</td>
<td>I-55 (MP 0.0)</td>
<td>Miss. River (MP 4.0)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-270</td>
<td>35.8</td>
<td>I-55 (MP 0.0)</td>
<td>Miss. River (MP 35.8)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>US 61</td>
<td>7.4</td>
<td>I-70</td>
<td>St. Charles County line (northern border)</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>US 67</td>
<td>75.8</td>
<td>Jefferson County line (southern border)</td>
<td>Miss. River</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>MO 370</td>
<td>13.0</td>
<td>I-70</td>
<td>I-270</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>MO 21</td>
<td>28.9</td>
<td>RT D</td>
<td>MO 30</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>MO 30</td>
<td>25.2</td>
<td>RT W/ RT M/M</td>
<td>I-55</td>
<td>St. Louis area</td>
</tr>
<tr>
<td>I-29</td>
<td>31.0</td>
<td>I-35 (MP 0.0)</td>
<td>Buchanan County line (MP 31.0)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-35</td>
<td>33.0</td>
<td>Kansas state line (MP 0.0)</td>
<td>Clay County line (MP 33.0)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-49</td>
<td>37.0</td>
<td>Bates County line (MP 147.0)</td>
<td>I-435 (MP 184.0)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-70</td>
<td>29.2</td>
<td>Kansas state line (MP 0.0)</td>
<td>Lafayette County line (e/o Oak Grove)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>Roadway</td>
<td>Length (miles)</td>
<td>Start (mile marker)</td>
<td>End (mile marker)</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>----------</td>
</tr>
<tr>
<td>I-435</td>
<td>54.8</td>
<td>Kansas state line (MP 75.4)</td>
<td>MO River (MP 20.6)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-470</td>
<td>17.2</td>
<td>I-435 (MP 0.0)</td>
<td>I-70 (MP 17.2)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-635</td>
<td>3.8</td>
<td>Kansas state line (MP 9.0)</td>
<td>I-29 (MP 12.8)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-670</td>
<td>2.4</td>
<td>Kansas state line (MP 1.0)</td>
<td>US 71 (MP 3.4)</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>US 50</td>
<td>53.7</td>
<td>I-470</td>
<td>RT FF</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>US 71</td>
<td>12.6</td>
<td>I-435</td>
<td>I-70</td>
<td>Kansas City area</td>
</tr>
<tr>
<td>I-44</td>
<td>16.0</td>
<td>69.0</td>
<td>85.0</td>
<td>Springfield</td>
</tr>
<tr>
<td>US 60</td>
<td>12.4</td>
<td>MO 350</td>
<td>RT F</td>
<td>Springfield</td>
</tr>
<tr>
<td>US 65</td>
<td>15.8</td>
<td>I-44</td>
<td>MO 14</td>
<td>Springfield</td>
</tr>
<tr>
<td>I-70</td>
<td>12.0</td>
<td>MP 121.0</td>
<td>MP 133.0</td>
<td>Columbia</td>
</tr>
<tr>
<td>US 63</td>
<td>5.5</td>
<td>RT AC</td>
<td>RT B</td>
<td>Columbia</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>737.3</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 4 represents segments for which historical data is highly desirable. Any variations or limitations between the segments identified below and those available should be clearly noted in the proposal.

**Table 4 – Highly Desirable Coverage – Historical Data Only (Option 2)**

<table>
<thead>
<tr>
<th>Roadway</th>
<th>Length (miles)</th>
<th>Start (mile marker)</th>
<th>End (mile marker)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-29</td>
<td>13.0</td>
<td>I-29 (MP 43.0)</td>
<td>I-29 (MP 56.0)</td>
<td>St. Joseph</td>
</tr>
<tr>
<td>I-229</td>
<td>15.0</td>
<td>I-29 (MP 0.0)</td>
<td>I-29 (MP 13.0)</td>
<td>St. Joseph</td>
</tr>
<tr>
<td>LP 29</td>
<td>14.0</td>
<td>I-29 (Exit 44)</td>
<td>I-29 (Exit 53)</td>
<td>St. Joseph</td>
</tr>
<tr>
<td>US 36</td>
<td>3.9</td>
<td>MO River</td>
<td>I-29</td>
<td>St. Joseph</td>
</tr>
<tr>
<td>I-44</td>
<td>7.0</td>
<td>MO 43 (MP 4.0)</td>
<td>I-49 (MP 11.0)</td>
<td>Joplin</td>
</tr>
<tr>
<td>LP 44</td>
<td>11.6</td>
<td>I-44 (Exit 6)</td>
<td>I-44 (Exit 15)</td>
<td>Joplin</td>
</tr>
<tr>
<td>LP 49</td>
<td>15.6</td>
<td>MO 175</td>
<td>MO 249</td>
<td>Joplin</td>
</tr>
<tr>
<td>MO 249</td>
<td>6.2</td>
<td>I-49 (Exit 53B)</td>
<td>I-49</td>
<td>Joplin</td>
</tr>
<tr>
<td>US 50</td>
<td>9.4</td>
<td>Truman Blvd.</td>
<td>Moreau River</td>
<td>Jefferson City</td>
</tr>
<tr>
<td>US 54</td>
<td>5.0</td>
<td>MO 179</td>
<td>US 63 (e/o MO River)</td>
<td>Jefferson City</td>
</tr>
<tr>
<td>I-55</td>
<td>6.0</td>
<td>US 61 (MP 93.0)</td>
<td>US 61 (MP 99.0)</td>
<td>Cape Girardeau/Jackson</td>
</tr>
<tr>
<td>US 61</td>
<td>17.4</td>
<td>I-55 (Exit 93B)</td>
<td>I-55 (Exit 99)</td>
<td>Cape Girardeau/Jackson</td>
</tr>
<tr>
<td>BU 65</td>
<td>9.0</td>
<td>US 60 (Republic Rd)</td>
<td>US 65 (Clacknutt)</td>
<td>Springfield</td>
</tr>
<tr>
<td>LP 44</td>
<td>9.7</td>
<td>I-44 (Exit 72)</td>
<td>I-44 (Exit 80)</td>
<td>Springfield</td>
</tr>
<tr>
<td>US 160</td>
<td>7.0</td>
<td>US 60</td>
<td>I-44</td>
<td>Springfield</td>
</tr>
<tr>
<td>MO 13</td>
<td>11.4</td>
<td>US 60</td>
<td>I-44</td>
<td>Springfield</td>
</tr>
<tr>
<td>MO 744</td>
<td>6.7</td>
<td>US 160</td>
<td>US 65</td>
<td>Springfield</td>
</tr>
</tbody>
</table>

**Subtotal:** 167.9

<table>
<thead>
<tr>
<th>Roadway</th>
<th>Length (miles)</th>
<th>Start (mile marker)</th>
<th>End (mile marker)</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>I-70</td>
<td>91.8</td>
<td>Lafayette County line (e/o Oak Grove)</td>
<td>MP 121.0</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-70</td>
<td>71.0</td>
<td>MP 133.0</td>
<td>MP 204.0</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-44</td>
<td>69.0</td>
<td>Oklahoma state line</td>
<td>MP 69.0</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-44</td>
<td>138.8</td>
<td>MP 85.0</td>
<td>Frueklin County line (MP 223.8)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>Roadway</td>
<td>Length (miles)</td>
<td>Start (mile marker)</td>
<td>End (mile marker)</td>
<td>Comments</td>
</tr>
<tr>
<td>---------</td>
<td>----------------</td>
<td>---------------------</td>
<td>-------------------</td>
<td>----------</td>
</tr>
<tr>
<td>I-29</td>
<td>12.0</td>
<td>Buchanan County line (MP 31.0)</td>
<td>I-229 (MP 43.0)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-29</td>
<td>67.3</td>
<td>I-229 (MP 56.0)</td>
<td>Iowa state line</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-35</td>
<td>81.4</td>
<td>Clay County line (MP 33.0)</td>
<td>Iowa state line</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-49</td>
<td>34.8</td>
<td>Pineville</td>
<td>I-44 (MP 39.0)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-49</td>
<td>137.3</td>
<td>I-44 (MP 46.0)</td>
<td>I-435 (MP 184.0)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-55</td>
<td>99.0</td>
<td>Arkansas state line (MP 0.0)</td>
<td>US 61 (MP 99.0)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-55</td>
<td>72.2</td>
<td>US 61 (MP 93.0)</td>
<td>Jefferson County line (MP 165.2)</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-57</td>
<td>22.3</td>
<td>I-55 (MP 0.0)</td>
<td>Illinois state line</td>
<td>Rural interstate</td>
</tr>
<tr>
<td>I-155</td>
<td>10.8</td>
<td>I-55 (MP 0.0)</td>
<td>Tennessee State line</td>
<td>Rural interstate</td>
</tr>
<tr>
<td><strong>Subtotal</strong></td>
<td><strong>907.7</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>1,075.6</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In addition to the segments in Tables 3 and 4, proposals may include a list of additional roadway segments for which historical data would be made available.
Data Validation

The Offeror shall agree to cooperate with data validation efforts either by MoDOT or an independent Offeror of the State's choosing. Such cooperation may include providing specific location information for roadway segments in order to allow for accurate comparisons between Offeror data and the independent data source. Data validation may be performed using a number of different processes as described below.

For all evaluation data, the speeds shall be rounded to the nearest whole number.

MoDOT reserves the right to test the data accuracy as often as once per month or as many segments as desired, and all validation results are publically distributable.

For validation purposes, the following definitions should be used:

- **The absolute speed error** is defined as the absolute value of the difference between the mean speed reported from the data service and the mean speed provided by validation procedures for a specified time period or polling interval. Speed data shall have a maximum average absolute error of 10 MPH.

  **Calculation Method**
  
  Let:  
  \[ A_i = \text{Speed data for link } i \text{ at time } j \text{ from the data service.} \]
  \[ B_{ij} = \text{Corresponding speed from the validation data} \]
  
  Average absolute error = mean(abs(Aij - Bij)).

  - **Speed range is dependent on the validation data (Bij)**.

- **Speed error bias** is defined as the average speed error (not the absolute value) in each speed range. Speed data shall have a maximum average error of ± 5 MPH in each of the following speed ranges: 0-30 mph, 31-45 mph, 46-60 mph, and >60 mph.

  **Calculation Method**
  
  Let:  
  \[ A_i = \text{Speed data for link } i \text{ at time } j \text{ from the data service.} \]
  \[ B_{ij} = \text{Corresponding speed from the validation data} \]
  
  Average error = mean(Aij - Bij).

  - **Speed range is dependent on the value B_{ij}. The calculation is similar to that of Average Absolute Speed Error, but without the absolute value operator.**

The following processes may be utilized to validate Offeror data:

**A. Validation using MoDOT-owned sensors and detectors**

In an effort to streamline validation, the Offeror shall make available to MoDOT, samples of probe data, when requested, for roadway segments where MoDOT collects
their own real-time traffic data (see Table 6). The segments chosen for testing under this process shall be determined by MoDOT and represent, at a minimum, both the St. Louis and Kansas City metro areas. Probe data provided by the Offeror for validation purposes shall not be used by MoDOT for any other purpose (travel times, public traveler information, etc.).

Using the sample probe data for selected segments, MoDOT will pull data from agency owned detectors and sensors for the same segments during the same time periods. For each 15-minute interval of each segment, the average speed will be determined from both data sources and subsequently compared to see if the data requirements of Table 5 are adequately met (see requirements 10 and 11). The average absolute errors for each 15-minute interval will be averaged to calculate a single average absolute error for the entire data set being validated.

A final average absolute error greater than 10 MPH shall result in unsatisfactory results. In addition, any single average absolute error greater than 20 MPH for an individual 15-minute interval shall result in unsatisfactory results.

B. Validation using Bluetooth detectors

When validation using MoDOT-owned sensors and detectors is not possible or feasible, MoDOT may choose to utilize Bluetooth technology to obtain sufficient ground truth data. The overall validation process will work similar to the process described above.

MoDOT will determine specific segments during a testing period for which traffic data will be obtained using Bluetooth detection. Segment lengths for Bluetooth testing will match, as much as possible, the same limits of the Offeror segments being tested. For each 15-minute interval of each segment, the average speed will be determined from both data sources and subsequently compared to see if the data requirements of Table 5 are adequately met (see requirements 10 and 11). The average absolute errors for each 15-minute interval will be averaged to calculate a single average absolute error for the entire data set being validated.

A final average absolute error greater than 10 MPH shall result in unsatisfactory results. In addition, any single average absolute error greater than 20 MPH for an individual 15-minute interval shall result in unsatisfactory results.

C. Validation using GPS-enabled travel time recorders

If necessary, MoDOT may also utilize GPS-enabled travel time recorders to validate reported travel times on select segments. If this method is used, a process will be established between MoDOT and the Offeror to adequately carry out such testing.

Results of the validation tests may be used as justification for contract termination as described in Section (3) and for determining whether or not contract renewal options are
exercised. If validation tests indicate the Offeror has not met the stated data requirements for a given month, the Offeror will be promptly notified in writing, and a follow-up validation test will be scheduled at an agreed upon time, no longer than 30 days from the noted unsatisfactory validation test. Upon notification, the Offeror shall submit to MoDOT a plan to correct the activity or an explanation for unsatisfactory results within ten (10) business days of said results. If validation tests for the subsequent testing period also indicate unsatisfactory results, MoDOT shall retain the right to withhold further payment, renegotiate the contract, or terminate the contract in accordance with Section (3).

The Offeror shall disclose any changes that may improve or reduce data quality including, but not limited to gaining or losing a key fleet of vehicles or a cellular carrier contact. In the event that a key data source becomes unavailable, data quality requirements shall remain in place.

Valid Sources of Data

Data sources shall only include actual, observed measurements using probe technology or infrastructure based systems. Estimates or projections based on historical data shall not be acceptable for the purpose of providing real-time data (Option 1).

The Offeror may choose to integrate real-time data from MoDOT sensors in existing formats or schemas to supplement existing data feeds. Any additional processing or formatting will be the responsibility of the Offeror. In the event the Offeror is using data from MoDOT sensors, the Offeror shall ultimately be held responsible for meeting all data requirements. MoDOT is not liable for failed or inaccurate data from its detectors. In the event that the Offeror obtains new sources of data, these may be incorporated into the system at no additional cost to MoDOT. Additionally, MoDOT may make available to the Offeror new data sources where feasible.
Data Format, Integration, Access, and Analytics

The Offeror shall provide data that meets the requirements in Table 5.

The Offeror shall provide a web-based tool to view real-time traffic data by MoDOT and its partners (not the general public). The website shall be password protected.

The Offeror shall provide a web-based archiving service to MoDOT in which data is stored, at a minimum, for three (3) years. Any data purchased shall include data from the time of purchase back through January 2012, or earlier. The web-based archiving service may be hosted by a third-party, but any requirements of Table 5 shall apply and MoDOT hardware, software, or network infrastructure shall not be required to maintain the service. The archiving service should also allow for data to be exported in a .csv or .xls format.

In addition to the archiving service, it is desirable for the Offeror to provide a web-based tool for data analytics. The web-based analytics tool may be hosted by a third-party, but any requirements of Table 5 shall apply and MoDOT hardware, software, or network infrastructure shall not be required to maintain the service. The analytics tool, if provided, shall be web-based and provide automated analytics for performance measures including, but not limited to:

- Average speeds
- Travel times
- Travel time index
- Planning time index and/or buffer time
- User delay costs

Such measures shall be available at various time intervals including, but not limited to yearly, quarterly, monthly, daily, and hourly. The analytics tool should allow for data analysis to be presented using graphs, tables, animations, and/or maps. The analytics tool should also allow for data to be exported in a .csv or .xls format.

The same web-based system may be used to provide the real-time view, the archiving service, and the data analytics, if desired.

Project Duties of the Offeror

The Offeror shall provide a Project Work Plan within ten (10) business days of Notice to Proceed. The Project Work Plan will include:

- A Project Schedule that outlines all necessary steps required to provide the selected traffic data. The schedule will include key milestones and the commencement date for the delivery of the traffic data feed shall be part of the schedule.
• A Quality Assurance/Quality Control (QA/QC) Plan that describes the Offeror’s plan for monitoring and maintaining data quality and coordination with MoDOT and any independent validation Offeror as supplied by MoDOT.

The Offeror shall submit monthly progress reports by the fifth business day of the next month. Prior to the commencement of the data feed, these progress reports shall provide the Offeror’s status relative to the milestones in the Project Schedule. After the commencement of the data feed, the Offeror shall submit monthly reports that include any key information affecting the quality, availability or reliability of the data feed in the previous month. For any issues that arise, the Offeror shall present a plan for how they will be resolved. The project will begin with a formal kick-off meeting, either in person or via phone, to review the Project Work Plan and provide an opportunity for MoDOT and the Offeror to share expectations for the project.

Traffic Data Requirements

The following section contains the baseline system specifications in the form of a response matrix (Table 5). Priority codes are given for each specification in the matrix. The definition of each priority code is defined below. Respondents are to provide information requested in their proposal in the matrix, as noted. If additional space is required for further explanation or supporting material is appended, directly reference the additional or supporting information within the corresponding cell within the matrix (for example: “see Attachment XX for a detailed explanation”), and the attachment should also explicitly refer to the section in the matrix to which it applies.

In the Offeror's technical response, the following matrix columns should be completed for each listed item:

1. **Response Code** – Employ the response codes noted below, defining compliance with the requirement.
2. **Respondent Comments** – Explain how the Offeror’s solution meets the requirement and identify any exceptions taken to the requirements.

**Priority Codes:**

* F: Information
  * M/C: Mandatory Specification – Offeror concurrence required
  * M/E: Mandatory Specification – Process explanation or supporting information required
  * H/D/C: Highly Desirable Specification – Offeror concurrence
  * H/D/E: Highly Desirable Specification – Process explanation or supporting information required
  * D/C: Desirable Specification – Offeror concurrence
  * D/E: Desirable Specification – Process explanation or supporting information required

**Response Codes:**

* E: Proposal exceeds the stated requirement. Provide a detailed explanation.
Proposal fully complies with the stated requirement. Provide a detailed explanation.

Proposal partially complies with the stated requirement. Provide a detailed explanation.

Proposal does not comply with the stated requirement.

### Table 5 – Data System Specification Matrix

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Priority Code</th>
<th>Response Code</th>
<th>Respondent Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data Elements</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Mean segment speed in miles per hour rounded to the nearest integer.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Mean segment travel time to the nearest whole second.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>A status flag shall be associated with each segment and reporting interval to indicate normal operations, periods of low-traffic flow, inoperable status or unavailable data, etc. Offeror should specify flags appropriate to methodology.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>A quality indicator should be used to provide a numerical score that reflects the confidence in the estimate of the mean speed and travel time. The intent is to provide a measure similar in concept to the standard error in the estimate of the mean. Offeror should provide explanation of the quality metric.</td>
<td>H/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Other traffic data valuable for roadway operations. This may include but is not limited to such metrics as volume, occupancy, event data, and incident data.</td>
<td>D/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Format</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Data shall be provided as XML-formatted content using an approved MoDOT schema and shall be made available through a web-based subscription service. The system will allow for appropriate access permission to limit distribution only to authorized subscribers. The service shall allow for selective content subscription so that various sections of MoDOT may subscribe only to the geographic area of interest. Each proposal shall contain, at a minimum, three (3) sets of sample data for evaluation purposes.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Data shall also be available in CSV format, if requested.</td>
<td>H/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>The format of the data shall conform to applicable TMDD standards or other comparable open and published standards. Offeror should provide a precise description of the processes and timing associated with their provision of the data.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Data files shall be delivered via HTTP or other standard protocol.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Priority Code</td>
<td>Response Code</td>
<td>Comments</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------------</td>
<td>---------------</td>
<td>----------</td>
</tr>
<tr>
<td>10</td>
<td><strong>Average Absolute Speed Error</strong>&lt;br&gt;The absolute speed error is defined as the absolute value of the difference between the mean speed reported from the data service and the mean speed provided by validation procedures for a specified time period or polling interval. Given that monitored links will be of different lengths, quality requirements based on speed rather than travel time will normalize the effect of varying link lengths.&lt;br&gt;&lt;br&gt;Speed data shall have a maximum average absolute error of 10 MPH.&lt;br&gt;&lt;br&gt;<strong>Calculation Method</strong>&lt;br&gt;Let: $A_i =$ Speed data for link at time $t$ from the data service.&lt;br&gt;      $B_i =$ Corresponding speed from the validation data&lt;br&gt;      Average absolute error $= \text{mean}(\text{abs}(A_i - B_i))$.&lt;br&gt;&lt;br&gt;Speed range is dependent on the validation data ($B_i$).&lt;br&gt;&lt;br&gt;<strong>Example:</strong> A source of validation data exists for various segments and for various time intervals within the I-70 corridor. For each 15-minute interval, a mean speed will be calculated for each segment for which validation speed data exists. Mean speeds from the validation data source will be compared with the respective mean speeds reported by the data service for each 15-minute interval. For each 15-minute interval, an average absolute error will be calculated.&lt;br&gt;&lt;br&gt;The individual average absolute errors for each segment and 15-minute interval will be averaged to produce a single average absolute error for the entire data set being validated.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Priority Code</td>
<td>Response Code</td>
<td>Respondent Comments</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>---------------</td>
<td>---------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| 11   | **Speed Error Bias**<br>Error bias is defined as the average speed error (not the absolute value) in each speed range. Speed data shall have a maximum average error of +/- 5 MPH.<br><br>**Calculation Method**<br>Let:  
\[ A_i = \] Speed data for link / at time / from the data service.<br>\[ B_i = \] Corresponding speed from the validation data<br>\[ \text{Average error} = \text{mean}(A_i - B_i) \]<br>\[ \text{Speed range is dependent on the value } B_i. \] The calculation is similar to that of Average Absolute Speed Error, but without the absolute value operator. | M/E |            |                   |
<p>| 12   | <strong>Accuracy requirements will be in effect for vehicle flows exceeding 500 VPH.</strong> | M/C |            |                   |
|      | <strong>Accuracy requirements will be in effect for vehicle flows exceeding 200 VPH.</strong> | HD/C |            |                   |
| 13   | <strong>Segmentation</strong>&lt;br&gt;Segmentation of the road network is the responsibility of the Owner and shall be performed in cooperation with MoDOT. Link definition shall be based on logical breaks in facilities where one would expect the potential for differing traffic conditions, such as at an interchange, a lane drop, or a major at-grade intersection. At a minimum, freeway segments shall break at each interchange. The following chart indicates guidelines for segment lengths of various road classifications.&lt;br&gt;&lt;br&gt;<strong>Link length guidelines</strong>&lt;br&gt;<strong>URBAN</strong>&lt;br&gt;FREeways: 1-3 miles&lt;br&gt;ARTERIALS: 0.5-5 miles&lt;br&gt;<strong>RURAL</strong>&lt;br&gt;FREeways: 3-10 miles&lt;br&gt;ARTERIALS: 2-3 miles | I/C |            |                   |
| 14   | Ramps (where provided) should be reported as separate links. | D/C |            |                   |
| 15   | Reversible lanes and other lane specific modes (where provided) should be reported as separate links. | D/C |            |                   |</p>
<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Priority Code</th>
<th>Response Code</th>
<th>Respondent Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Segment definitions shall, at a minimum, contain beginning and ending latitude, longitude, heading, common name or route number, and a unique identifier (such as a TMC code). Use applicable TMDT standards or comparable open and published data standards. A segment definition file shall be provided and updated as changes are made and shall conform to applicable standards or comparable open and published data standards. The segment definition file shall be in XML format in a MoDOT approved schema. The segment definition file shall also be available in CSV format. Segmentation shall be translatable to the MoDOT geographic framework.</td>
<td>16</td>
<td>M/E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Tables depicting the roadways within the state for which traffic data is requested are included in Section 2 of the RFP. These tables represent a consensus vision of the network of roadways for which data is desired. Actual implementation of roadway segments may differ from those depicted in the tables, and the selection of the routes depicted in the tables in whole or in part is at the sole discretion of MoDOT. Using the tables as a guide indicate the following: - Variations or limitations between the proposed coverage and that identified in Tables 1-4. - Any regions in the tables for which real-time traffic data cannot be provided. For consistency, proposals shall include pricing in the format described in Section (5).</td>
<td>17</td>
<td>M/E</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Traffic data shall be provided 24 hours per day, 7 days per week.</td>
<td>18</td>
<td>M/C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data shall be updated whenever the mean speed changes by 3 MPH or greater OR when the travel time changes by 5% or greater OR when the status flag changes. At a minimum, a full data set shall be supplied at least once every five (5) minutes. In either case the latency requirements of the data prevail (Items 9 &amp; 10).</td>
<td>19</td>
<td>M/E</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Priority Code</td>
<td>Response Code</td>
<td>Respondent Comments</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>20</td>
<td>Data shall be updated whenever the mean speed changes by 3 MPH or greater OR when the travel time changes by 5% or greater OR when the status flag changes. At a minimum, a full data set shall be supplied at least once every three (3) minutes. In either case the latency requirements of the data prevail (Items 9 &amp; 10).</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Maximum data latency shall be less than or equal to five (5) minutes.</td>
<td></td>
<td>M/B</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Maximum data latency shall be less than or equal to three (3) minutes.</td>
<td></td>
<td>HD/E</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td><strong>Availability:</strong> &lt;br&gt; Data availability is defined as the percent of time for which the data service was available (system uptime). &lt;br&gt; Data subscription services shall maintain at least 99% availability, excluding any scheduled system maintenance. &lt;br&gt; Scheduled maintenance shall be limited to 40 hours per year and only during non-peak hours. The Offeror shall work with MoDCT to obtain prior approval for when such maintenance will occur. &lt;br&gt; The Offeror shall provide a method for reporting data availability to MoDCT each month.</td>
<td></td>
<td>M/C</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td><strong>Reliability:</strong> &lt;br&gt; Reliability is defined as the ability of the data service to produce traffic data estimates consistently for each segment at all times. Data reliability is measured simply as the percentage of measurement intervals (combination of space and time) when traffic data estimates are delivered. &lt;br&gt; Note: Valid traffic data estimates occur only when sufficient base level data exists to support an estimate of the mean travel time or mean speed for a particular time period. Estimates based purely on imputation (for example, the historical average) are not considered a valid estimate in terms of the availability requirement. Periods of low flow (&lt;500 VPH) are excluded. &lt;br&gt; Traffic data shall be provided for at least 95% of all segments at all required time reporting intervals. &lt;br&gt; The Offeror shall provide a method for reporting data reliability to MoDCT each month.</td>
<td></td>
<td>M/E</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Hardware, software and network capacity shall be sufficient to initially support up to 25 concurrent data subscriptions, with the capability to scale to 100 data subscriptions as needed. It is the responsibility of the Offeror to provide sufficient capacity to service all subscription demands.</td>
<td></td>
<td>M/E</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
<td>Priority Code</td>
<td>Response Code</td>
<td>Respondent Comments</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>26</td>
<td>Offerors shall provide an archiving service for all real-time or historical data provided to MoDOT. Historical data shall be kept for at least 3 years and begin with January 2012.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Historical data, if purchased, shall be available for each month within ten (10) business days from the end of said month.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Historical data, if purchased, shall be available for each month within five (5) business days from the end of said month.</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Historical data, if purchased, shall be delivered, at a minimum, in 15-minute intervals.</td>
<td>M/C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Website for Monitoring Traffic Data**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Priority Code</th>
<th>Response Code</th>
<th>Respondent Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>Offerors shall provide a web-based tool to view real-time traffic data by MoDOT and its partners (not the general public). Partners may include MPO's, consultants, and universities. The web site shall be password protected.</td>
<td>M/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>The web-based tool shall have the capacity to initially support up to 100 concurrent users with the ability to scale to 500 concurrent users as needed.</td>
<td>M/C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Data from the real-time traffic service shall be viewable in real-time via the web-based tool.</td>
<td>M/C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>33</td>
<td>Archived traffic data shall be accessible via the web-based tool.</td>
<td>M/C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>The web-based tool shall allow routes and data to be selected and viewed in an electronic map-based interface.</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>35</td>
<td>The web-based tool shall perform data analytics including, but not limited to average speed, travel time, travel time index, planning time index, buffer time, and user-delay costs.</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>The web-based tool shall allow analytics to be done for various time periods including, but not limited to, yearly, quarterly, monthly, daily, and hourly.</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>37</td>
<td>The web-based tool shall allow for data analysis to be presented and/or visualized in graphical, table, animations, and map formats.</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
<tr>
<td>38</td>
<td>The web-based tool shall allow for the export of data in .csv or .xls format.</td>
<td>HD/E</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Project Deliverables**

The Offeror shall have three (3) months from the Notice to Proceed to provide access to the data as described in Section (2).

(C) **Administration of Program:** The Offeror will consult MHTC's representative regarding any problems involved with the administration of the services provided pursuant to this RFP.
III. Cost and Fees

Here are estimated costs for Option 1 and Option 2 below. Both options include $3,000, one time startup costs, required for UMD CATT Lab to procure necessary hardware and to configure the RTTS system. One time startup costs also include costs to integrate MoDOT traffic volume data with the system.

Option 1 – Real Time Data (Includes Historical Data)

<table>
<thead>
<tr>
<th>No.</th>
<th>Data Packages</th>
<th>Start-Up Cost (if applicable)</th>
<th>Recurring Subscription (per year)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Set A (134.2 miles)</td>
<td>$88,500</td>
<td>$56,000</td>
</tr>
<tr>
<td>2</td>
<td>Data Sets A and B (309.0 miles)</td>
<td>$89,900</td>
<td>$169,500</td>
</tr>
<tr>
<td>3</td>
<td>Data Sets A, B, and C (532.8 miles)</td>
<td>$95,500</td>
<td>$145,000</td>
</tr>
<tr>
<td>4</td>
<td>Data Sets A, B, C, and D (640.6 miles)</td>
<td>$99,500</td>
<td>$162,000</td>
</tr>
<tr>
<td>5</td>
<td>Data for the entire state</td>
<td>$189,500</td>
<td>$198,000</td>
</tr>
</tbody>
</table>

Based on the available budget, it may not be feasible for MoDOT to purchase entire data sets. When data is to be purchased apart from the defined packages above, the rates in the table below shall be used.

<table>
<thead>
<tr>
<th>Total Centerline Miles Subscribe To</th>
<th>0-100 miles</th>
<th>100-200 miles</th>
<th>200-300 miles</th>
<th>300+ miles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-Up (one-time)</td>
<td>$0 per mile</td>
<td>$0 per mile</td>
<td>$0 per mile</td>
<td>$0 per mile</td>
</tr>
<tr>
<td>Recurring Subscription</td>
<td>$11.00 per mile</td>
<td>$10.00 per mile</td>
<td>$9.60 per mile</td>
<td>$8.00 per mile</td>
</tr>
</tbody>
</table>

NOTE: The pricing per centerline mile model will be used when portions of a data set are desired. For example, if MoDOT elects to purchase Data Set A but only a portion of Data Sets B and C, the subscription rate for the selected segments from Data Sets B and C will be determined using the rates established in the table above. When determining the “total centerline miles subscribed to”, quantities from entire data sets purchased shall be included. For example, if MoDOT elects to purchase Data Set A but only a portion of Data Sets B and C, the “total centerline miles subscribed to” would include the 134.2 miles from

Technical and Fee Proposal | 60 | November 4, 2013 |
Data Set A plus the additional miles desired from Data Set B and C. In the table above, "miles" always refers to centerline miles.

Option 2 – Historical Data Only

<table>
<thead>
<tr>
<th>No.</th>
<th>Data Packages</th>
<th>Start-Up Cost (if applicable)</th>
<th>Recurring Subscription (per month)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data Set E (737.3 miles)</td>
<td>$90,000</td>
<td>$6,800</td>
</tr>
<tr>
<td>2</td>
<td>Data Sets E and F (905.3 miles)</td>
<td>$100,500</td>
<td>$8,500</td>
</tr>
<tr>
<td>3</td>
<td>Data Sets E, F, G (1,122.9 miles)</td>
<td>$167,500</td>
<td>$11,500</td>
</tr>
<tr>
<td>4</td>
<td>Data for the entire state</td>
<td>$145,500</td>
<td>$12,500</td>
</tr>
</tbody>
</table>

Based on the available budget, it may not be feasible for MoDOT to purchase entire data sets. What data is to be purchased apart from the defined packages above, the rates in the table below shall be used.

<table>
<thead>
<tr>
<th>Total Centerline Miles Subscribe To</th>
<th>0-500 miles</th>
<th>500-1,000 miles</th>
<th>1,000-1,500 miles</th>
<th>1,500+ miles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start-Up (one-time)</td>
<td></td>
<td>$0</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td></td>
<td>per mile</td>
<td>per mile</td>
<td>per mile</td>
<td>per mile</td>
</tr>
<tr>
<td>Recurring Subscription</td>
<td>$5.25</td>
<td>$5.00</td>
<td>$4.50</td>
<td>$4.00</td>
</tr>
<tr>
<td></td>
<td>per month</td>
<td>per month</td>
<td>per month</td>
<td>per month</td>
</tr>
</tbody>
</table>

NOTE: The pricing per centerline mile model will be used when portions of a data set are desired. For example, if MoDOT elects to purchase Data Set E but only a portion of Data Set F, the subscription rate for the selected segments from Data Set F will be determined using the rates established in the table above. When determining the "total centerline miles subscribed to", quantities from entire data sets purchased shall be included. For example, if MoDOT elects to purchase Data Set E but only a portion of Data Set F, the "total centerline miles subscribed to" would include the 737.3 miles from Data Set E plus the additional miles desired from Data Set F. In the table above, "miles" always refers to centerline miles.

Technical and Fee Proposal 51 November 4, 2013
RENEWAL PERIODS: The Offeror shall provide below the maximum percentage of increase or
decrease for the renewal periods. The percentage shall be computed against the original contract
period prices for each renewal period. If a renewal percentage is not provided, the prices for the
renewal periods shall be the same as the original contract period.

1<sup>st</sup> Renewal Period 0 ___% of maximum increase and/or 0 ___% of maximum decrease.

2<sup>nd</sup> Renewal Period 0 ___% of maximum increase and/or 0 ___% of maximum decrease.

3<sup>rd</sup> Renewal Period 0 ___% of maximum increase and/or 0 ___% of maximum decrease.

4<sup>th</sup> Renewal Period 0 ___% of maximum increase and/or 0 ___% of maximum decrease.

HERE

[Signature]

Name of the Offeror's Firm

Signature of Authorized Representative

Date Signed

November 4, 2013
EXHIBIT III
HERE DATA LICENSE TERMS

Contract Services Agreement, dated February 21, 2014 between
HERE North America LLC and MoDOT (the “Agreement”)

These License Terms include the following exhibits:

Exhibit A - APPLICATION SCHEDULE NO. 1

Coverage Area: As specified in Exhibit I (Scope of Work) of the Agreement

Authenticated Users: 100 maximum

Term: See Sections (23) Contract Period and (24) Renewal Information of the Agreement

RFP: Request for Proposal No. 131028BR issued by Missouri Dep. of Transportation

Permitted Application: Traffic Information System Application

1. License Grant: HERE grants the Commission a non-exclusive, non-transferable, non-sublicensable license, to use the HERE Data for the Coverage Area (including updates thereto, if applicable) during the term of the Agreement. "Authenticated Users" shall mean individuals to whom the Commission has granted access to use the Permitted Application solely for the Commission’s internal business purposes. Except as expressly provided and authorized in the RFP, the Commission shall not: (i) publish, sell, transfer, disclose or otherwise reveal the HERE Data to any third party, or (ii) copy or reproduce the HERE Data other than to the extent required to exercise the license granted hereunder.

Notwithstanding any language to the contrary in the Agreement, the Commission may not monetize its derivative products and/or reports in which HERE Data is used. Derivative products and/or reports must be made available at no cost.

2. License Fees. See Section 4 of the Agreement and Exhibit I.

3. Ownership & Subpiral Requirements. The Commission acknowledges that HERE and its licensors and suppliers own all intellectual property rights in and to the HERE Data and related documentation. HERE and its licensors and suppliers retain all such rights under this Agreement. Notwithstanding any other provision of this Agreement, the Commission shall comply with any and all requirements and restrictions imposed on HERE by its present and future data licensors and suppliers and other entities. To the extent not already set forth herein, HERE will notify the Commission of such requirements and restrictions.

4. Confidentiality. Each party agrees that all business, technical, financial and other information that it obtains from the other, and marked as “Confidential Information”, is the confidential property of the disclosing party (“Confidential Information” of the disclosing party). Except as expressly and unambiguously allowed herein, or as required or authorized under the Missouri Sunshine Law (Chapter 610 of the Revised Statutes of Missouri), the receiving party will hold in confidence and
not use or disclose any Confidential Information of the disclosing party and shall similarly bind its employees in writing. Upon termination of this Agreement or upon request of the disclosing party, the receiving party will return to the disclosing party or destroy (and certify such destruction) all Confidential Information of such disclosing party, all documents and media containing such Confidential Information and any and all copies or extracts thereof. The receiving party shall not be obligated under this Section with respect to information the receiving party can document: (a) is or has become readily publicly available without restriction through no fault of the receiving party or its employees or agents; or (b) is received without restriction from a third party lawfully in possession of such information and lawfully empowered to disclose such information; or (c) was rightfully in the possession of the receiving party without restriction prior to its disclosure by the other party; or (d) was independently developed by employees or consultants of the receiving party without access to such Confidential Information; or (e) is required to be disclosed by law or order of court of competent jurisdiction.

5. Error Reporting. The Commission shall promptly provide any information it learns concerning errors, problems, complaints, and related matters concerning the HERE Data to HERE, without charge, for HERE's unlimited use, including incorporation into the HERE Data. The Commission shall not retain, acquire or assert any right, title or interest in or to the HERE Data or the Intellectual property rights thereto based on the transfer of such information to HERE or HERE's use or incorporation of such information in the HERE Data or otherwise.

6. Disclaimer. Subject to Section (2)(B), Data Validation, of the RFP, and except as expressly set forth in this Agreement, the HERE Data is provided "as is" and HERE makes no representations or warranties. HERE expressly disclaims any implied warranties or conditions of any kind, including, without limitation, any warranty of or condition of quality, performance, merchantability, fitness for a particular purpose or non-infringement. Except as specifically set forth in this Agreement, HERE does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the HERE Data or any other materials in terms of correctness, accuracy, reliability or otherwise.

7. Limitation of Liability.

7.1 Except as otherwise provided in Sections 7.2 and 7.3 below and to the maximum extent permitted by law, the liability of both parties shall be limited to direct damages only, thus excluding liability for any other damages such as indirect, special, incidental, consequential or punitive damages (including but not limited to lost profits, lost data, lost revenue, lost savings, lost business and loss of goodwill).

7.2 The total liability of HERE with respect to the HERE Data or the performance thereof will be limited exclusively to replacement of the HERE Data or, if in HERE's opinion, replacement is impracticable, a refund of the applicable license fee. Notwithstanding the foregoing, and notwithstanding any failure of the essential purpose of any right or remedy set forth herein, or that might be found or inferred herein, in no event shall HERE's aggregate liability with respect to any matters whatsoever arising under or in connection with the Agreement exceed an amount equivalent to the greatest amount of license fees paid to HERE for any year of this Agreement. The Commission understands that HERE is not responsible for and will have no liability for hardware, software or other items or any services provided by any person other than HERE.

7.3 The limitations set out in this Section 7 shall not limit a party's obligation to indemnify the other under Section 8 below.

7.4 The Commission acknowledges and agrees that the fees and allocation of the risks (as expressed in the indemnities and the limits on warranties, liabilities, damages and remedies) contained herein reflect the economic basis of the Agreement, in the absence of which this Agreement would not have been made.

8. Indemnification.

8.1 Intellectual Property Indemnification. Subject to the Commission's performance of its obligations under this Agreement, HERE shall at its sole option defend or settle at its expense any claim or suit against the Commission arising out of or in connection with an assertion that the
HERE Data infringes any copyrights and HERE shall indemnify and hold harmless the Commission from damages, costs, and attorneys' fees, if any, finally awarded in such suit or the amount of the settlement thereof, provided that (i) HERE is promptly notified in writing of such claim or suit, (ii) HERE shall have the sole control of the defense and/or settlement thereof, and (iii) the Commission furnishes to HERE, on request, all relevant information available to the Commission and reasonable cooperation for such defense. The foregoing in this Section 8.1 shall be the sole obligation of HERE and the exclusive remedy of the Commission with respect to any alleged infringement by the HERE Data of any third party's intellectual property rights. The Commission shall not admit or settle any such claim or suit without the prior written consent of HERE. HERE shall have no obligation under this Section 8.1 if and to the extent that such claim or suit arises from: (1) compliance by HERE with the Commission's specifications, (2) modification of the HERE Data other than by HERE, (3) the combination of the HERE Data with products or services other than those supplied by HERE, (4) the Commission continuing any use of the HERE Data after being notified of any allegedly infringing activity or after being informed of or provided with modifications that would have avoided the alleged infringement, or (5) the Commission's use of the HERE Data that is not strictly in accordance with the license granted under this Agreement.
EXHIBIT A to License Terms

APPLICATION SCHEDULE NO. 1

Territory License No.: 1
Permitted Application(s): Traffic Information System Application

1. Definitions:

"Traffic Information System" means an automated service that is set up by, or with the direction of, the Client and uses at least one Traffic Management Center to provide the general public with information pertaining to traffic (e.g., drive time, incident reports, driving conditions, etc.) through various means accessible to the general public (e.g., IVR phone system, internet site, SMS alerts, mobile phone applications, etc.) at no charge to the public/end users.

"Asset" means a person (including an End-User), animal, device, site, transportation means (e.g., a car, truck or other vehicle) or other mobile or fixed object.

"Map Transaction" means a single raster image depicting a map for a pre-determined or End-User-specified geographical area (but not in any way based on a Sensor-generated location).

"Sensor" means any type of sensor that can be used for determining the location of an Asset (e.g., GPS, triangulation, odometer, compass, gyroscope, accelerometer, etc.)

"HERE Data" refers to real-time and historical traffic data, information and content (but not including other non-traffic dynamic content, such as weather) for certain markets in the Coverage Area as generally made available by HERE, and as specified in Exhibit I (Scope of Work) of the Agreement. All other HERE data and content is not included in the Traffic Information System Application, although it may be licensed for an additional fee.

"Traffic Management Center" or "Traffic Operations Center" refers to a facility that collects and analyzes historical traffic, real-time traffic, and/or other traffic-related information to monitor and manage traffic on a particular transportation network.

A "Website Deployment" refers to a Traffic Information System accessible to the general public/end users via an interactive website that is managed by the Client. A website deployment may also refer to, or include, an email notification or alert system for which the public/end users can setup via the internet. If this deployment/application involves advertising, HERE Data may only be used if all involved parties can agree on the advertising terms. For example, an individual may visit the website to receive route and/or drive time information by providing his/her current location, desired destination, and other relevant information through the website's user interface.

An "IVR System Deployment" refers to a Traffic Information System accessible to the general public/end users via a phone call and has an automated Interactive Voice Response system that is managed by the Client. If this deployment/application involves advertising, HERE Data may only be used if all involved parties can agree on the advertising terms. For example, an individual may call a 1-800 number and be able to receive route and/or drive time information from the fully automated IVR Traffic Information System by providing his/her current location, desired destination, and other relevant information through voice instructions.

A "Mobile Phone Application Deployment" refers to a Traffic Information System accessible to the general public/end users via an application that can be installed on their mobile phones. If this deployment/application involves advertising, HERE Data may only be used if all involved parties can agree on the advertising terms.
For example, an individual may download and install an application on his/her mobile phone and be able to use the application to view a map of major roadways showing traffic level, receive traffic alerts and/or driving directions based on HERE Data.

A 'Dynamic Message Signs Deployment' refers to a Traffic Information System accessible to the general public and users and provides traffic information to drivers via electronic signs/boards that are situated along and visible from major roadways. If this deployment/application involves advertising, HERE Data may only be used if all involved parties can agree on the advertising terms.

For example, ODOT may have Dynamic Message Signs along a busy stretch of a highway to convey to drivers the travel time till a certain point/exit on the highway.
APPENDIX C.3

OREGON DEPARTMENT OF TRANSPORTATION
DATA PRIVACY POLICY

AND

POLICY ADM 08-01 ON PASSIVE ELECTRONIC DATA COLLECTION
DMV POLICY MANUAL

Customer Services
Driver and Motor Vehicle Services

NUMBER
CS-R 0100

SUGGESTED
New

DATE
08-20-2003

PAGE NUMBER
1 of 2

REFERENCE
ORS 802.175-802.191
Oregon Constitution, Article 9, Section 3a, CRS 192.410-192.505.
ORS 802.183, CRS 902.230.
Department of Justice Opinion dated 4/26/88, File #735-100-G0031-88

SUBJECT
DMV RECORDS PROGRAM PRINCIPLES

AUTHORIZATION
/s/ William G. Seely

Policy Statement
DMV will exercise responsible stewardship of the Records Program by maintaining a balance between lawful public access to records information and protecting customer information contained in the records entrusted to DMV by the citizens of Oregon.

Purpose
The purpose of this policy is to communicate DMV’s principles regarding the collection, storage, and disclosure of DMV records and records information maintained by the Records Program.

Guidelines
1. DMV will collect and store only that customer information necessary to conduct DMV business, or that is required by law.
2. DMV will use effective and secure storage methods that comply with the Secretary of State archival standards and record retention schedules.
3. DMV will show consideration for the privacy of DMV customers by ensuring proper disclosure of protected record information. We will disclose protected information to only those requestors qualified to receive it as permitted by the Public Records Law and Oregon’s Record Privacy Law.
4. DMV will establish practices that ensure the least risk of improper disclosure of protected information.
5. DMV will establish and publish standards and common processes for managing external requests for DMV records.
6. DMV will establish practices that aid in the detection and termination of record misuse.
7. DMV will establish practices that ensure employees are aware of and understand their responsibilities and obligations regarding the maintenance and release of protected information in DMV records.
8. DMV will not tolerate internal misuse of protected record information for unauthorized, inappropriate, or illegal use.
9. DMV will ensure that the Highway Fund remains whole by recovering at least the actual cost to provide the record when it is supplied for a non-Highway Fund purpose.
# DMV Policy Manual

## DMV Records Program Principles

**Background**

The Customer Services Group Manager is responsible for the implementation of all records policies created by the service group, as delegated by the DMV Administrator.

The DMV Records Program is part of DMV Customer Services. The Records Program is responsible for ensuring that DMV records are retained and disclosed as required by law and disclosed as required under DMV policy. The Service Group Manager delegates the authority and responsibility for managing the Records Program to the Records Section Manager.

The Records Program maintains protected customer information that is contained in DMV records. Due to the sensitive nature of the information and the need to protect against improper disclosure, a policy is needed that communicates the principles of the Records Program for managing this information.

This policy is intended to foster understanding of the decisions made by the Records Program. These are the underlying principles used by the program to make decisions about any release of records information under its control. The program avoids unnecessary risk to strengthen the integrity of the program, and the declaration of these principles will aid in having those decisions understood.

---

<table>
<thead>
<tr>
<th>Subject</th>
<th>DMV Records Program Principles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reference</td>
<td>ORS 802.175-802.191, Oregon Constitution, Article 9, Section 3e, ORS 192.410-192.565, ORS 802.163, ORS 832.230, Department of Justice Opinion dated 4/26/88, File #735-100-G0031-88</td>
</tr>
<tr>
<td>Number</td>
<td>CS-R 0160</td>
</tr>
<tr>
<td>Status</td>
<td>New</td>
</tr>
<tr>
<td>Effective Date</td>
<td>08-29-2003</td>
</tr>
<tr>
<td>Page Number</td>
<td>2 of 2</td>
</tr>
</tbody>
</table>

/s/ William G. Seely
DMV POLICY MANUAL

DMV
Customer Services
Driver and Motor Vehicle Services

C-51

Policy Statement
DMV considers the information referenced in this policy protected, and will only disclose the information in accordance with the statute, administrative rule, or policy that permits disclosure.

DMV employees may disclose protected information only when doing so is a part of their assigned job duties, or at the direction of their manager.

Purpose
The purpose of this policy is to provide a single reference for all DMV data or records that are in some way restricted from disclosure. The policy includes the release conditions for the information, who is authorized to release the information, and the statute, administrative rule or policy governing disclosure.

Guidelines
DMV employees must be aware of the information DMV considers protected, when the information can be released, and by whom.

The protected information topics can be complex. Whenever there is any doubt about what action to take, employees should seek the advice of their supervisor. If more information is needed, the supervisor should contact the Records Policy Unit Manager.

Policy Matrix

<table>
<thead>
<tr>
<th>Protected Information</th>
<th>Description</th>
<th>DMV Policy Number or Disclosure Conditions</th>
<th>ORS/OAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Name</td>
<td>The (non-business) name associated with an individual on DMV records.</td>
<td>See Policy CS-R0102</td>
<td>ORS 602.175-602.191</td>
</tr>
<tr>
<td>Customer Address</td>
<td>The (non-business) address associated with an individual on DMV records.</td>
<td>See Policy CS-R0102</td>
<td>ORS 602.175-602.191</td>
</tr>
<tr>
<td>Protected Address</td>
<td>The home address of an individual on DMV records that needs protection as the person or their family member(s) safety is in danger.</td>
<td>With a court order, by request of law enforcement, or with the person's permission. Only Records Policy may disclose a protected address.</td>
<td>ORS 192.445</td>
</tr>
<tr>
<td>Driver License, Driver Permit, or Identification Card Number</td>
<td>The Driver License, Driver Permit, or Identification Card Number associated with an individual on DMV records.</td>
<td>See Policy CS-R0102</td>
<td>ORS 602.175-602.191</td>
</tr>
</tbody>
</table>
### DMV POLICY MANUAL

**Customer Services**  
Driver and Motor Vehicle Services

---

**Subject:**  
DMV Protected Data

**Authorizer:**  
/s/ William G. Seely

---

<table>
<thead>
<tr>
<th>Protected Information</th>
<th>Description</th>
<th>DMV Policy Number</th>
<th>ORS/OAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Telephone Number</td>
<td>The telephone number associated with an individual on DMV records.</td>
<td>See Policy CS-R0102</td>
<td>ORS 802.175-802.191</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The e-mail address of a DMV customer.</td>
<td>Disclosed By: The Record Services Unit and &quot;the Records Policy Unit. Disclosure Conditions: Requests for e-mail addresses must be decided on a case by case basis to determine if the address contains personal information. The Records Policy Unit will determine if the information can be disclosed.</td>
<td>ORS 802.175-802.191, ORS 102.502(2).</td>
</tr>
<tr>
<td>Mother's Maiden Name</td>
<td>The Mother's Maiden Name of an individual's mother as shown on DMV records.</td>
<td>See Policy CS-R0103</td>
<td>ORS 192.502(2)</td>
</tr>
<tr>
<td>Place Of Birth</td>
<td>The place of birth of an individual as shown on DMV records.</td>
<td>See Policy CS-R0103</td>
<td>ORS 192.502(2)</td>
</tr>
<tr>
<td>Medical Information</td>
<td>DMV records containing information related to a medical condition of an individual.</td>
<td>See Policy CS-R0105</td>
<td>ORS 192.502(2)(4)</td>
</tr>
</tbody>
</table>
# DMV Policy Manual

## Certificate of Medical Eligibility
A form (##735-6587) used by DMV to determine if a person should be allowed to drive.
- See Policy CS-R0105
- ORS 192.502(2), OAR 735-074

## Reports of Disorders Affecting Consciousness
A form (##735-6834) completed by a physician or health care provider stating that a person has a disorder affecting consciousness.
- See Policy CS-R0105
- ORS 807.710, OAR 735-074

## Protected Information
<table>
<thead>
<tr>
<th>Description</th>
<th>DMV Policy Number or Disclosure Conditions</th>
<th>ORS/OAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory Impairment Referral</td>
<td>See Policy CS-R0105</td>
<td>ORS 807.710, OAR 735-074</td>
</tr>
<tr>
<td>Mandatory Impairment Recertification</td>
<td>See Policy CS-R0105</td>
<td>OAR 735-074</td>
</tr>
<tr>
<td>Drug Test Results</td>
<td>Disclosed By: Record Services Unit Disclosure Conditions: Only with signed permission of the individual whose record is being requested, using Form #735-7195.</td>
<td>ORS 802.202</td>
</tr>
<tr>
<td>Fictitious Vehicle Information</td>
<td>Disclosed By: Not applicable. Disclosure Conditions: The Records Policy Unit will not release this information.</td>
<td>ORS 805.060</td>
</tr>
<tr>
<td>Fictitious Driver License Information</td>
<td>Disclosed By: Not applicable. Disclosure Conditions: The Records Policy Unit will not release this information.</td>
<td>Attorney General Opinion dated March 17th, 1977</td>
</tr>
</tbody>
</table>
DMV POLICY MANUAL

DMV
Customer Services
Driver and Motor Vehicle Services

Subject
DMV PROTECTED DATA

SUPERVISOR

CS-R0101
06-02-2004
08-02-2004

PREPARED
12-01-2006

REVISION

See Policy Matrix

AUTHOR/EDITOR
/s/ William G. Seely

---

DMV Photographs
The photographic representation of a person on a driver license or identification card.

See Policy CS-R0105
ORS 807.115, OAR 735-610-0055.

Oregon Traffic Accident and Insurance Reports/Motor Carrier Crash Reports
Information a party submits to DMV or to Motor Carrier when they have been involved in a reportable accident.

Copies of the report are only available for the confidential use of state enforcement and administrative agencies. Records Policy determines when the reports may be released.

ORS 802.220(5)

<table>
<thead>
<tr>
<th>Protected Information</th>
<th>Description</th>
<th>DMV Policy Number or Disclosure Conditions</th>
<th>ORS/OAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>DMV Knowledge Tests</td>
<td>Tests given for issuance of driving privileges.</td>
<td>Disclosed By DMV does not disclose this information</td>
<td>ORS 192.501(4)</td>
</tr>
</tbody>
</table>

Background

DMV captures and maintains certain customer information that is subject to various levels of protection under the law. Numerous statutes, administrative rules, and policies govern the release of these pieces of information. There is no single document that defines all protected information maintained by DMV, the release restrictions placed on that information, and who is authorized to release it.

This policy identifies every record or data element that is protected in some way, giving employees a convenient reference.

Definitions

In this, and all policies in this series, the following definitions apply:

Protected Information: Customer information of a sensitive nature including name, address, driver license number, telephone number, Social Security Number, mother's maiden name, place of birth, photographs, medical information, protected person information, and law enforcement undercover information.

Personal Information: Name; Address; Driver License, Driver Permit or Identification Card Number; and Telephone Number.
Use: The act of using personal or protected information for purposes permitted in Oregon's Record Privacy Law (ORS 802.175-802.191) and/or Oregon's Public Records Law. (ORS 192.410-192.505)

Disclosure: The act of DMV providing or otherwise making available personal or protected information to persons or entities qualified to receive it under Oregon's Record Privacy Law (ORS 802.175-802.191) and/or Oregon's Public Records Law. (ORS 192.410-192.505)

Re-Disclosure: The act of a person or entity who receives personal or protected information from DMV to make available by re-selling or otherwise providing personal or protected information to another person or entity also qualified to receive it under Oregon's Record Privacy Law (ORS 802.175-802.191) and/or Oregon's Public Records Law. (ORS 192.410-192.505)
DMV POLICY MANUAL

Customer Services Group
Driver and Motor Vehicle Services

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>SUPERVISOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-R 0155</td>
<td>New</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EFFECTIVE DATE</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>06-24-2007</td>
<td>1 of 1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORS 802.175-602.101, ORS 102.502-102.505, CS-R 0107</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SUBJECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>USE OF DMV RECORDS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APPROVAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>/s/ William G. Seely</td>
</tr>
</tbody>
</table>

Policy Statement

DMV employees may not use DMV record information for personal use and may only use record information for authorized business purposes. If an employee needs DMV record information in order to complete a DMV transaction for themselves, a friend or family member, the employee must follow the same process a DMV customer would use to receive the information.

Purpose

The purpose of this policy is to define authorized use of DMV records and make a clear distinction between using records for authorized business purposes and using records for personal use.

Background

DMV maintains driver and vehicle record information of Oregon citizens in order to license drivers and register vehicles. DMV employees have access to this information in order to carry out their official job duties. If an employee needs information about their own record, or if their friends or family members need information about their records, the DMV employee may not access record information for themselves or on behalf of others. This is true even if the employee is accessing their own information or information of someone they know to use as a training or reference example. (See DMV Policy CS-R0107, Accessing Protected Information For Examples, Training, and Reference Materials.)

Definitions (Optional)

Authorized Business Purpose: Those duties that a DMV employee performs as outlined in their position description and/or as otherwise assigned by their supervisor.

Personal Use: Using DMV records for any purpose unrelated to the employee's official job duties or as otherwise outlined in the employee's position description. Personal use includes but is not limited to accessing DMV records about oneself, friends, family members, or other persons to assist with or provide information concerning an individual's record or DMV transaction, out of curiosity, or for unethical or criminal purposes.

Record Information: Any driver or motor vehicle related information contained in DMV hardcopy files, notes, memorandum, or electronically maintained in computer systems.
DMV POLICY MANUAL

Customer Services Group
Driver and Motor Vehicle Services

DMV DATA BREACH POLICY

Policy Statement
Per the requirements of the Oregon Consumer Identity Theft Protection Act, DMV is responsible for the following:

1. Notification of a Security Breach. In the event of a security breach, DMV will notify all affected customers if DMV computer files containing personal information have been accessed via a breach. Notification will occur as soon as possible unless law enforcement determines that notification would impede a criminal investigation.

2. Protection of Social Security numbers. DMV will not print Social Security Numbers on cards or documents that are mailed except as required by law or if the customer has requested information that requires an SSN and is authorized to receive it.

3. Safeguarding Data. DMV will develop, implement and maintain reasonable safeguards to protect the security and confidentiality of customer information including proper disposal of information.

4. The DMV Records Section is responsible for coordinating any notification required in the event of a security breach involving protected customer information and/or subject to the requirements above. Any required notification will be a coordinated effort in cooperation with representatives from each of the Service Groups, the DMV Fraud Prevention Section and DMV's Public Information Officer.

Purpose
The purpose of this policy is to outline DMV's responsibility in the event of a security breach as required by the Oregon Consumer Identity Theft Protection Act.

Background
The Oregon Consumer Identity Theft Protection Act was passed during the 2007 Legislative Session and applies to all businesses, organizations, government agencies, and individuals that collect and maintain personal identifying information. The intent of the law is to ensure the security of customer information and to outline steps that must be taken in the event of a security breach. DMV's Record Section has developed a security plan addressing the requirements of the law as well as a model for responding to breaches.
### DMV POLICY MANUAL

<table>
<thead>
<tr>
<th>NUMBER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>CS-R 0156</td>
<td>New</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EFFECTIVE DATE</th>
<th>PAGE NUMBER</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/21/2007</td>
<td>2 of 2</td>
</tr>
</tbody>
</table>

**REFERENCE**
- Oregon Consumer Identity Theft Protection Act, ORS 902.175-902.191

**S U B J E C T**
- **DMV DATA BREACH POLICY**

**APPROVED SIGNATURE**
- js/ Diane L. Reeves

---

### Definitions

1. **Breach of Security**: Unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information maintained by the person.

2. **Personal Identifying Information**: A person's name in combination with a Social Security number, Oregon driver's license number or Oregon identification card number, financial, credit or debit card numbers along with security or access codes or password that would provide access to a financial account.

Note that the definition of personal information above is from the Oregon Consumer Identity Theft Protection Act. DMV already considers name and drivers license number personal information protected under Oregon's Record Privacy Law (ORS 902.175-902.191) along with address and telephone number.

DMV has additional protections in place for other sensitive customer information including Social Security Number, Mother's Maiden Name, Place of Birth, Photographs, Medical Information, and Drug Test Information. Refer to DMV's Protected Data Policy (CS-R0101) and DMV's Disposal of Paper Waste Policy (CS-R0300) for more information.
APPENDIX C.4

RHODE ISLAND DEPARTMENT OF TRANSPORTATION

TRAFFIC MANAGEMENT POLICY FOR THE DESIGN AND OPERATION OF CLOSED-CIRCUIT TELEVISION IN ADVANCED TRAFFIC MANAGEMENT SYSTEMS
RHODE ISLAND DEPARTMENT OF TRANSPORTATION

TRAFFIC MANAGEMENT

Policy for the Design and Operation of
Closed-Circuit Television (CCTV) in
Advanced Traffic Management Systems

I. Introduction.

The Rhode Island Department of Transportation ("Department") has and is installing closed-circuit television systems ("CCTV systems") along certain state roadways as part of its Intelligent Transportation Systems ("ITS") program. The ITS program includes the use of technology to address transportation needs. The CCTV system is an element of Advanced Traffic Management Systems ("ATM Systems") that allows the Department to manage its roadway system in a manner that maximizes the efficiency of the existing facilities. This is critically important in congested urban areas where it may not be possible or desirable to add roadway capacity.

ATM Systems use technologies such as CCTV systems, traffic detectors and electronic message signs to monitor and collect information on traffic conditions, manage traffic, quickly detect incidents, dispatch the proper response and provide motorists advance notice of congestion, reducing the possibility of secondary accidents and allowing motorists to consider alternate routes, modes or travel times. These systems are run from the Transportation Management Center ("TMC") where managers and operators analyze the input from the field devices, manage traffic via the ATM system elements and coordinate the fastest and best response to the incident.

The use of CCTV cameras is an integral part of this system in Rhode Island as well as throughout the country. The CCTV systems are a valuable source of data, specifically, traffic conditions, and/or traveler information to be provided to the public. Traffic or traveler information is provided to the traveling public to alert them to roadway conditions, incidents ahead or on adjacent roadways, anticipated travel times, congestion, detour recommendations, and advance notice of future roadway condition changes anticipated as a result of special events or roadway construction activities. Accordingly, the Department shares the data with media and traveler information service providers for the purpose of distributing information to the widest audience possible. In this context, CCTV systems are data/information-collecting tools. They must be utilized in a consistent manner that strives to uphold the public's expectation of privacy, while serving their function as a traffic management and traveler information tool.

II. Applicability.

This Policy establishes the manner in which the public’s reasonable expectation of privacy is protected where the Department deploys Closed-Circuit Television Systems as elements of Advanced Traffic Management Systems. This Policy provides principles which will be followed by the Department in the management of Traffic Management Systems.
III. Definitions.

A. "Closed-Circuit Television System ("CCTV system")" shall mean a video camera system and/or network used to collect, transmit and monitor data electronically via a data stream and project such data onto a video monitor, television screen or other monitoring equipment. The CCTV system is a closed circuit in that it has limited access and all elements are directly connected and controlled by authorized operators of the system. Directly connected in this context includes systems linked by microwave, infrared beams, electric wiring, etc.

B. "Advanced Traffic Management Systems ("ATM Systems")" shall mean technologies that collect information, manage traffic, quickly detect incidents, dispatch the proper response and provide motorists advanced notice of congestion, reducing the possibility of secondary accidents and allowing motorists to consider alternate routes, modes, or travel times.

C. "Transportation Management Center ("TMC")" shall mean the central station site for monitoring, analyzing and using the data collected by the Advanced Traffic Management System.

D. "Data" shall mean information collected by a CCTV system, including a live feed or any recording from such, from the Advanced Traffic Management System closed-circuit television system.

E. "Entity" shall mean a private corporation or other private organization, including media or other information service provider, which is duly authorized under an agreement with the Department consistent with this Policy to receive Advanced Traffic Management System data.

F. "Incident" shall mean an activity that occurs on the road, roadway, right-of-way or in proximity to it, such as a vehicular accident, flat tire, fire, or similar situation that has or could have a roadway safety or congestion impact on travel conditions on such roadway.

G. "Personal Identifier Information" shall mean any data that
   i. identifies an individual, drivers or passengers
   ii. identifies license plate of vehicles
   iii. identifies contents of the enclosed interior of passenger vehicles
   iv. tracks the individual travel pattern of a specific vehicle

H. "Public Partner" shall mean any public agency, government, municipality, authority, accredited academic institution or coalition of such bodies that enters into an agreement with the Department for the use of CCTV data consistent with the provisions set forth in this Policy.

I. "Mine/Mining" shall mean any process wherein data containing personal identifier information is collected, manipulated, enlarged, enhanced, analyzed, and/or otherwise used.

IV. Principles.

The planning, design, deployment, operation and maintenance of all CCTV systems deployed by the Department, as elements of ATM System shall conform to the following principles:

A. Privacy.

The individual's right of personal privacy shall be respected and protected. The Department shall consider the protection of personal privacy in all aspects of system planning, design, deployment, operation, and maintenance and shall not collect or disseminate any personal identifier information.
except as set forth herein. CCTV systems shall be used only as needed to perform necessary
transportation planning, traffic management and traveler information functions as defined in this Policy
and shall not be used to monitor persons or private property, except as provided for in VI. A. 1 of this
Policy. In addition, CCTV systems shall not be used to monitor individuals or groups in a
discriminatory manner contrary to applicable state law. The Department shall provide for a level of
privacy consistent with reasonable expectations and the requirements of using CCTV systems for traffic
management and traveler information purposes.
For purposes of this Policy, the Department defines providing for a "reasonable expectation of privacy"
as implementation of CCTV systems design and management and operational procedures, which do
not include the collection of personal identifier information as defined in this Policy, except as
specifically provided for herein. This means that the Department shall take all reasonable efforts to
ensure that CCTV systems shall not be used to collect personal identifier information consistent with
this Policy.

B. Visibility.
The Department shall disclose to the public information regarding the location of cameras.

C. Security/Integrity.
Cameras shall be operated in a wide angle view that does not collect personal identifier information. When
it is necessary to zoom a camera in a way that personal identifier information may be collected,
dissemination of such data should be discontinued until such time as the camera is returned to a view
where personal identifier information is not being collected except as provided in VI. A. 2 and VI. A. 5 of
this Policy.

D. Extent/Use
CCTV systems shall be aimed and focused to collect only the minimum amount of information as
necessary for transportation planning, traffic management and traveler information purposes. CCTV
data shall only be used for the specific purposes set forth in this Policy. The Department may share CCTV
views with other public partners to achieve common transportation objectives in improving transportation
planning, traffic management and traveler information.
Data sharing in accordance with statewide regulations and this Policy will be done to promote the
performance of those functions, and only pursuant to written agreements that provide for the protection
of personal privacy consistent with this Policy. The agreements shall limit use of CCTV data to
prescribed purposes, shall restrict the ability to record, retransmit, enhance or mine data from the
CCTV systems and further preclude knowingly distributing any data that may contain personal identifier
information.
The Department may also distribute CCTV data directly to the public via the internet or other means
for the purpose of providing traveler information. The Department shall take all reasonable efforts to
ensure that any CCTV data disseminated in this manner shall not provide personal identifier information
as previously defined in this Policy. The sole purpose of providing such data shall be for the
dissemination of traveler information to facilitate traffic management and the efficient balancing of
transportation infrastructure demand and supply and all such uses and dissemination shall be consistent
with statewide regulations, and this Policy.

E. Access/Accountability/Retention.
Internal access to data shall be available only to Department traffic operations personnel, agents of the
Department involved in ATM system management, operations and maintenance, and duly authorized
public partners. This will not preclude internal distribution to the general employee population within the
Department of the same data as is available to the public for traveler information purposes via the
internet, media or traveler information service providers.
Access to CCTV and ATM systems shall be controlled by pre-determined administrative and supervisory policies based on design and operational considerations and shall be tracked for adherence to procedures. Disciplinary procedures shall be established to address improper access, data manipulation, mining or data disclosure, as well as for assessment of procedural security. Procedures shall be developed to ensure appropriate training of personnel with access to CCTV systems and other instrumentation with respect to the requirements of this Policy. Data shall not be recorded except in accordance with this Policy.

In all cases, recording shall be done in accordance with this Policy and shall be retained only for the minimum possible time frame after use of the archived data for its intended purpose. Recorded data shall not include personal identifiers unless absolutely necessary to accomplish the intended purpose. Routine archiving of CCTV data shall not be part of the operational procedures. Public access to any temporarily archived CCTV data shall be in accordance with applicable state law.

F. Commercial Use.

CCTV data may be shared with other entities for commercial use in order to provide for the widest distribution of the information to allow travelers to make informed travel decisions. For this purpose, the entity shall be regularly involved in the distribution of traveler information for commercial purposes and provides significant value to the Department in providing for widespread dissemination of traveler information to the public.

The Department shall take all reasonable efforts to ensure that any CCTV data as disseminated to these entities, shall not provide personal identifier information. The sole purpose of providing such data to these entities shall be for the dissemination of transportation information to facilitate traffic management and the efficient use of the transportation infrastructure and all such uses and dissemination shall be consistent with this Policy. Dissemination of data shall only be done by written agreement containing privacy protection language consistent with this Policy. The agreement shall limit the entities use of the CCTV data to prescribed purposes, shall prohibit their ability to enhance, mine, analyze and utilize personal identifier information from the data, shall restrict their ability to record, resell or retransmit the video and further preclude them from knowingly distributing any data that may contain personal identifier information as defined in this Policy. Any agreements entered into by the Department with any other entity shall expressly provide that such agreement will be void if the entity fails to adhere to the privacy protections set forth in this Policy. The Department shall discontinue the sharing of data if the privacy protection criteria are not adhered to.

G. Enforcement.

CCTV systems should be designed and used primarily for the traffic management and traveler information purpose for which they were installed and for which the public would reasonably expect. Enforcement agencies play an important public safety role in incident management activities. Accordingly, the Department partners with enforcement agencies to provide for the best incident management service to the public. As a result, enforcement agencies may have access to CCTV data directly or remotely through the TMC for the purpose of coordinating incident management and incident-related public safety activities. Enforcement agencies shall be responsible for ensuring that any use of the CCTV systems is done in accordance with statutory authority, appropriate legal process, or emergency circumstances as defined by law.
V. Design and Operations Guidelines.

The following principles and guidelines shall apply to the Department's use of CCTV systems on its roadways:

A. TMC Policy Implementation.
1. The TMC manager or designee shall designate a person responsible for the implementation and ongoing compliance with this Policy including monitoring of local system design and operation to accommodate system and technology changes consistent with this Policy.
2. Such person shall be responsible for monitoring research of the latest hardware and software technology for CCTV systems which are consistent with the design of the system, the policies set forth in this Policy, and shall implement into the local CCTV systems such feasible technologies necessary for upholding the principles set forth in this Policy.

B. Deployment of CCTV.
1. The public shall be made aware of projects to initially deploy or significantly expand CCTV systems at a facility, in a corridor or throughout a region in accordance with applicable requirements of this Policy.

C. Location of CCTV System Cameras.
1. Cameras shall be placed to provide the best available viewing of the roadway section, taking into account existing physical restrictions and topography.
2. Cameras should generally be installed in areas of traffic safety concerns and/or traffic congestion.
3. CCTV systems should generally be installed in conjunction with other ATM system elements including variable message signs, highway advisory radio, traffic detectors, etc. to provide for transportation planning, traffic management, and traveler information needs.
4. CCTV system cameras shall not be concealed and shall be installed at locations which provide an open view of the camera from the roadway, except as necessary and in response to accommodating public concern with roadside aesthetics.

VI. Operation of CCTV Systems.

A. CCTV Operations
1. No CCTV system shall monitor persons or private property, provided however, this provision shall not prohibit such monitoring on or adjacent to the roadway or right-of-way where it is not practical to avoid such monitoring during CCTV operation as provided in this Policy, and this provision shall not prohibit such monitoring in the event of a public health danger or safety emergency, and this provision shall not prohibit the viewing of traffic-related conditions in plain view only as necessary for the Department to perform its traffic management activities as provided in this Policy.
2. Personal identifier information data shall not be collected by the CCTV system, except that such data may be collected to provide for the safety of the public, respond to incidents, and the performance of necessary traffic and planning management functions.
3. CCTV systems shall operate in a wide-angle view mode which shall enable operators to view a large segment of the roadway without providing the ability to view any personal identifier information except as provided in Section VI. A. 2 or otherwise provided herein.
4. CCTV systems shall have physical and/or software controls which shall restrict the viewing area to the extent practical to that required for the intended traffic/incident management function.

5. CCTV systems shall only be used in a zoom mode where personal identifier information may be being collected on an exception basis, as defined in this Policy. CCTV systems shall be returned to a view not containing personal identifiers when the need for such zooming has been met.

B. Recording of CCTV System Video.

1. Except as provided for in this Policy, CCTV data shall not be recorded and all data disseminated from CCTV systems shall be transferred in a real time or limited time delay data feed. In all cases, recording shall only be done in a manner that protects the privacy of the public in accordance with this Policy.

2. CCTV data shall only be recorded in response to a specific need where a review of the data would contribute to improving safety and/or future traffic operations procedures or system planning and performance including:
   i. review of a traffic operations or safety problem;
   ii. provision of a training review for future operator training;
   iii. research activities that will improve future technology or operations;
   iv. post-incident review of a particularly complex incident and emergency response for the purposes of improving operational procedures and response;
   v. demonstrating or testing equipment or system functions; or
   vi. collection of data for transportation planning management purposes where personal identifier information is subsequently removed from the data.

3. If a recording is made, it shall be retained in a specifically designed and secure location with access restricted by supervisory level personnel.

4. CCTV system data which have been recorded shall be retained only for the minimum possible time after use of the archived data for its intended purpose.

C. Training and Accountability.

1. All operators shall be trained and certified in the proper operation of the CCTV systems according to the Policy and principles set forth in this Policy. Such certification shall be required before operators are allowed to operate CCTV systems. Operator training shall be maintained as an evolving, continuous process.

2. The TMC shall have a written procedures manual for operation of CCTV systems. This manual shall include the principles and Policy set forth in this Policy, and may either be a part of an overall TMC Operations Manual or a specific CCTV system Operations Manual.

3. All TMC personnel authorized to operate the CCTV system shall be provided with a copy of the operations manual, and verify in writing that they have received it, reviewed it and agree to follow the procedures in the manual.

4. Disciplinary criteria shall be established for personnel who knowingly violate the established CCTV system operations procedures and principles or Policy set forth in this Policy, regardless of the agency or entity by whom they are employed. Department personnel shall be disciplined in accordance with appropriate personnel procedures. Any contracts with firms involving the operation of CCTV for the Department shall include appropriate language requiring conformance with this Policy and identifying an acceptable disciplinary procedure. The disciplinary procedures shall be a part of the TMC or CCTV system operations manual.
VII. Agreements

The Department shall not provide CCTV data containing personal identifier information to any public partner except for the purposes set forth in VI. A.2 and VI. A.5 of this Policy, or to a private entity except for the purposes as set forth in VI. A.2 of this Policy at any time, provided, however that the Department may provide such data, consistent with this Policy, to consultants retained by the Department in the performance of Department functions. The sole purpose of providing such data shall be for the dissemination of transportation information to facilitate traffic management and the efficient use of the transportation infrastructure and all such uses and dissemination shall be consistent with this Policy.

A. No data shall be shared or otherwise disseminated except in accordance with this Policy.

B. Any agreement entered into by the Department with any public partner or entity, except as otherwise provided in this Policy, shall provide that there shall be no dissemination of data containing personal identifier information to any third party without written agreement containing privacy protection language consistent with this Policy. Such agreement shall limit the use of the CCTV data to prescribed purposes consistent with this Policy, and shall prohibit the mining of such data.

C. Any agreements entered into by the Department with any public partner or entity shall expressly provide that the party to such agreement shall no longer receive data if the entity fails to adhere to the privacy protections set forth in this Policy.

D. The Department may terminate any agreement or execution of such agreement that does not conform with the provisions of this regulation.

E. Agreements entered into under this Policy shall provide the Department with complete authority and retain control over the CCTV systems data that is provided to other public partners, entities and the public, including when it shall be made available. Such agreements shall provide that when CCTV systems collect personal identifier information, data feed to any entity shall be discontinued until such time as the CCTV systems is returned to a mode where personal identifier information is not being collected except as provided in VI. A. 2 and VI. A. 5 of this Policy.

F. Agreements entered into under this Policy shall provide that entities receiving data shall not have the right to re-transmit, enhance for personal identification, mine or otherwise modify data containing personal identifier information.

G. All agreements between public partners or entities and third parties for receipt of CCTV data shall be consistent with the privacy restrictions and policies of this Policy.
Traffic Operations Center Control Room

**Policy:** CCTV Etiquette  
**Effective Date:** 01/23/2015  
**Number of Pages:** 2

**Purpose:**  
Establish basic standards and guidelines for use of the CCTV system and software

**Definition:**  
UDOT controls and maintains 900+ cameras throughout the state of Utah. These cameras are used for a variety of reasons. Because of the sensitivity that is possible from camera images throughout the state, particularly those with zoom and pan capability, it is imperative that all users of VCS and any other video control software be educated on the proper use of those cameras. The guidelines below should adequately serve to prevent misuse of this resource.

**Operational Guidelines**  
Misuse of CCTV cameras by any individual will result in strict disciplinary action (including dismissal). Use of CCTV cameras for surveillance or violating the personal privacy of others is considered misuse. UDOT encourages all partner agencies to enforce these policies so that we may maintain high quality standards for use of CCTV cameras.

CCTV will be used to monitor the general travel condition of the roadways when not actively being used for another acceptable purpose as defined in this guideline. Operators will return the cameras to general roadway monitoring positions when not being actively used for another acceptable purpose.

CCTV may be used to monitor police activity. DPS may occasionally request the use of the CCTV to help monitor police activities. This use of the CCTV system is encouraged in support of public safety. They should generally be cleared through the Shift Supervisor or Lead Operator and should not be broadcast to outside destinations, such as the media or the website. If an Operator is unclear on the procedure for a specific request, they will contact the TOC Shift Supervisor. Cameras will not be used to issue citations or aid in any criminal investigation. Accident scenes can and will be monitored to assess traffic situations and determine public safety. Law enforcement agencies can use the cameras to aid in dispatching units, assessing traffic situations or for officer safety.

CCTV images will not be recorded or archived, except for the purposes of engineering studies or for use in training.

Agencies and Media Partners with Viewing Only privileges may select and view any available camera through their Internet website interface. All camera views are also available to the public on UDOT’s UDOTTraffic website.
Traffic Operations Center Control Room

Agencies and Media Partners may request a different camera view for a traffic accident or problem through the Shift Supervisor on duty. If a Supervisor is not available, the Lead Operator may either decide on the request or page a Supervisor or the TOC Manager. Such requests will be accommodated based on the reasonability, current operations workload and other operational needs of the camera.

Live broadcasting of cameras is permitted by the Media by contractual agreement. UDOT Community Relations must approve the rebroadcast of recorded images.

As many cameras as possible shall be displayed on the video wall and large screen projectors for monitoring purposes. Sequences which cycle through roadway segments at reasonable rates shall be used during peak periods to ensure that all sites and sections of the roadway are being monitored. The sequences used should be appropriate for the time of day. At all times when other uses do not require use of the main wall projectors, as many sequences as possible shall be run as long as it is within the monitoring capability of the Operators.

When viewing an incident using the CCTV you should not be able to recognize make and model of vehicles and you should not be able make out the identities of individuals. Whenever there are injuries involved, make sure that the cameras do not in any way show the injured people, turn the camera away if necessary to avoid shots of the injured. Only zoom in to verify the details of an incident, and only keep the camera zoomed in enough to be aware of changes to the scene (i.e. when lanes are blocked or reopened). If the camera must be left zoomed in on the incident, use the camera blocking feature so that the image does not go out to the public.

Operators will, on a regular basis, sweep through the cameras looking for technical problems with cameras and repositioning any that may not have a reasonable view of the roadway, as well as locate and identify any traffic issues such as stalls, debris or unusual congestion.
Traffic Operations Center Control Room

Policy: CCTV Blocking Policy
Effective Date: 07/08/14
Number of Pages: 2

Purpose:
Establish a concrete policy for use of the blocking function available to VCS users. Because content sometimes viewed on UDOT camera’s by operators and other VCS users is sensitive and because video feeds are readily available to multiple entities including mass media organizations, definition of how and when to use the blocking function must be established.

Definition:
The blocking function available through VCS software is available to all VCS users. The blocking function has two options: media and web. The option is available by right clicking any listed camera in VCS and selecting the “block” option.

Camera feeds to media will never be blocked except under two circumstances, outlined in the Operational Procedure section. Our media partners will be responsible for editorial control of the content they provide to the public.

Camera feeds to the web (UDOT’s own website) will be blocked if they are sensitive or graphic in nature. Sensitive or graphic in this document refers to any content that is gruesome, sensational, or has the potential to cause emotional distress for any party.

Operational Procedure:
1. Operators will never block a camera feed to the media UNLESS either of the two following situations occur:
   a. A camera that is malfunctioning or otherwise inappropriate for public consumption for technical reasons. (For example, a malfunctioning camera is pointed at and/or zoomed in on a private establishment like someone’s home)
   b. A direct request from DPS or another law enforcement agency is made for a camera to be blocked. Should operators receive communication from a law enforcement agency requesting a view that would cause an image to become sensitive in nature, the operator will ask the requesting party if the image should be blocked for privacy concerns. Should a camera need to be blocked the operator should proceed with camera repositioning to remove sensitive content from view.

2. Operators will block camera feeds distributed to the web if images are sensitive in nature. If an operator determines that an image is sensitive in nature, the camera
Traffic Operations Center Control Room

should be repositioned to an acceptable view. If the image is needed for incident response by either the control room or dispatch operators should use VCS software control to block the image from the web. This is done by right clicking any camera feed in VCS and selecting the "block" option, followed by placing a checkmark in the "web" box but not the "media" box.

Operators should use camera control functions to minimize the capture of graphic or sensitive images. Operator function is primarily traffic control and camera angles and viewing should represent the traffic control role. In cases where sensitive or graphic images are important for traffic control, or are requested by law enforcement, camera blocking will occur as listed above.
APPENDIX C.6

UTAH DEPARTMENT OF TRANSPORTATION

PRIVACY PROTECTION FOR BLUETOOTH/WI-FI TIMES
Privacy Protection Plan for Bluetooth/Wi-fi Travel Times

Prepared by Glenn Blackwelder, October 2013

UDOT’s Executive Director, Carlos Braceras has challenged us to ensure that we have procedures, processes, documentation and controls in place to ensure that we are able to protect driver’s privacy when using Bluetooth or Wi-fi to generate travel times. This document lays out our plan for protecting driver’s privacy.

Executive Summary
Travel times can be measured using the unique identifiers (MAC addresses) broadcast by cell phones and other devices that use Wi-fi or Bluetooth. This is a simple, inexpensive way to measure travel times, but there are privacy concerns regarding how this information is handled. A plan is needed to protect driver privacy. Here are our findings:

- A sufficiently tech-savvy and privacy concerned driver can shut off Wi-fi and Bluetooth on their device. However, this is inconvenient and many drivers are unaware of how to do this.
- It is possible to secure the data against unauthorized access through encryption and network security.
- The data can be stored in a manner that disconnects the individual MAC addresses from the data. This means that the data can be used for travel analysis (and requested under GRAMA) without privacy concerns.
- UDOT can be required via court order to track MAC addresses through the system. At this point, two things happen:
  - Privacy protection for individuals is determined by the courts, not UDOT.
  - UDOT would only have data collected after the court order to retain it.

Our conclusion is that with appropriate safeguards, UDOT can protect driver privacy. The only situation where UDOT will release MAC addresses is when required to do so by an appropriate legal authority. We recommend that UDOT implements Bluetooth/Wi-fi travel time measurement - the privacy issues can be addressed, and the technology allows us to generate travel times at a fraction of the cost and more effectively than other technologies.

System Outline
Bluetooth/Wi-fi can be used to measure travel times by using MAC addresses to uniquely identify devices such as cell phones when they pass a detection point and noting when they pass a second detector. The time between the detections is the travel time between the two points.
Privacy Protection Plan for Bluetooth/Wi-fi Travel Times October 2013

The other valuable data that can be gleaned from this system is origin-destination information. For instance, if we have multiple routes through the system we can place detectors at both ends, and on the alternate routes to determine what percentage of traffic detected at both ends took each route.

The Bluetooth readers currently in use by UDOT's Regions use central systems that belong to the field device manufacturers. MAC addresses are passed from the devices in the field to the central servers (UDOT does not retain any record of the MAC addresses in our servers), and the provider returns a data feed identifying the travel time between the field devices.

Privacy Concerns
The privacy concern here is that the unique identifiers (MAC addresses) used to track vehicles through the system can be tied back to an individual in order to demonstrate positively where someone was at a given time. To generate a travel time, UDOT will use a unique identifier for each Bluetooth or Wi-fi device that passes – we cannot measure travel times unless we can re-identify a vehicle farther down the road.

There are three potential avenues for MAC addresses or other identifying information to leave UDOT's custody.

- A GRAMA request or subpoena that requires the information
- A breach of UDOT's ATMS network and interception of MAC addresses
- A UDOT or DTS employee with access to the ATMS network improperly accesses the data.

The remainder of this document addresses the concerns regarding how the MAC addresses will be handled.

Lifecycle of a MAC Address
This section will review how MAC addresses are handled.

1. Detection – MAC addresses will be detected in the field, and will be encrypted at the point of detection.
2. Encryption – there are several acceptable methods for this, either using a salted hash function at the point of detection, or establishing a secure encrypted connection between the point of detection and the database.
3. The encrypted data is transmitted to a central location for processing. UDOT may do this on our servers, but more likely we will use a contractor provided processing service.
4. Processing and Storage of MAC addresses – MAC addresses will be modified prior to processing and storage by use of a salted hash function with regularly changing salt (or some other equivalent process).
   a. Salted Hash Function – a hash function is a cryptographic function that changes a string of data into another string of data as a repeatable, but non-reversible process. A salted hash function takes the item to be hashed and adds "salt", which is another string of
text. To find a matching MAC address, simply treat the second MAC address with the
same salt and hash function and compare.

b. Salt - the salt value will be changed once a day (probably at 2 a.m.). The prior salt value
will be deleted and overwritten with a new randomly generated value. At this point,
we cannot take a known MAC address and find historical matches for that MAC address.

5. The salted hashed addresses can be stored indefinitely because there is no way to match them
to a known MAC address. In addition, because the hash values for any given MAC address
can change daily, the database is not susceptible to analysis that reveals a daily travel pattern for a
given hashed MAC address.

Example Hash

Cryptographic Hash Functions are mathematical operations that take a data string and return a
fixed length value (called a hash) that is reproducible, but is also a one-way transaction. So, if we
take a MAC address such as 24:AB:31:F6:38:26 and run it through the MD5 hash algorithm, we get
69b695652e02006f0bba3df5c7519. This string is always the same for 24:AB:31:F6:38:26, but
there is no way to take 69b695652e02006f0bba3df5c7519 and do a mathematical operation to
get back to the MAC address.

However, this doesn't protect someone with a known MAC address – to track 24:AB:31:F6:38:26
just hash it and compare it to the recorded hash values. The way around this is to add salt to the
hash. A random number generator can be used to generate salt – in this case 372. So we add salt
by doing the MD5 hash of 24:AB:31:F6:38:26:372, which is ba76e5cc799845950c11531e009680c.
And as long as the salt is 372, we can match MAC addresses and get travel times. However, if the
salt changes every 24 hours and the old salt is deleted - then we can match MAC addresses to
measure traffic or look at origin/destination patterns within each 24 hour period, but we can't tell
which specific phone we're looking at.

Privacy of System as Designed

With the system functioning as designed, here are the safeguards against privacy loss, starting with the
most general and ending with the specific elements:

- User imposed safeguards –
  - Bluetooth/Wi-fi can be turned off: It may not be immediately obvious, or widely known,
    but a user can turn off the features that broadcast a MAC address
  - No Comprehensive MAC Address/Personal Information Database: It's hard to get from
    a MAC address to a person – UDOT is not aware of a current database of all MAC
    addresses tied to the owner of each device.
- UDOT Imposed safeguards – System Design

UDOT Traffic Management Division
Privacy Protection Plan for Bluetooth/Wi-fi Travel Times  

- Encryption of MAC addresses at the field device: "raw" MAC addresses are never transmitted, so they cannot be intercepted. To get the raw address, a hacker would have to intercept it within the individual devices.

- Salt and hash the MAC addresses prior to processing and storage. Before hashing the MAC address add "salt" — a string of random information. This starts the process of breaking the connections between MAC addresses and the data UDOT or its contractors store.

- Change the salt daily and delete the old salt. By doing this, UDOT eliminates our ability to take a known MAC address and match it against other values in the database. We also remove the situation where it is possible to follow a hashed MAC address across multiple days. In exchange for this security, we will not be able to track vehicles on the system across the daily change in salt. By choosing a less critical time of day (2 a.m.), UDOT minimizes the impact of this loss of capability.

- UDOT imposed safeguards – contracts and procedures
  - In our contracts with vendors, apply all appropriate DTS standards and practices to secure information.
  - In our contracts, reserve all rights to data collected in our right-of-way but housed on vendor’s servers. That is, the vendor cannot release the data without our approval (or an appropriate legal order).

- UDOT imposed safeguards – policy
  - Proposed Policy Language
    - Within 48 hours of a MAC address being detected, UDOT and/or their contractors will perform operations on the data such that a MAC address cannot be connected to the hashed or encrypted data in UDOT or contractor databases.
  - The proposed policy language does not say that UDOT will give up the trip data, rather that the trip data will be permanently disconnected from any association with MAC addresses.

Attacks on the System

It is said nothing is foolproof. There are some potential ways to attack this system; however the difficulty of carrying these out is far more difficult than the alternate methods of obtaining this information, which is to simply hide a Wi-fi/Bluetooth reader somewhere near the road. There are several potential ways for non-approved access of information from this system:

- Intercept MAC addresses internal to the field devices.
- Intercept the encrypted MAC addresses as they are transmitted and break the encryption.
- If the MAC addresses are hashed and salted on the server and not in the field, there is a chance to intercept them on the server.

These methods involve breaking into UDOT or our contractor’s network. The UDOT ATMS network is a private network, isolated from the internet. In addition to isolation, the system is managed by DTS to
incorporate the latest security standards as determined by DTS. DTS works actively to secure this system against any type of attack.

Once the data leaves the ATMS network, our contracts with vendors will be written to require the latest standards set by DTS to ensure the proper handling of private information. The privacy concerns here are similar to the handling of credit card information. DTS uses industry standard protocols when writing contracts with third party vendors dealing with credit card information, and will base the handling of MAC addresses on similar protocols.

**GRAMA and Court Orders**
The system as designed does not retain links between the MAC address and the hashed form of the MAC address. Any request for UDOT's data will provide a lot of information about the performance of the system, and driver routing choices, but will not provide a method to identify an individual driver. As a result, UDOT should be comfortable providing the information to anyone who wants it.

When it becomes known that UDOT has this system, there is a possibility that we may be asked to use our system to track known MAC addresses via a court order in a criminal investigation. With the system as laid out in this document, UDOT would not be able to provide past information, but would be able to provide information going forward. This could be done several ways:

- Turn off encryption and keep the MAC addresses
- Keep encryption on and save the salt values – which would allow us to check for known MAC addresses in the database. Ideally UDOT wouldn’t save the salt values, but would transmit them daily to the law enforcement entity along with the database of encrypted MAC addresses.
- Have law enforcement provide UDOT with the known MAC addresses and separate them out when they are read and provide a report on those addresses only.

In any case, UDOT could be required to use our system to track users travel through the system at the discretion of the courts.

**Acknowledgments**
I would like to thank the following people for their input on this document. Each of these people has reviewed the document and has provided input and concurs with the findings.

- David Bernard, UDOT’s state agency council
- Jimmy Hofeltz, Director of UDOT’s fiscal audit and his staff
- Rudy Zamora, DTS
- Chuck Felice, Traffic Management Division Software Manager
- Rob Clayton, Traffic Management Division Director
APPENDIX C.7

UTAH DEPARTMENT OF TRANSPORTATION

AGREEMENT BETWEEN UTAH DOT AND DIGIWEST LLC
STATE OF UTAH CONTRACT

1. CONTRACTING PARTIES: This contract is between the following agency of the State of Utah:
   Department Name: Department of Technology Services (UDOT), Agency Code: 316, and the Department of
   Transportation, referred to as (STATE), and the following CONTRACTOR:

   Digivers LLC
   Name: 
   610 SW Alder ST 700
   Address: 
   Portland, OR 97206
   City: State: OR

   Contract Person: Paul White
   Phone: Email: paulwhite@igov.com
   Vendor #: 009901497
   Commodity Code: 050110, 59491, 33682, 5509

2. GENERAL PURPOSE OF CONTRACT: The general purpose of this contract is to provide hardware, software, and hosted backend services to an in-service traffic management. For additional information, see Attachment B: Scope of Work, Contract Pricing, and Contract Payments.

3. PROCUREMENT: This contract is entered into as a result of the procurement process under UDM 8, OSHA, FY 14
   Bid: DOT14-JSPT or a preapproved sole source authorization (from the Division of Purchasing) in accordance with Utah
   Code Title 72.

4. CONTRACT PERIOD: Effective Date: 07/15/2014, Termination Date: 07/14/2017. Unless terminated early or extended in accordance with the terms and conditions of this contract. Renewal options (if any): two (2) years. All payments under this contract will be completed within 40 days after the Termination Date.

5. CONTRACT COSTS: CONTRACTOR will be paid a maximum of $3. Requirements for costs authorized by this contract. Additional information regarding costs: see Attachment B: Scope of Work, Contract Pricing, and Contract Payments.

6. ATTACHMENT A: State of Utah Standard IT Terms and Conditions
   ATTACHMENT B: Scope of Work, Contract Pricing, and Contract Payments
   ATTACHMENT C: Special Terms and Conditions

   Any conflicts between Attachment A and other Attachments will be resolved in favor of Attachment A. C then B.

7. DOCUMENTS INCORPORATED INTO THIS CONTRACT? BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Idaho State Procurement Code, Procurement Rules, and CONTRACTOR's response to Bid # DOT14-JSPT dated 07/03/2014.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

STATE

[Signature] [Date]
Paul White

[Signature] [Date]
Paul White, Director of Operations

[Signature] [Date]
Executive Director, DTS / CIO

[Signature] [Date]
UDOT Title 72

[Signature] [Date]
Director, Division of Finance

[Signature] [Date]
[Title] [Date]
ATTACHMENT A
STATE OF UTAH STANDARD INFORMATION TECHNOLOGY TERMS AND CONDITIONS
(FOR DTS RELATED CONTRACTS ONLY)

1. AUTHORITY: Provisions of this contract are pursuant to the authority set forth in 63G-6, Utah Code, as amended, Utah State Procurement Rules (Utah Administrative Code Sections 801), and related statutes which permit the State to purchase certain specified services, and other approved purchases for the State.

2. CONTRACT JURISDICTION, CHOICE OF LAW, AND VENUE: The provisions of this contract shall be governed by the laws of the State of Utah. The parties will submit to the jurisdiction of the courts of the State of Utah for any dispute arising out of this Contract or the breach thereof. Venue shall be in Salt Lake City, in the Third Judicial District Court for Salt Lake County.

3. LAWS AND REGULATIONS: The Contractor and any and all suppliers, services, equipment, and construction furnished under this contract will comply fully with all applicable Federal and State laws and regulations, including applicable licensing and certification requirements.

4. RECORDS ADMINISTRATION: The Contractor shall maintain, or supervise the maintenance of all records necessary to properly account for the payments made to the Contractor for costs authorized by this contract. These records shall be retained by the Contractor for at least four years after the contract terminates or until all audits initiated within the five years, have been completed, whichever is later. The Contractor agrees to allow State and Federal auditors, and State Agency Staff access to all the records to this contract, for audit and inspection, and monitoring of services. Such access will be during normal business hours, by appointment.

5. CERTIFY REGISTRATION AND USE OF EMPLOYMENT "STATUS VERIFICATION SYSTEM": The Status Verification System, also referred to as "E-verify", only applies to contracts issued through a Request for Proposal process, and to sole sources that are included within a Request for Proposal. It does not apply to other types of procurement processes, including but not limited to invitations for bids or to Multiple Stage Bids.

1. Status Verification System
(1) Each officer and each person signing on behalf of any officer certifies as to his own entity, under penalty of perjury, that the named Contractor has registered and is participating in the Status Verification System to verify the work eligibility status of the contractor's new employees that are employed in the State of Utah in accordance with applicable immigration laws including UCA Section 59A-12-302.
(2) The Contractor shall ensure that the following provisions be placed in each subcontract at every tier: "The subcontractor shall certify to the main (prime or general) contractor by affidavit that the subcontractor has verified through the Status Verification System the employment status of each new employee of the respective subcontractor, all in accordance with applicable immigration laws including UCA Section 59A-12-302 and to comply with all applicable employee status verification laws. Such affidavit must be provided prior to the notice to proceed for the subcontractor to perform the work."
(3) The State will not consider a proposal for award, nor will it make any award where there has been non-compliance with this Section.
(4) Manually or electronically signing the Proposal is deemed the Contractor's certification of compliance with all provisions of this employment status verification certification required by all applicable status verification laws including UCA Section 59A-12-302.

2. Indemnity Clause for Status Verification System
(1) Contractor (including, but not limited to any Contractor, Design Professional, Designer or Consultant) shall protect, indemnify and hold harmless, the State and its officers, employees, agents, representatives and anyone that the State may be liable for, against any claims, damages or liability arising out of or resulting from violation of the above Status Verification System Section whether violated by employees, agents, or contractors of the following: (a) Contractor; (b) Subcontractor at any tier; and or (c) any entity or person for whom the Contractor or Subcontractor may be liable.
(2) Notwithstanding Section 1. above, Design Professionals or Designers under direct contract with the State shall only be required to indemnify the State for a liability claim that arises out of the design professional's services, unless the liability claim arises from the Design Professional's negligent act, wrongful act, error or omission, or other liability imposed by law except that the design professional shall be required to indemnify the State in regard to subcontractors or subconsultants at any tier that are under the direct or indirect control or responsibility of the Design Professional, and includes all independent contractors, agents, employees, or anyone else for whom the Design Professional may be liable at any tier.

6. CONFLICT OF INTEREST: Contractor represents that none of its officers or employees are officers or employees of the State of Utah, unless disclosed has been made in accordance with 19-16-6, Utah Code, as amended.

7. CONFLICT OF INTEREST WITH STATE EMPLOYEES: In addition to the provisions of State of Utah Terms and Conditions # 6, Conflict of Interest, the Contractor certifies that no person in the State's employment, directly or through subcontract, will receive any private financial interest, direct or indirect, in the contract. The Contractor will not hire or subcontract with any person having such conflicting interest.

8. CONTRACTOR, AN INDEPENDENT CONTRACTOR: The Contractor shall be an independent contractor, and as such, shall have no authority, express or implied, to bind the State to any agreements, settlements, liabilities, or understanding whatsoever, and agrees not to perform any acts as agent for the State, except as herein expressly set forth. Compensation stated herein shall be the total amount payable to the Contractor by the State. The Contractor shall be responsible for the payment of all income tax and social security amounts due as a result of payments received from the State for these contract services. Persons employed by the State and acting under the direction of the State shall not be deemed to be employees or agents of the Contractor.

9. CONTRACTOR ACCESS TO SECURE STATE FACILITIES, DATA, AND TECHNOLOGY / CRIMINAL CONVICTION INFORMATION / FORMER POLICE: Any agents or employees, and the agents and employees of a subcontractor (if any) are required to complete federal criminal background check, in accordance with DTS Policy 2000-0014 Background Investigations. If they will (A) enter upon secure premises controlled, held, leased, or occupied by the State, B) have access to, maintain, or develop any hardware, software, State of Utah IT Contract - Digwit LLC - Attachment A
A federal criminal background check may be completed by the Contractor (at its own expense) and the results provided to the State, or the Contractor may provide the State with sufficient personal information (at its own expense) to that one may be completed by the State at State expense. Contractor will provide results of said background checks before work is started by the agent or employee and said background check must have been completed within the two years prior to the contract effective date. The Contractor will notify the State of any negative result (such as conviction of a felony) found during the agent or employee's background check. The State reserves the right to conduct additional background checks on agents or employees whose provided background checks were deemed out of compliance with State standards. If an additional background check is needed, the Contractor will provide the State with sufficient personal information (at its own expense) for a federal criminal background check to be completed, at State expense, on such personnel by the State. "Sufficient personal information" about its agents or employees, and the agents and employees of its subcontractors (if any) means for the Contractor to provide to the State Project Manager, in advance of any work, a list of the full names of the designated employees, including their: social security number, drivers license number and the state of issuance, and their birth date. Thereafter, one week prior to starting work, each contractor employee shall be fingerprinted by the State, and the State is authorized to conduct a federal criminal background check based upon those fingerprints and personal information provided. The State will use this same information to complete a Name Check in the Utah Criminal Justice Information System (UCJIS) every two years and reserves the right to revoke any access or security rights granted in the event of any negative results. Contractor, in exercising any duty or exercising any right under this contract, shall not cause or permit any of its agents or employees, and the agents and employees of their subcontractors (if any) who have been convicted of a felony and misdemeanor other than minor misdemeanors at A) enter upon State premises controlled, held, leased, or occupied by the State, B) have access to, maintain, or develop any hardware, software, firmware, or any other technology, that is used by the State, or C) have access to or receive any State Data. A felony and misdemeanor are defined by the jurisdiction of the State of Utah, regardless of where the conviction occurred. Upon request, DTS agents to provide Contractor with a copy of the latest version of the DTS Policy 2000-0014 Background Investigations.

10. DRUG-FREE WORKPLACE: The Contractor agrees to abide by the Department of Technology Services (DTS) drug-free workplace policies while on State of Utah premises. DTS will provide the Contractor with a copy of these written "drug-free workplace policies" upon request.

11. CODE OF CONDUCT: When Contractor employees are working on-site, the Contractor agrees to follow and enforce DTS Policy 2000-0001 Code of Conduct. If Contractor is working at facilities controlled by other State agencies, Contractor agrees to follow and enforce the Code of Conduct Policy of those other State agencies when Contractor is providing services at those facilities under provisions of this contract. The Contractor will assure that each employee or volunteer under Contractor's supervision receives a copy of each Code of Conduct, and a signed statement to this effect must be in each Contractor or subcontractor employee supervisor's file and is subject to inspection and review by the State. Contractor will provide a copy of any applicable code of conduct. If a Contractor or Subcontractor is working at any State agency which has a Code of Conduct applicable to this Contract, the DTS Project Manager will provide the Contractor with a copy of the Contractor's on-site contract services performance.

12. INDEMNITY CLAUSE: The Contractor agrees to indemnify, save harmless, and release the State of Utah, and all its officers, agents, volunteers, and employees from and against any and all loss, damage, injury, liability, suit, and proceedings arising out of the performance of this contract which are caused in whole or in part by the acts or negligence of the Contractor's officers, agents, volunteers, or employees, but not for claims arising from the State's sole negligence. The parties agree that if there are any Limitations of the Contractor's Liability, including a limitation of liability for anyone for whom the Contractor is responsible, such Limitations of Liability will not apply to injuries to persons, including death, or to damages to property.

13. EMPLOYMENT PRACTICES CLAUSE: The Contractor agrees to abide by the provisions of Title VII and VII of the Civil Rights Act of 1964 (29 USC 2000e et seq) which prohibits discrimination against any employee or applicant for employment or any applicant or recipient of services, on the basis of race, color, religion, or national origin, and further agrees to abide by Executive Order No. 11246, as amended, which prohibits discrimination on the basis of sex; 42 CFR 89 which prohibits discrimination on the basis of age and Section 504 of the Rehabilitation Act of 1973, as amended, which prohibits discrimination on the basis of disabilities. Also, the Contractor agrees to abide by Utah's Executive Order, dated December 13, 2005, which prohibits sexual harassment in the work place.

14. SEPARABILITY CLAUSE: A declaration by any court, or any other binding legal source, that any provision of this contract is illegal and void shall not affect the legality and enforceability of any other provision of this contract, unless the provisions are mutually dependent.

15. RENEGOTIATION OR MODIFICATION: This contract may be amended, modified, or supplemented only by written agreement to the contract, executed by authorized persons of the parties hereto, and attached to the original signed copy of the contract. Automatic renewals will not apply to this contract.

16. DEBARMENT: The Contractor certifies that neither it nor its principals are presently or have ever been disbursed, suspended, proposed for disbarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract), by any governmental department or agency. If the Contractor cannot certify this statement, attach written explanation for review by the State. The Contractor must notify the State Director of Purchasing within 30 days if disbursed by any governmental entity during the contract period.

17. TERMINATION: Unless otherwise stated in the Special Terms and Conditions, this contract may be terminated, with cause by either party, in advance of the specified termination date, upon written notice being given by the other party. The party in violation will be given ten (10) working days after notification to correct and cease the violations, after which the contract may be terminated for cause. This contract may be terminated without cause, in advance of the specified expiration date, by either party, upon sixty (60) days prior written notice being given the other party. On termination of this contract, all accounts and payments will be processed according to the financial arrangements set forth herein for approval services extended date of termination. In the event of such termination, and professional services apply to the contract, the Contractor shall be compensated for services properly performed under this contract up to the effective date of the notice of termination. The Contractor agrees that in the event of such termination for cause or without cause, Contractor's sole remedy and monetary recovery from the State is limited to full payment for all work properly performed.
performed as authorized under this Contract up to the date of termination as well as any reasonable notices issued as a result of the Contractor having to terminate contracts necessarily and appropriately entered into by the Contractor pursuant to this Contract. Contractor further acknowledges that in the event of such termination, all work product, which includes but is not limited to all manuals, forms, contracts, schedules, reports, and any and all documents produced by Contractor under this Contract up to the date of termination, are the property of the State and shall be promptly delivered to the State.

18. SUSPENSION OF WORK: Should circumstances arise which would cause the State to suspend the work, but not terminate the contract, this will be done by formal notice. The work may be reinstated upon advance written notice from the State.

19. NONAPPROPRIATION OF FUNDS, REDUCTION OF FUNDS, OR CHANGES IN LAW:

19.1 Upon written notice delivered to the Contractor, this contract may be terminated in whole or in part at the sole discretion of the State, if the State reasonably determines that a change in Federal or State legislation or applicable laws materially affects the ability of either party to perform under the terms of the contract.

19.2 Upon written notice delivered to the Contractor, this contract may be terminated in whole or in part, or the services and purchase obligations of the State proportionately reduced, at the sole discretion of the State, if the State reasonably determines that a change in applicable funds affects the State’s ability to pay under the contract. A change of available funds as used in this paragraph, includes, but is not limited to, a change in Federal or State funding, whether as a result of a legislative act or order by the President or the Governor.

19.3 If a notice is delivered under paragraph 1 or 2 of this Section 19 “NONAPPROPRIATION OF FUNDS, REDUCTION OF FUNDS, OR CHANGES IN LAW,” the State will immediately terminate the Contractor for products properly delivered or services properly performed up until the effective date of said notice. The State will not be liable for any performance, commitments, penalties, or liquidated damages that accrue after the effective date of said notice.

19.4 Notwithstanding any other paragraph or provision of this Section 19 “NONAPPROPRIATION OF FUNDS, REDUCTION OF FUNDS, OR CHANGES IN LAW,” if the State in said notice to the Contractor indicates that the Contractor is in immediately cease from placing any orders or commitments with suppliers, subcontractors or other third parties, the Contractor shall immediately cease such orders or commitments upon receipt of said notice and the State shall not be liable for any such orders or commitments made after the receipt of said notice.

20. SALES TAX EXEMPTION: The State of Utah’s sales and use tax exemption number is 117055850-016-RTC, located at http://purchasing.utah.gov/contract/documents/sales Consumption Form.pdf. The tangible personal property or services being purchased are being paid from State funds and used in the exercise of that entity’s essential functions. If the items being purchased are construction materials, they will be converted into real property by employees of the government entity, unless otherwise stated in the contract.

21. WARRANTY: The Contractor agrees to warrant and assume responsibility for all products (including hardware, firmware, and software products) that it licenses, contracts, or sells to the State of Utah under this contract for a period of one year, unless otherwise specified and mutually agreed upon elsewhere in this contract. The Contractor (seller) acknowledges that all warranties granted to the buyer by the Uniform Commercial Code of the State of Utah apply to this contract. Product liability disclaimers and/or warranty disclaimers from the seller are not applicable to this contract unless otherwise specified and mutually agreed upon elsewhere in this contract. In general, the Contractor warrants that:

1) The product will do what the solicitation response said it would do,
2) The product will live up to all specific claims that the manufacturer made in their solicitation response,
3) The product will be suitable for the ordinary purposes for which such product is used,
4) The product will be suitable for any special purpose that the State has relied on the Contractor’s skill or judgment to consider when it advised the State about the product,
5) The product has been properly designed and manufactured, and
6) The product is free of significant defects or unusual problems about which the State has not been warned. Remedies available to the State include the following: The Contractor will repair or replace at its cost the products which malfunction is discovered and made known to the Contractor in writing. If the repaired and/or replaced product proves to be inadequate, or fails of its essential purpose, the Contractor will refund the full amount of any payments that have been made. Nothing in this warranty will be construed to limit any rights or remedies the State of Utah may otherwise have under this contract.

22. SECURE PROTECTION AND HANDLING OF DATA:

1. Network Security: Contractor agrees at all times to maintain network security that - at a minimum - includes: network firewall protection, intrusion detection systems, and regular third party penetration testing. Likewise Contractor agrees to maintain network security that conforms to one of the following:

   a. Those standards of the State of Utah apply to its own network, found defined in DTS Policy #800-5.00 Enterprise Information Security Policy (copy available upon request)

   b. Current standards set forth and maintained by the National Institute of Standards and Technology, includes those at http://nvd.nist.gov/nvdsecpubs/SpecialPublicationsNISTSP800-51a.pdf or

   c. Any generally recognized comparable standard that Contractor applies to its own network and approved by DTS in writing.

2. Data Security: Contractor agrees to protect and maintain the security of the State of Utah data with protection that is at least as good as or better than that maintained by the State of Utah. These security measures include but are not limited to maintaining secure environments that are patched up to date with all appropriate security updates as designated, (e.g., Microsoft Notice).

State of Utah IT Contract - Didgwest LLC - Attachment A
3. Data Transmission: Contractor agrees that any and all transmission or exchange of system application data with the State of Utah and/or any other parties expressly designated by the State of Utah, shall take place via secure means, (e.g. HTTPS or IPS).

4. Data Storage: Contractor agrees that no State of Utah data at any time will be processed on or transmitted to any portable or laptop computing device or any portable storage medium, unless such medium is part of the Contractor's designated backup and recovery process.

5. Data Encryption: Contractor agrees to store all State of Utah backup data as part of its designated backup and recovery process in encrypted form, using no less than 128 bit key.

6. Password Protection: Contractor agrees that any portable or laptop computer that has access to a State of Utah network, or stores any non-public State of Utah data is equipped with strong and secure password protection.

7. Data Re-Use: Contractor agrees that any and all data exchanged shall be used expressly and solely for the purpose enumerated in this Contract. Contractor further agrees that no State of Utah data of any kind shall be transferred, exchanged or otherwise passed to other Contractors or assigned parties except on a case-by-case basis as specifically agreed to in writing by DTS.

8. Data Destruction: The Contractor agrees that upon termination of this Agreement it shall erase, destroy, and render unaccountable all State of Utah data from all non-state computer systems and backups, and certify in writing that these actions have been completed within 30 days of the termination of this Agreement or within 7 days of the request of DTS, whichever shall come first.

23. NOTIFICATION AND DATA BREACHES: Contractor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other events requiring notification in accordance with DTS Policy 3900-002 Enterprise Information Security Policy (copy available upon request). In the event of a data breach of any Contractor's security obligations or other event requiring notification under applicable law (Utah Code § 13-14-101 thru 391 et seq), Contractor agrees at its own expense to assume responsibility for informing all such individuals in accordance with applicable laws and to indemnify, hold harmless and defend the State of Utah against any claims, damages, or other harm related to such Notification Event.

24. CHANGE MANAGEMENT: Contractor agrees to comply with DTS Change Management Policy 4000-004. This DTS policy requires that any work performed by the Contractor has the potential to cause any form of outage, and any significant change to the State's information management architecture must first be reviewed by the DTS Change Management Committee, and coordinated accordingly. The DTS Project Manager will inform the Contractor of the change control requirement is applicable. Following this notification, any failure by the Contractor that causes outages or data security breaches caused by the Contractor as a direct result of failure to comply, will result in the Contractor's liability for the damages.

Upon request, DTS agrees to provide Contractor with a copy of the latest version of DTS Change Management Policy 4000-004.

25. PUBLIC INFORMATION: Contractor agrees that the contract, related Sales Orders, and Invoices will be public documents, and may be available for distribution. Contractor agrees that the State will make copies of the contract, related Sales Orders, and Invoices in accordance with Utah’s Government Records Access and Management Act (GRAMA). Except for items identified in writing and expressly approved by the State Division of Purchasing, Contractor also agrees that the Contractor’s response to the solicitation will be a public document, and copies may be given to the public under GRAMA law. The information the Contractor may disclose and the provisions of confidentiality, proprietary information, copyright information, or similar notation.

26. CREDITING DEPARTMENT IN ADVERTISING / PUBLICITY: Any publicity given to the project or services provided herein shall identify the State of Utah’s managing agency as the sponsoring agency and shall not be released without prior written approval of that State agency’s Project Manager.

27. STATE AGENCY WEB SITE BRANDING: The Contractor agrees to use the DTS logo, or a new color version if replaced in the future, on websites produced under terms of this contract. Contractor further agrees to allow a State agency to also utilize their own website branding and logo, if requested by that State agency.

28. DELIVERY: Unless otherwise specified in this contract, all deliveries will be F.O.B. destination with all transportation and handling charges paid by the Contractor. Reasonable and liability for loss or damage will remain with Contractor until final inspection and acceptance when responsibility will pass to the State except as to late deliveries, claims, and Contractor’s warranty obligations.

29. ORDERING AND INVOICING: All orders will be shipped promptly in accordance with the delivery schedule. The Contractor will promptly submit invoices (within 30 days of shipment or delivery of services) to the State. The State contract number and/or the agency purchase order number shall be noted on all invoices, freight tickets, and correspondence relating to the contract order. The prices paid by the State will be those prices listed in the contract. The State has the right to adjust or return any invoice reflecting incorrect pricing.

30. PROMPT PAYMENT DISCOUNT: Effective May 99, a prompt payment discount based upon early payment; however, discounts offered for less than 30 days will not be considered in making the award. Contractor shall list Payment Discount Terms on invoices. The prompt payment discount will apply to payments made with purchasing cards and checks. The date from which discount terms is calculated will be the date a correct invoice is received or receipt of shipment, whichever is later; except that if payment is performed, the date will be the date of acceptance of the mechanism;

31. PAYMENT:

1. Payments are normally made within 30 days following the date the order is delivered or the date a correct invoice is received, whichever is later. After 60 days from the date a correct invoice is received by the appropriate State official, the Contractor may assess interest on overdue, undiscounted accounts charged up to a maximum of the interest rate paid by the IRS on taxpayer refund claims, plus two percent, computed State of Utah IT Contract - Digwest LLC - Attachment A
similarly as the requirements of Utah Code Section 15-6-3. The IRS interest rate is adjusted quarterly, and is applied on a per annum basis, on the invoice amount that is outstanding.

1. The contract total may be changed only by written amendment executed by authorized personnel of the parties. Unless otherwise stated in the Contract, all payments to the Contractor will be made for mail, electronic funds transfer, or State of Utah's purchasing card (major credit card). The State of Utah will not allow the Contractor to charge and users electronic payment fees of any kind.

2. The acceptance by the Contractor of final payment without a written protest filed with the State within ten (10) working days of receipt of final payment shall release the State from all claims and all liability to the Contractor for fees and costs of the services pursuant to this Contract.

3. Notice: Wherever under this contract one party is required to give formal notice to the other, such notice shall be deemed given upon receipt of electronic mail and e-mail attachments. Formal Notice to the Contractor and to DTS shall be addressed as follows:

   Contractor:
   State of Utah - DTS
   E-mail sent to: iftcontract@state.utah.us
   State of Utah Contract (Cover) Page of this
   Contract.

5. Overpayment: The Contractor agrees that if during or subsequent to the contract performance, a CPA audit, or a State agency audit determines that payments were incorrectly reported or paid, the Department may adjust the payments. The Contractor shall, upon written request, immediately refund to DTS any such overpayments. The Contractor further agrees that the Department shall have the right to withhold any or all subsequent payments under this or other contracts that the Contractor may have with the State until recoupment of overpayment is made.

6. Payment withholding: The Contractor agrees that the adequate reporting, record keeping, and compliance requirements specified in this contract are material elements of performance and that the Contractor's record keeping practices, compliance, and reporting to DTS are not conducted in a timely and satisfactory manner, DTS may withhold part or all payments due under this or any other contract until such deficiencies have been remedied. This includes, but is not limited to, Contractors failure to provide timely invoicing, and/or other requirements described elsewhere within this contract. In the event of the payment(s) being withheld, DTS agree to provide ten (10) day advance notice to the Contractor of the deficiencies that must be corrected in order to bring about the release of withheld payments. Contractor shall have ten (10) days thereafter to correct the cited reporting or record keeping practice deficiencies or the contract may be terminated.

52. PATENTS, COPYRIGHTS, ETC.: The Contractor will release, indemnify and hold the State, its officers, agents and employees harmless from liability of any kind or nature, including the Contractor's use of any copyrighted or uncopyrighted composition, secret process, patented or unpatented invention, article or appliance furnished or used in the performance of this contract.

53. COPYRIGHT: The contractor agrees that any and all Deliverables prepared for the State of Utah as required by this contract, to the extent to which it is eligible under copyright law in any country, shall be deemed work made for hire, such that all rights, titles and interest in the work and Deliverables shall be exclusively owned by the State of Utah. State of Utah reserves a royalty-free, non-exclusive, irrevocable license to reproduce, publish, or otherwise use and to authorize others to use for Federal or State Government purposes, such software, modifications and documentation. To the extent any Deliverable is deemed not to be, for any reason whatsoever, work made for hire, Contractor agrees to assign and hereby assigns all right, title and interest, including but not limited to copyright, patent, trademark and trade secret, title to Deliverable, and all extensions and renewals thereof, to the State of Utah. Contractor further agrees to provide all assistance reasonably requested by the State of Utah in the establishment, preservation, and enforcement of its rights in such Deliverables without any additional compensation to Contractor.

54. OWNERSHIP, PROTECTION AND USE OF RECORDS: Except for confidential medical records held by direct care providers, the State shall own exclusive title to all information gathered, reports developed, and conclusions reached in performance of this contract. The Contractor may use, except in meeting its obligations under this contract, information gathered, reports developed, or conclusions reached in performance of this Contract without the express written consent of the State. The improper use or disclosure of any information concerning a State of Utah client, or a State of Utah employee for any purpose not directly connected with the administration of the State, or the Contractor's responsibilities with respect to services purchased under this agreement, is prohibited except on written consent of the State agency employee, state agency client, their attorney, or their responsible parent or guardian. The Contractor will be required to sign a Confidential Information Certification form in situations where they will be given access to confidential experimental records. The Contractor agrees to maintain the confidentiality of records held as agent for the State as required by Government Records Access and Management Act (GGRAMA), or other applicable federal or state law. The State of Utah shall own and retain unlimited rights to use, disclose, or duplicate all information and data (copyrighted or otherwise) developed, derived, documented, stored, or furnished by the Contractor under this contract. The Contractor, and any subcontractor under its control, expressly agrees not to use confidential client, or confidential federal, state, or local government data, without prior written permission from the State of Utah Project Manager and appropriate officials of the State Agency.

55. OWNERSHIP, PROTECTION. AND USE OF CONFIDENTIAL FEDERAL, STATE, OR LOCAL GOVERNMENT INTERNAL BUSINESS PROCESSES AND PROCEDURES: The improper use or disclosure by any party of protected internal Federal or State business processes, policies, procedures, or practices is prohibited. Confidential federal or state business processes, policies, procedures, or practices shall not be disclosed by the Contractor, Contractor's employees, or their Subcontractors, unless prior written consent has been obtained in advance from the State of Utah Project Manager.

State of Utah/IT Contract - Digweld LLC - Attachment A
35. OWNERSHIP, PROTECTION, AND RETURN OF DOCUMENTS AND DATA UPON CONTRACT TERMINATION OR COMPLETION: All documents and data pertaining to work required by this contract will be the property of the State and must be delivered to the State within 10 working days after termination or completion of the contract, regardless of the reason for contract termination, and without restriction or limitation to their future use. Any data that may be returned under provisions of this clause must either be in the format as originally provided, or in a format that is readily usable by the State or that can be formatted in a way that it can be used. Costs for all of these described items will be considered as included in the basic contract compensation of the work described used by the State.

37. CONFIDENTIALITY: Contractor, and anyone for whom the Contractor may be liable, must maintain the confidentiality of any non-public personal information. Personal information includes, but is not limited to, names, social security numbers, birth dates, addresses, credit card numbers and financial account numbers. The State reserves the right to identify additional reasonable types or categories of information that must be kept confidential by the Contractor and anyone for whom the Contractor may be liable. This duty of confidentiality shall be ongoing and survive the term of this contract.

38. ASSIGNMENT/SUBCONTRACT: Contractor will not assign, sell, transfer, subcontract or delegate rights, or delegate responsibilities under this contract, in whole or in part, without the prior written approval of the State.

39. DEFAULT AND REMEDIES: Any of the following events will constitute cause for the State to declare contractor in default of the contract:
1. Non-performance of contractual requirements.
2. A material breach of any terms or conditions of this contract. The State will issue a written notice of default providing a ten (10) day period in which Contractor will have an opportunity to cure. Time allowed for cure will not diminish or eliminate Contractor’s liability for damages. If the default remains, after Contractor has been provided the opportunity to cure, the State may do one or more of the following: 1. Exercise any remedy provided by law; 2. Terminate this contract and any related contracts or portions thereof; 3. Impose liquidated damages, if liquidated damages are listed in the contract. 4. Suspend Contractor from receiving future solicitations.

40. TERMINATION UPON DEFAULT: In the event this contract is terminated as a result of a default by the Contractor, the Department may procure or otherwise obtain, upon such terms and conditions as the Department deems appropriate, services similar to those terminated, and Contractor shall be liable to the Department for any and all damages arising therefrom, including, but not limited to, attorneys’ fees and excess costs incurred by the Department in obtaining similar services.

41. FORCE MAJEURE: Neither party to this contract will be held responsible for delay or default caused by fire, riot, act of God and/or war which is beyond that party’s reasonable control. The State may terminate this contract after determining such delay or default will reasonably prevent successful performance of the contract.

42. PROCUREMENT ETHICS: The Contractor understands that a person who is interested in any way in the sale of any supplies, services, construction, or insurance to the State of Utah is violating the law if the person gives or offers to give any compensation, generally, kickback, bribe, loan or reward, or any promise thereof to any person acting as a procurement officer or agent of the State, or who is any official capacity participates in the procurement of such supplies, services, construction, or insurance, whether it is given for their own use or for the use or benefit of any other person or organization (U.S.C. 20-234.3 Utah Code, as amended).

43. WORKERS’ COMPENSATION: The Contractor shall furnish proof to the State, upon request and maintain during the life of this contract, workers’ compensation insurance for all its employees as well as any subcontractor employees related to this contract.

44. LIABILITY INSURANCE: The Contractor agrees to provide and to maintain during the performance of this contract, at its sole expense, a policy of liability insurance. The limits of this insurance shall be as less than $1,000,000/000 for each occurrence and $3,000,000/000 aggregate.

It shall be the responsibility of the Contractor to require any of their Subcontractor(s) to secure the same insurance coverage as prescribed herein for the Contractor.

45. CONFLICT OF TERMS: Conflicting Terms and Conditions that apply must be in writing and attached to the contract. No other Terms and Conditions will apply to this contract including terms listed or referenced on a Contractor’s website, terms in another contract’s order, etc. In the event of any conflict in the contract terms and conditions, the order of precedence shall be: 1. Attachment A: State of Utah Standard IT Terms and Conditions; 2. State of Utah Contract Signature Pages; 3. State Additional Terms and Conditions; 4. Contractor Terms and Conditions.

46. ENTIRE AGREEMENT: This Agreement, including all Attachments, and documents incorporated hereunder, and the related State Solicitation constitute the entire agreement between the parties with respect to the subject matter, and supersedes any and all other prior and contemporaneous agreements and understandings between the parties, oral or written. The terms of this Agreement shall supersede any additional or conflicting terms or provisions that may be set forth or printed on the Contractor’s work place, cost estimate forms, receiving tickets, invoices, or any other related standard forms or documents of the Contractor that may subsequently be used to implement, execute, or invoice services hereunder from time to time, even if such standard forms or documents have been signed or initialed by a representative of the State. The parties agree that the terms of this Agreement shall prevail in any dispute between the terms of this Agreement and the terms printed on any such standard forms or documents, and such standard forms or documents shall not be considered written instruments of this Agreement.

47. SURVIVABILITY: This paragraph defines the specific contractual provisions that will remain in effect after the completion of or termination of this contract, for whatever reason: (a) State of Utah Standard IT Terms and Conditions # 2, Contract Administration, Choice of Law, and Venue; (b) State of Utah Standard IT Terms and Conditions # 23, Severance Provision and Handling of Data; (c) State of Utah Standard IT Terms and Conditions # 31, Copyright; (d) State of Utah Standard IT Terms and Conditions # 34, Ownership, Protection, and Use of Records, including Residues of such records; and (e) State of Utah Standard IT Terms and Conditions # 35, Ownership, Protection, and Use of Confidential Federal, State, or Local Government Internal Business Processes, including Residues of such confidential business processes; (a) State of Utah Standard IT Terms and Conditions # 36, Ownership, State of Utah IT Contract - Bipartisan LLC - Attachment A
Protection and Return of Documents and Data Upon Contract Termination or Completion; (b) State of Utah Standard IT Terms and Conditions # 37, Confidentiality; (c) State of Utah Standard IT Terms and Conditions # 45, Conflict of Terms.

48. WAIVER: The waiver by either party of any provision, term, covenant or condition of this Contract shall not be deemed to be a waiver of any other provision, term, covenant or condition of this Contract nor any subsequent breach of the same or any other provision, term, covenant or condition of this Contract.

If professional services are applicable to this solicitation/contract, the following terms and conditions apply:

48. TIME: The Contractor shall complete the scope of services work in a manner to achieve any milestones identified in the procurement documents related to this Contract and the attachments to this contract. The full scope of services will be completed by any applicable deadline stated in the solicitation.

50. TIME IS OF THE ESSENCE: For all work and services under this Contract, time is of the essence and Contractor shall be liable for all damages to the State of Utah and anyone for whom the State of Utah may be liable, as a result of the failure to timely complete the scope of work required under this Contract.

51. CHANGES IN SCOPE: Any change in the scope of the services to be performed under this Contract shall be in the form of a written amendment to this Contract, mutually agreed to and signed by duly authorized representatives of both parties, specifying any such changes, fee adjustments, any adjustment in terms of performance, or any other significant factors arising from the changes in the scope of services.

52. PERFORMANCE EVALUATION: The State of Utah may conduct a performance evaluation of the Contractor’s services, including specific personnel of the Contractor. Reference in the Contract to Contractor shall include Contractor, Contractor’s subcontractors, or subconsultants at any tier, if any. Results of any evaluations will be made available to the Contractor.

53. WAIVERS: No waiver by the State or Contractor of any default shall constitute a waiver of the same default at a later time or of a different default.

54. INSURANCE:

1. To protect against liability, loss and/or expense in connection with the performance of services described under this Contract, the Contractor shall obtain and maintain in force during the entire period of this Contract, without interruption, at its own expense, insurance as listed below from insurance companies authorized to do business in the State of Utah. If the solicitation document has qualification requirements for the financial stability of the insurance company, these requirements must be met.

2. The following are minimum coverages that may be supplemented by additional requirements contained in the solicitation for this Contract or provided in an Attachment to this Contract, if no insurance limits are identified in the solicitation, insurance minimums will default to Section 10. Liability Insurance Requirements:
   (1) Workers’ Compensation Insurance and Employers’ Liability Insurance. Worker’s compensation insurance shall cover all liability under the worker’s compensation laws of the jurisdiction in which the services are performed at the statutory limits required by said jurisdiction.
   (2) Professional liability insurance in the amount as described in the solicitation for this Contract, if applicable.
   (3) Any other insurance described in the solicitation for this Contract, if applicable.

3. Any type of insurance or any increase in limits of liability not described in this Contract which the Contractor requires for its own protection or on account of any statute, rule, or regulation shall be its own responsibility, and shall be provided at Contractor’s own expense.

4. The carrying of insurance required by this Contract shall not be interpreted as relieving the Contractor of any other responsibility or liability under this Contract or any applicable law, statute, rule, regulation, or order.

55. STANDARD OF CARE: The services of Contractor and its subcontractors and subconsultants at any tier, if any, shall be performed in accordance with the standard of care exercised by licensed members of their respective professions having substantial experience providing similar services which simulates the type, magnitude and complexity of the services that are the subject of this Contract. The Contractor shall be liable to the State of Utah for claims, liabilities, additional burdens, penalties, damages or third party claims (i.e. another Contractor’s claim against the State of Utah), to the extent caused by wrongful acts, errors or omissions that do not meet this standard of care.

56. STATE REVIEWS, LIMITATIONS: The right of the State to perform spot checks, plan reviews, other reviews and/or comment upon the services of the Contractor, as well as any approval by the State, shall not be construed as relieving the Contractor from its professional and legal responsibility for services required under this Contract. No review by the State or any engineering, approval or acceptance, or payment for any of the services required under this Contract shall be construed as waiving any right the State may have at law in any case of action arising out of the performance or nonperformance of this Contract, and the Contractor shall be and remain liable to the State in accordance with applicable law for all damages to the State caused by the wrongful acts, errors and/or omissions of the Contractor or its subcontractors or subconsultants at any tier, if any.

(Revision Date: 25 Mar 2014)
## ATTACHMENT B:
**Scope of Work, Contract Pricing, and Contract Payments**

### I. Scope of Work

**SECTION 1 – POTENTIAL DEPLOYMENT AND FIELD CONDITIONS**

The value and desire to obtain travel times on road segments is not limited to any specific location or condition, so it is conceivable and desired that these MAC reader devices will operate in both urban and rural areas under a variety of challenging conditions. Site conditions will range from areas having low volumes of Wi-Fi or Bluetooth enabled devices to measure, to segments of closely spaced intersections where interference from other radio sources may exist. Hence the ability of these units to adapt and support a wide and varying range of conditions, as well as an ability to remotely monitor and detect failures of devices that are located in distant rural areas will be important.

Specifically, UDOT will likely deploy and monitor the travel time measurements from these MAC readers at locations possessing the following features:

<table>
<thead>
<tr>
<th>Road Type</th>
<th>Location</th>
<th>Freeway / Highways</th>
<th>Freeway / Highways</th>
<th>Arterials</th>
<th>Field Infrastructure &amp; Potential Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freeway / Highways</td>
<td>Urban</td>
<td>High</td>
<td></td>
<td></td>
<td>• SC-powersource</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Fiber/Ethernet based communications</td>
</tr>
<tr>
<td></td>
<td>Rural</td>
<td>Low</td>
<td></td>
<td></td>
<td>• Solar Power</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Cellular Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Remote and difficult to maintain due to long distances from maintenance stations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Maintenance may need to be performed by personnel that are trained in ITS type electronics</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Mounted in Traffic Signal Cabinets with SC-power and Ethernet Communications</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• 1 mi. mile spacing of intersections</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• High potential of 2.4 GHz interference from radio businesses, wireless radios or other access points</td>
</tr>
</tbody>
</table>
SECTION 2 – FUNCTIONAL REQUIREMENTS

The functional requirements are divided into the following two sections (Wi-Fi and/or Bluetooth Sensor Hardware, and Backend Travel Time Processing System).

If there is a conflict between the stated requirements of the RFP and the product offered in the vendor’s proposal, the vendor shall supply the product offered in their proposal.

2.1 – Wi-Fi and/or Bluetooth Sensor Hardware

General Overview:

MAC sensors shall be capable of monitoring and measuring vehicular and pedestrian movement by identifying and comparing unique MAC (Media Access Control) addresses associated with Wi-Fi and/or Bluetooth-enabled electronic devices. Proposed uses will be to collect and disseminate travel time to the public via traditional Advanced Traveler Information Systems (ATIS) such as signs, websites or phone apps. Potential uses may consist of estimating segment travel times, Origin-Destination splits, segment (freeway, highway, arterial or work zone) congestion, and delay times.
2.1.1 Minimum Technical Specification Requirements:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Temperature Range</td>
<td>-30° to 65°C</td>
</tr>
<tr>
<td>Relative Humidity Range</td>
<td>10% to 90% non-condensing</td>
</tr>
<tr>
<td>Dimensions (Max)</td>
<td>16 in x 13 in x 8 in</td>
</tr>
<tr>
<td>Power consumption (Max)</td>
<td>10 Watts</td>
</tr>
<tr>
<td>Power Options:</td>
<td>Hardwire:</td>
</tr>
<tr>
<td></td>
<td>• AC (110-220 VAC)</td>
</tr>
<tr>
<td></td>
<td>• Power over Ethernet (PoE)</td>
</tr>
<tr>
<td></td>
<td>Solar:</td>
</tr>
<tr>
<td></td>
<td>• Complete system (panels, long-life or deep cycle</td>
</tr>
<tr>
<td></td>
<td>battery, cables, mounting hardware and all</td>
</tr>
<tr>
<td></td>
<td>appurtenant parts) sufficient to operate proposed</td>
</tr>
<tr>
<td></td>
<td>MAC Reader for 7 days without sun</td>
</tr>
<tr>
<td></td>
<td>• Capable of maintaining full charge based on 5</td>
</tr>
<tr>
<td></td>
<td>hours of sun/day</td>
</tr>
<tr>
<td>Connectivity (wired)</td>
<td>• 10/100BaseT</td>
</tr>
<tr>
<td></td>
<td>• RS-232 Serial</td>
</tr>
<tr>
<td>Connectivity (cellular)</td>
<td>• Support GSM</td>
</tr>
<tr>
<td></td>
<td>• Support CDMA 3G</td>
</tr>
<tr>
<td>Wi-Fi and/or Bluetooth</td>
<td>• 2.4GHz Spectrum</td>
</tr>
<tr>
<td></td>
<td>• Class 1</td>
</tr>
<tr>
<td>Data Latency</td>
<td>≤ 45 seconds</td>
</tr>
<tr>
<td>Data Storage Capacity (Max)</td>
<td>2GB</td>
</tr>
</tbody>
</table>

2.1.2 Deployment Locations:

Readers shall be capable of working in rural areas where the volume of MAC enabled units from which to calculate accurate travel times is limited. The volume of successful MAC ID pairings and the accuracy of the processed data under low volume conditions will be evaluated.

2.1.3 Interference:

Readers shall be capable of working in a congested urban environment and at closely spaced intersections where the readers might be subjected to 2.4 GHz interference from another closely spaced reader and/or from local businesses, wireless radios or other access points within the area. This interference may result in a degradation of data, thereby reducing the number of successful pairings and statistical significance of the travel time, O-D and intersection delay calculations.
2.1.4 Lag, Latency and Accuracy

The inherent lag time for a reader to scan and process all device inquiries can both decrease accuracy and increase the chance that detection of a MAC ID might be missed. Due to the desire to install readers on signalized arterials with closely spaced intersections, this latency may impact the accuracy of delay and travel time calculations.

2.1.5 Installation Limitations, Maintenance and System Support:

UDOT's intent is to use these MAC readers to collect travel time data throughout the State. This however results in the need to use maintenance resources from all regions of the State to maintain or troubleshoot the field equipment.

Likewise, there may be deployments in challenging areas that may require special attention to ensure units are optimally installed.

2.1.6 Example Data Reports:

Provide reports from other system deployments to provide data for a 24 hour period. The intent of these reports is to illustrate the type and quality of data currently being collected from active field deployments under similar conditions to those anticipated in Utah. Data shall be generated from a live or recent deployment, and reports shall be provided for travel time systems that are/were deployed on the following road types:

1) Rural highway;
2) Signalized arterial; and
3) Freeway

Include with this data:

A. Measured traffic volumes;
B. # of MAC reads;
C. # of successful pairings;
D. Road location / name and agency contact information

2.2 - Backend Travel Time Processing System

The system provider shall be responsible for the hosting and processing of all MAC Reader data in a secure and redundant environment. This processing system, working in conjunction with all field deployments of the MAC Reader hardware and communications equipment / network, must be able to support the data collection and processing that is necessary to deliver accurate and real-time speed and travel time information for the road(s) where the sensors are deployed. The system shall be able to accommodate the addition of an unlimited number of sensors (constrained solely by the back end hardware) to form a network of manageable travel routes. Each route will display data for each sensor (i.e., local delay / congestion and O-D splits) and travel times for each segment in the network.
Mandatory and desired outputs of the analyzed and processed data follow:

2.2.1 Mandatory Requirements:

Processed data shall include:

- Segment travel times shall be provided between multiple reader pairs (i.e., a one-to-many relationship) to provide travel times for short individual segments, and for the entire network as a whole. Reader pairs to define the segment and network shall be user configurable.

- Segment travel time between any pair of readers shall be in seconds (or decimal units that can be converted to seconds).

- A time or timestamp with each sample.

- Delay time measurements at all reader locations.

- O-D splits shall be provided between multiple reader pairs (i.e., a one-to-many relationship) to provide O-D splits from one reader to a minimum of 3 downstream routes. O-D pairs to define the segments shall be user configurable.

- O-D splits shall be provided as a percentage.

- Collection period duration (i.e., the number of seconds samples were collected for each time stamped segment data sample).

- System health and status definition.

- Web based user configuration screens to allow end users to enter all required setup parameters (i.e. lane geometrics, distance).

- GPS location of deployed units.

2.2.2 Optional Requirements:

Identify all other processed and analyzed data feeds that will be included with their bespoke data processing. Examples of data elements that are considered useful include:

- Travel Times for different percentiles (i.e., an array) to differentiate between defined patterns of vehicle classifications. For example, slow moving trucks vs cars.

- Levels of Service (LOS).

- Numbers of unique MAC ID’s that are read in each data sample.

- Number of successful pairings per data sample.

- Number of all MAC ID’s read in each data sample.
2.2.3 Processed Data Format and Access

Processed data shall be made available to UDOT for subsequent integration with their Advanced Traffic Management System (ATMS). UDOT shall be able to poll the hosted data for integration into the ATMS for purposes of enhancing their traveler information. All data (raw or processed) shall be the sole and exclusive property of UDOT without any limitations of use or additional cost, unless otherwise specified or agreed to by UDOT.

Flexibility will be allowed in how this data will be made available, however the following features are expected to be provided as a minimum baseline:

- Data Collection – Collect, process, and timestamp data at regular intervals (i.e., every N seconds, where N is programmable and N is an offset from 00:00 such as 00:00:00, 00:00:20, 00:00:40, 00:01:00, etc.).
- Real-time – Processed data should be available in real-time (i.e., as it is collected, such that the previously collected sample set becomes available before the current sample's collection period has expired).
- Access – The processed data should be available via a network accessible service such as an HTTP-based web service or raw TCP/IP socket.
- Availability – The service must be available over the Internet, 24 hours / day, 7 days a week.
- Data Types – The provided data as stated above (2.2.1 – required, and 2.2.2 optional) shall be include within the message set for each defined segment.

2.2.4 Provider Hosted Website

In addition to the data processing and analysis transmissions to UDOT, a secondary vendor maintained web-based application shall also be made available to UDOT and authorized personnel to provide remote access to the processed data for viewing and downloading of performance metrics, system health and vendor generated reports. The hosted website shall provide access to the processed data in graphical or tabular format from the vendor's website. At a minimum, this information shall consist of:

- Travel time data for all defined segments.
- Sensor and paired data for all defined segments.
- Statistical metrics of data reads / matches for all defined segments.
- Delay calculations at sensor locations.
- Origin-Destination splits.
- Mapping display to graphically show processed data in real-time.

2.2.5 Data Encryption

It is imperative that sensor reads of all MAC ID's not be associated with any specific user account or any specific vehicle, hence all MAC reads shall be encrypted at the server prior to processing, by use of a salted hash (or approved equivalent) cryptographic function to preserve anonymity of the source. To further preserve and protect the anonymity of sources, a new "Salt" shall be randomly generated every 24 hours at a configurable time of day.
MAC addresses that are read shall be modified into a new string of data as a repeatable, but non-reversible process. A salted hash function is intended to take the item to be hashed (the MAC address) and add "salt" (which is another string of text) to it. This same salt and hash function is then applied to all other MAC address reads throughout the day so that a comparison and match can be made.

The ability to safeguard a specific MAC address and/or to associate it to a particular user is accomplished by randomly changing the salt on a daily basis. This change shall occur at some configurable off-peak time period (most likely 2 a.m.). Although the change in salt will make it impossible to match pairs at this cutoff time, this is precisely the security feature that is desired as it will also prevent the modified string of data from being reversed back into an identifiable MAC address.

2.2.6 Data Access, Security and Archiving

Hosted data shall be stored and archived in a secure facility with backup power and internet connectivity to ensure system redundancy and unrestricted polling access by UDOT to the processed data.

Data shall be archived and made available to UDOT for downloading throughout the life of the contract plus an additional 60 days after Contract termination. Downloads shall be accessible at minimum intervals of 24 hours. This historical data is intended to allow UDOT to recreate a travel time or O-D analysis from historical MAC ID reads, and therefore only needs to consist of the encrypted MAC ID's from successfully paired reads. This data shall be output into a format that can be opened and analyzed from a spreadsheet, and aside from the encrypted MAC ID's, shall contain any other relevant information that is required to analyze and recreate travel times and/or O-D splits between readers (i.e., timestamp, location).

II. Detailed Responses for Scope of Work

Digwest Services

Our current services meet or exceed all qualifications currently established for DOT14-4097T for all aspects of travel time and Origin-Destination. In addition to the basic requirements, our system was designed for real-time reporting of any size sample set within just a few seconds, making it possible for users to evaluate multiple speed, travel or origin-destination scenario's within seconds. Our web interface allows for:

- New project setup and takes less than 15 seconds
- Data report updates to the server every 1, 5 or 15 minutes
- Real-Time reports on the fly for both travel Time and Origin-Destination
- The State OWNS the data
- Comparative view and analysis capabilities
- Complete API documentation for machine to machine report data
- Built in GPS for automatic lat/lon coordinates
- Remote device update and connection capabilities
- Remote monitor for device temperature, battery power (on solar model) and radio antenna strength
- Multiple filter capabilities allows user to see ALL MAC data and ALL matched pair data for Travel Time and/or O-D
- The BlueMAC Bluetooth default detection diameter of 300 feet can be adjusted to maximum of 1000'
- All BlueMAC reader enclosures are NEMA certified, trenched poly-carbonate with additives to withstand extreme hot and cold temperature. All enclosures are water proof with water sealed connection ports.
The BlueMAC webserver and web services, in an eloquent yet professional manner, can present data quickly and with flexible access to real-time as well as archived data reporting. Data feeds are parsed and encrypted at collection. Individual device backup provides 5 or more years of data storage and continues collecting even when the network is unavailable.

**Functional Requirements: Section 2.1 – Sensor Hardware**

All device requirements are currently supported in our basic level package of services.

<table>
<thead>
<tr>
<th>Section 2.1.1 Digwest Meets the Minimum Technical Specification Requirements:</th>
<th>Minimum</th>
<th>Y/N</th>
<th>BlueMAC Capabilities and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Temperature Range</strong></td>
<td>-30 degrees to 65 degrees C</td>
<td>Yes</td>
<td>BlueMAC uses only industrial grade components</td>
</tr>
<tr>
<td><strong>Relative Humidity</strong></td>
<td>10% to 50% non-c</td>
<td>Yes</td>
<td>See brochure with design specifications</td>
</tr>
<tr>
<td><strong>Dimensions (Max)</strong></td>
<td>16 in x 13 in x 8 in</td>
<td>Yes</td>
<td>BlueMAC devices are very small, measuring 8 in x 6 in x 4 in</td>
</tr>
<tr>
<td><strong>Power consumption</strong></td>
<td>10 Watts (Max)</td>
<td>Yes</td>
<td>BlueMAC devices operate at 1 watt (one) allowing for a much smaller solar panel</td>
</tr>
<tr>
<td><strong>Power Options:</strong></td>
<td>Hardware: AC (110-220 VAC) or Power over Ethernet (PoE)</td>
<td>Yes</td>
<td>BlueMAC can use either method for power</td>
</tr>
<tr>
<td></td>
<td>Solar: As detailed</td>
<td>Yes</td>
<td>Solar panel attaches to housing body (please see image) There is no need for a separate installation of the solar panel assembly</td>
</tr>
<tr>
<td><strong>Connectivity (wired)</strong></td>
<td>10/100 Base-T</td>
<td>Yes</td>
<td>Dual RS-232 ports, dual USB ports</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Yes</td>
<td>micro USB, Ethernet port all located on device</td>
</tr>
<tr>
<td><strong>Connectivity (cellular)</strong></td>
<td>Supports GSM</td>
<td>Yes</td>
<td>Edge, and 3G are both fully supported</td>
</tr>
<tr>
<td></td>
<td>Supports CDMA</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Wi-Fi and/or Bluetooth</strong></td>
<td>2.4 GHz Spectrum Class</td>
<td>Yes</td>
<td>Variable power settings 0 thru 4, user adjustable</td>
</tr>
<tr>
<td><strong>Data Latency</strong></td>
<td>&lt; 45 Seconds</td>
<td>Yes</td>
<td>BlueMAC data access latency less than 4 seconds</td>
</tr>
<tr>
<td><strong>Data Storage Capacity (min)</strong></td>
<td>2GB</td>
<td>YES</td>
<td>4GB Standard, (provides min 5 years storage)</td>
</tr>
</tbody>
</table>
2.1.2 Capable of working in locations of low volume MAC-enabled devices

1. Bluetooth devices use the most powerful Bluetooth radio collector allowed by law. In addition to the available 100’ device capture range, the power setting can be adjusted up or down remotely to increase or decrease the area of coverage based on local conditions, traffic patterns and deployment location.
2. Standard deviation information is provided on all travel time reports. Server system will calculate report data on any segment data is captured.
3. Some types of readers will require several times more power to operate and collect a much larger range making close-in and portable deployment more problematic, even when there are fewer devices to capture. Basically, a greater range is not always the best solution to data capture since collected data may be outside the study area.
4. For O-D study, deployments should be as consistent as possible, using the same type gear at the same power setting and, if possible, in the same proximity to the roadway. This will provide the most accurate and consistent data collected between all sites.

2.1.3 Capable of working on arteries where the device might be susceptible to interference

1. Again, Bluetooth devices use the most powerful radio collector allowed by law allowing for the best opportunity to collect available data.
2. Individual filter options available on each report allow the user to identify and filter out unusually or inaccurate data based on interference or deployment anomalies.
3. Filter options allow access to complete data, pre-sorted or partial data order to allow the user to gauge and evaluate the level of outside interference to the study area.

2.1.4 Latency of data and limitations of monitoring data in real-time

1. Our Bluetooth driver is customized to use the maximum inquiry window and interval available in the Bluetooth Core specification. Extended inquiry features to request additional information from discoverable devices is removed from our driver in order to focus on maximizing the number of devices which can be discovered within the available inquiry slots by using rapid succession of basic inquiry. In addition, our driver considers every possible inquiry response as valid data, even from the same device in the same inquiry window.
   
   Data signal strength is also collected. This information allows the Bluetooth device to estimate relative distance from the device and calculate travel time data from the capture within the closest proximity to the Bluetooth reader.

2.1.5 Maintenance and Support Services

1. Digwest provides an extensive Helpdesk system for opportunity tracking and results reporting. The Digwest Helpdesk is manned Monday through Friday from 9:00 am to 6:00 pm (PST).
2. Digwest also maintains 24-hour on-call services and off-hour support.
3. Additional benefits include, the previously mentioned on-site support for hardware assistance as well as next-day replacement of both permanent and portable collection gear.
4. Device firmware and server software updates are handled automatically. Once approved by your administrator, updates automatically download to the individual devices through the network and install. In this manner new features and patches are instantly available.
5. Server updates are provided free of charge over the first years, and include any and all new features and enhancements to current offerings.

2.1.6 Report: Features for 24 hour period to illustrate data quality (See attached report section)
Section 2.2 Backend Travel Time Processing System

All backend requirements are currently supported in our basic level package of services.

<table>
<thead>
<tr>
<th>2.2.1 Mandatory Requirements</th>
<th>Y/N</th>
<th>BlueMAC Capabilities and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment travel time shall be provided between multiple reader pairs</td>
<td>Yes</td>
<td>On BlueMAC, called &quot;Routes&quot; Up to the total number of devices in a project can be user defined as a combination of segments called route and combine all of their data into a single report.</td>
</tr>
<tr>
<td>Segment travel time between any pair of readers shall be in seconds</td>
<td>Yes</td>
<td>All BlueMAC report features include GUI, table and report data in seconds, as well as all is speed.</td>
</tr>
<tr>
<td>A timestamp with each sample</td>
<td>Yes</td>
<td>Each sample data receives a timestamp and signal strength indicator.</td>
</tr>
<tr>
<td>Delay time measurements at all reader locations</td>
<td>Yes</td>
<td>Intersection delay data available from downloadable CSV file samples.</td>
</tr>
<tr>
<td>O/D split shall be provided between multiple reader pairs one to many</td>
<td>Yes</td>
<td>All O-D calculations provide the ability to identify any locations origin and the balance destination, next, allow a change of choices in seconds to view a different origin and related results.</td>
</tr>
<tr>
<td>O/D Splits shall be provided in percentages</td>
<td>Yes</td>
<td>O-D splits are provided in percentages and number of samples.</td>
</tr>
<tr>
<td>Collection period duration</td>
<td>Yes</td>
<td>Collection period is user definable by segment or project. All sample data is collected and time-stamps in seconds.</td>
</tr>
<tr>
<td>System health and status definition</td>
<td>Yes</td>
<td>Health available per device, project or by client combined devices. All data available is aggregated on individual (summary) views.</td>
</tr>
<tr>
<td>Web based user configuration screens allow all required setup</td>
<td>Yes</td>
<td>BlueMAC project and device setup user configurable from web site services.</td>
</tr>
<tr>
<td>GPS Location of deployed units</td>
<td>Yes</td>
<td>Automated GPS on board all cellular and portable systems and available on permanent system. User definable parameters on all devices for GPS.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.2.2 Optional Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Standard deviation as well as 15, 85 and 95% data automatically calculated for all project segments and routes.</td>
</tr>
<tr>
<td>2. LCS indicators including device &quot;ag&quot; time history, connectivity legend, history power sample collection history and reporting, snapshot sample history view, device temperature history and snapshot plus other reports.</td>
</tr>
<tr>
<td>3. Multiple report view features require very little setup.</td>
</tr>
<tr>
<td>4. Capabilities to identify and separate pedestrian and vehicle.</td>
</tr>
<tr>
<td>5. Detailed individual device report features for comment and control.</td>
</tr>
<tr>
<td>6. Battery management features.</td>
</tr>
<tr>
<td>7. Multiple level of downloadable database for captured data.</td>
</tr>
<tr>
<td>8. Number of successful pairings per data sample, number of unique MAC ID's that are read in each data sample.</td>
</tr>
<tr>
<td>9. Number of all MAC ID's read in each data sample.</td>
</tr>
</tbody>
</table>
3.2.3: Processed Data Format and Access

1. All data collected is owned and controlled by UDOT and for their exclusive use.
2. Digiwest provides a fully documented API with instructions, and cut and paste in code to integrate any report information from the BlueMAC server into any software program.
3. The connection and transfer of data is controlled by a 36 Digiwest client key code.
   All data is collected, processed and received a timestamp each individual second.
4. Data is collected in real time. Report generation can be provided in real-time assessing the time to travel the segment + the reporting schedule + approximately 6 up to 15 seconds data processing time.
5. Website and processed data is accessible by HTTP based web service and raw TCP/IP socket with credentials.
6. All data types included under mandatory requirements are provided in each defined segment.

2.2.8: Provider Hosted Website

1. All mandatory requirements are currently part of the BlueMAC basic level package of services.
2. See "Report Section" for virtual representation of IT and OD report capabilities.
3. All sensor and paired data is provided for all segments.
4. Mapping is displayed graphically and can show all processed data in real-time or historically.
5. Statistical metrics or data reads & matches are provided for all defined segments.
6. Website services are updated with new features for all clients throughout the year.

2.2.5: Data Encryption

1. System update scheduled prior to deployment to accommodate required encryption method.

2.2.6: Data Access, Security and Archiving

1. All data systems and storage maintained in a Digiwest maintained and controlled data center, with multiple backup systems and redundant 100MB Internet connectivity.
2. All data, raw and filtered are available 24/7 by download from the BlueMAC server as .CSV format files.
   This includes hits, matched pairs and G-D data.
3. All data from client owned device is the property of that client for their exclusive use.
4. All raw and processed data is available immediately from the website 24 hours a day.
5. Downloaded file output is delivered as .CSV for use in any spreadsheet.
6. All collected data archived daily and stored in three separate locations should device data recover be necessary.

2.2.7: Value Added Features

1. Small and very compact lightweight devices (30 lbs, respectively). Easy & fast to install. Low profile.
2. Multiple power and cellular connectivity options for both portable and permanent deployments.
3. Single component integration for portable devices small size solar panel fits directly to the device.
4. BlueMAC provides complete documented API for machine to machine access of data for TMC/UTC, roadway signage and public facing websites for traffic information.
5. Origin/Destination data.
BlueMAC

Introduction
BlueMAC data collectors capture unique Bluetooth identifier information from discoverable Bluetooth-enabled devices such as automobiles, smart phones, GPS navigation units or wireless headsets passing within range. In addition to the unique Bluetooth identifier, the BlueMAC data collector attaches a date, timestamp, signal strength, and location identifier. When this information is combined with similar observations from multiple devices, the operator can then accurately determine travel times between two locations during any time period the devices were active. The data collector pushes data into the BlueMAC server system either wirelessly, through a connected cellular network or directly over the LAN. Standard configurations include wireless setup and configuration to upload automatically.

Travel Time
Travel time reports can be generated at any time once data is received from two deployed devices. Data can be evaluated in the report section through a variety of filters and is updated with the newest data through Operator defined schedules. Further analysis can be done offline by exporting matched pairs of travel time observations. Travel time data is also available over the web services, SOAP and JSON methods, which are outlined in the accompanying API documentation.

Origin-Destination
Data collected from multiple devices can be combined into a single project allowing the evaluation of the origin of travelers and their destinations or exit points throughout a specific study area. Data collected for origin-destination studies can be filtered and reported in a variety of graphs or tables, and will continue to update as long as the project continues.

Device Overview
Alert policies are available to Operators and defined based on device status and health, including capture rate, battery voltage, internal temperature, device storage, and GPS coordinates. Alerts allow the Operator to quickly identify anomalies and other situations of interest over a larger number of device settings.

Total Performance
BlueMAC data collection systems combine state-of-the-art technologies to provide the Operator with the ultimate collection of features and performance. The BlueMAC Bluetooth module uses the most current technologies available to ensure the highest possible collection rate for roadway data while providing among the lowest power requirements in the market for Bluetooth gear. BlueMAC gear combined with the appropriate solar attachment may provide continuous performance in the harshest environments.

Total Security
BlueMAC data collection components collect the MAC address data from devices testing within range of the device. In addition to standard safety protocols, data collected by BlueMAC devices are transmitted over their first 24 bits. The data is then converted into a binary code, encoded for compression, and then finally transmitted through the Client's private APN over wireless or hard-wired network. These added steps provide a very high level of data security and privacy while still providing matchable data with complete traveler anonymity.

Total Coverage
BlueMAC provides outstanding Bluetooth signal coverage with up to beyond 100 meters on a standard antenna. For areas requiring greater coverage, reliable range can be extended to over 300 meters with upgraded antenna equipment.

610 SW Adair St, STE 700 Portland, OR 97205 | 503.224.2765 | sales.digivent.com | www.myblumac.com

State of Utah IT Contractor - Digivent LLC - Assignment B
BlueMAC Bluetooth Field Devices are Class I rated. Devices have a standard user adjustable detection radius up to 300 feet (distance based on a dipole antenna detecting Class 2 devices). Different antenna may be installed at individual sites to better suit local conditions.

Devices use TCP/IP and/or UDP/IP communication protocols over 10/100-BaseTX Ethernet network. Device network settings are user configurable.

Permanently devices can operate from 120V AC power source with a 5V adapter or from a 12V DC power supply. Portable devices can be powered in the same manner and include an on-board 5-day or longer battery supply, a solar charger panel, and a solar charger controller inside the device.

BlueMAC portable and external mount devices have waterproof NEMA enclosures for external mounting on vertical traffic support structures (signal supports, laminaire poles, sign supports, wood poles, Falcon Eye).

Devices collect and archive, using unique device identifier based on MAC address using encryption or data degradation.

Each device collects and archives all detections. Systems record multiple hits as a device travels through a device's detection range and maintain the strongest hit entry per Bluetooth device per device.

Devices collect and report data continuously, 24/7. Devices may be taken offline in user definable settings as power conservation measure or remain online continuously.

Devices upload data to a data collection server or optional cloud site at a regular operator defined schedule at the start of a project, and can be edited at any point through the life of the project. Reporting schedules can be preset to several options, including: upload every day, hourly, every 15 minutes, 5 minutes or every minute depending on power consumption limitations for continuously running projects.

Data is uploaded to the server automatically.

System has provisions for not losing data if upload fails by backing up data to an on-board SD Card.

The operating temperature range of all components is -22°F to 185°F (-30°C to 85°C) or better.

Each device checks with the central server each day to synchronize internal clock and generate daily time drift. In addition, each device carries a battery backed real-time clock source, 32.768 KHz min oscillator with +/- 10 ppm worst-case accuracy, or 36 seconds per day without any network time sync.

Each device supports replaceable external antennas. The external RF connector for Bluetooth signal is an N- type or RP-SMA connector. Omni-directional antennas are provided.

Received Signal Strength Indicator (RSSI) is recorded with each detection as reported by Bluetooth module firmware. All MAC data is parsed and data is binary encoded for transmission over a private APN network.

Device degrades all MAC data to eliminate ability to confidently trace scored data to private devices while maintaining dataset quality. Examples: truncation, division, randomization, or similar forms of data scrubbling. MAC address truncation occurs before the partially degraded MAC address is recorded to disk. Dataset quality is maintained by discarding 24 of 48 bits, which leaves 15,777,216 possible bit combinations to represent MAC addresses. If at the peak period 1000 unique MAC address detections occur per hour, the chance of collision is only 0.006%, yet high enough to cast reasonable doubt on definitively linking a truncated MAC address to a full MAC address.

Devices scan all frequency channels. 32 channels are defined by the universal General Inquiry Access Code and divided in to 2 "banks" of 16 channels each. During device inquiry, the Devices will search sequentially on the first group of 16 channels 100 times taking a total of 2.56 seconds after which the next group of 16 channels are sequentially searched 100 times. In this way all 32 channels are scanned at least once within 2.6 seconds.

Devices cache raw data in non-volatile (local memory unit) and upload to data collection system. Raw data (after MAC truncation) is written to SD storage in addition to being transmitted to the server. If transmission acknowledgement from the server does not occur after reporting, prior data is re-tested each sequential reporting interval until an acknowledgement is received for all data. Minimum 4GB of SD storage is provided, which can hold a minimum of 3 years capture data from a single station.

610 SW Alder St. STE 700 Portland, OR 97205 I 503.724.7465 | sales@digwest.com | www.mybluemacs.com
BlueMAC
Backend Software & Server Features

Raw and processed data is stored and permanently accessible at a data warehouse. Raw data includes original collected unique device identifiers with time stamps. Processed data includes matched unique device identifiers and estimated travel times.

Operators can define a travel time route between any two devices.

Operators can create origin-destination (O-D) reports. Operators are able to define O-D routes based on device placement.

System generates route travel time estimate from unique device identifiers matches suitable for near real-time analysis.

Near real-time is defined by “Data that depicts an event as it existed at the current time plus the processing time. The data varies from real time data because it is dependent on the type and speed of transmission. This data is usable for identifying changes in traffic flows.”

The agency has access to all raw and processed data and maintains data on a local server.

System supports concurrent logging in Operators.

Operators can create travel time reports on-the-fly once a pair of devices in the same project report in with project data.

Server automatically backs up archived data on a regular schedule.

System generates alerts based on user defined criteria. Examples

- Travel time for route exceeds 20 minutes.
- Sensor communications fail.
- System alert notifications, such as sensor fail, are user configurable.
- Traffic incident Detection alerts such as “travel time exceeding 150% of historical travel time for this time of day” is also user configurable.

The system logs changes or edits to system configuration, including changes, time, and user. All database deletes, updates, and inserts are minimally logged. It can be expanded to log more detailed information such as original value in the case of updates, with a small performance hit.

The system is capable of providing an XML or JSON feed with near real-time travel times for traveler information systems. Most recent match per travel time segment can be made available as an XML feed for any segment.
BlueMAC
Backend Software & Server Features (Continued)

Senors and routes can be identified with user definable logical names for each deployment. Each location name can be user defined, and pairs will be displayed with both location names.
System management has a webserver-based management, data, and reports interface where access is provided or available. The system is managed over a web interface compatible with all modern web browsers. Flash / Java is not required. Systems with closed-based services can be managed by a smartphone device or tablet.
System management shows system and sensor status. System and sensor status is displayed on the web interface.
System shows recent travel times on a map. Routes are color coded routes red, yellow, and green with user-defined threshold. Routes on a map will appear as a gradient of color between red, yellow and green as a proportion of the expected travel time versus the observed travel time.
System shows multiple sensors concurrent to display current travel times for multiple routes. The Travel Time Overview page displays a view with each color coded segment and route on it, plus a table of most recent travel times, speeds, and last observation.

The system supports multiple users at the same time for different locations.
The system supports multiple user accounts access rights levels. Example: Administrators and read-only accounts.
Administrative functions are available through the web interface, and the web services are a read-only interface. A read-only website user login option is also under development.
The system generates travel time summaries by route for hour, day, month, and year. Travel time summaries can be filtered by any date and time range, and will calculate travel time summary information (times, speeds, standard deviation, 15th, 85th, 95th percentile) for that defined time period only.
Reports are user configurable using 5, 15, and 60 minute data bins with daily groupings as an option.
O-D routes can be defined and analyzed using archived data.
All reports include sample size under the heading “number of trips” on the travel time summary.

610 SW Alder St. STE 700 Portland, OR 97204 1 503 232 2763 sales.digisite.com | www.mybluemap.com
III. Contract Pricing

PRICE ITEM DEFINITIONS:

1. **Basic MAC Reader Unit**: A unit bid price for a single, fully functional MAC Reader field unit that meets or exceeds the requirements of this RFP. This bid item assumes all appurtenances (i.e., cables, reader enclosures, mount, mounting hardware, etc.) that are needed to procure a functional MAC Reader unit will be included in this bid item. The communications interface shall consist of a 10/100 Ethernet interface. The power provided for this unit will be a 120 VAC source.

2. **System and Encryption Set Up**: A one-time price to implement, integrate, test, coordinate with UDOT's IT and Software support team, and train users on the basics of this system. This bid item shall also include all costs associated with the development, testing and verification of the salted hash function.

3. **Data Processing and Hosting Service**: A price to host and process the data from the field MAC reader units as defined in Section 2.2 - Backend Travel Time Processing System. This bid item should include all communication, maintenance, support and incidental costs needed to provide a fully functional backend host and processing system complete with the required data export feed and secondary web-based access.

4. **Cellular Communications Option**: A unit price to add or deduct to item #1 above to enable this MAC Reader unit to communicate via a cellular service to the offeror's hosting center that is fully paid, managed and configured by the offeror. This bid item should include all hardware, cellular service provider connections, and monthly communication fees as needed to enable a fully functional and remote connection between the field unit and the backend processing system.

5. **Solar Power Option**: A unit price to add or deduct to item #1 above to convert the power source to solar. The solar equipment to be included in this bid item must comply with the minimum power and hardware requirements as defined in Section 2.1.1 Minimum Technical Specification Requirements.

6. **Value-Add**: Optional components and parts that do not fit within the hardware or operational considerations listed in this document.

<table>
<thead>
<tr>
<th>Item 1 - Basic MAC Reader Unit (hardwired)</th>
<th>Quantity</th>
<th>Volume Discount</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Units 1-15</td>
<td>100%</td>
<td>$1,200/unit</td>
<td></td>
</tr>
<tr>
<td>Units 16-45</td>
<td>20%</td>
<td>$1,020/unit</td>
<td></td>
</tr>
<tr>
<td>Units 46-80</td>
<td>25%</td>
<td>$900/unit</td>
<td></td>
</tr>
<tr>
<td>Units 100-149</td>
<td>50%</td>
<td>$50/unit</td>
<td></td>
</tr>
</tbody>
</table>

Discount off of replacement component parts: 100% (warranty first year) (25% discount thereafter is extended warranty not purchased)

| Item 2 - System and Encryption Setup       | Lump Sum | $3,500          |

| Item 3 - Data Processing and Hosting Service | Back End Data and Support Fees | $15/unit/month |

| Item 4 - Cellular Communication Option (service / hardware) | Cellular Communication Option | $15/unit/month |

| Item 5 - Solar Power Option                  | Units 1-15 | $1,200/unit     |
|---------------------------------------------| Units 16-45 | $1,020/unit     |
| Units 46-100                                | 20%        | $900/unit       |

Discount off of replacement component parts: 100% (warranty)

Delivery time from receipt of order: 36 days

State of Utah IT Contract - Digwest LLC - Attachment B
Optional replacement parts (*Common replacement parts)

<table>
<thead>
<tr>
<th>Item</th>
<th>Model #</th>
<th>Price ($)</th>
<th>Per Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nimos G20</td>
<td>DIGI-NCG20</td>
<td>$450.00</td>
<td>1</td>
</tr>
<tr>
<td>SIM5330 Small Breakout</td>
<td>DIGI-SS330</td>
<td>$200.00</td>
<td>1</td>
</tr>
<tr>
<td>Assembled Cartridge Board</td>
<td>DIGI-CLA1</td>
<td>$200.00</td>
<td>1</td>
</tr>
<tr>
<td>SunSaver Gen 3</td>
<td>DIGI-SSS6</td>
<td>$600.00</td>
<td>1</td>
</tr>
<tr>
<td>Antenna Enclosures (8x10x4)</td>
<td>DIGI-AB1084</td>
<td>$150.00</td>
<td>1</td>
</tr>
<tr>
<td>Internal Frame Sets</td>
<td>DIGI-FP5</td>
<td>$250.00</td>
<td>1</td>
</tr>
<tr>
<td>Blue Nanoe Enclosure</td>
<td>DIGI-BNE</td>
<td>$400.00</td>
<td>1</td>
</tr>
<tr>
<td>IPX to RP-SMA Jumper*</td>
<td>DIGI-UELI</td>
<td>$60.00</td>
<td>1</td>
</tr>
<tr>
<td>RP to SMA Jumper*</td>
<td>DIGI-UELI2</td>
<td>$60.00</td>
<td>1</td>
</tr>
<tr>
<td>RP-SMA Jumper (14in.)*</td>
<td>DIGI-RPSMA14</td>
<td>$50.00</td>
<td>1</td>
</tr>
<tr>
<td>Omni-Directional Antenna*</td>
<td>DIGI-OB1</td>
<td>$25.00</td>
<td>1</td>
</tr>
<tr>
<td>GPRS/3GSM Antenna</td>
<td>DIGI-GLA1</td>
<td>$85.00</td>
<td>1</td>
</tr>
<tr>
<td>10W Solar Panel*</td>
<td>DIGI-SP10</td>
<td>$100.00</td>
<td>1</td>
</tr>
<tr>
<td>Alternative 15W Solar Panel</td>
<td>DIGI-SP15</td>
<td>$150.00</td>
<td>0</td>
</tr>
<tr>
<td>Alternative 20 W Solar Panel w/Mount</td>
<td>DIGI-SP20</td>
<td>$275.00</td>
<td>0</td>
</tr>
<tr>
<td>Alternative 50 W Solar Panel w/Mount</td>
<td>DIGI-SP50</td>
<td>$525.00</td>
<td>0</td>
</tr>
<tr>
<td>RAM Mounting Bracket</td>
<td>DIGI-AM1</td>
<td>$75.00</td>
<td>1</td>
</tr>
<tr>
<td>10/15W Solar Panel Mounting Plate</td>
<td>DIGI-SPM1</td>
<td>$75.00</td>
<td>1</td>
</tr>
<tr>
<td>SD Card*</td>
<td>DIGI-S28</td>
<td>$20.00</td>
<td>1</td>
</tr>
<tr>
<td>Pole Mounting Bracket*</td>
<td>DIGI-PMB</td>
<td>$75.00</td>
<td>1</td>
</tr>
<tr>
<td>Mounting Strap*</td>
<td>DIGI-MS2</td>
<td>$8.00</td>
<td>2</td>
</tr>
<tr>
<td>Yeni</td>
<td>DIGI-DY1</td>
<td>$10.00</td>
<td>1</td>
</tr>
<tr>
<td>Rubber Grommets</td>
<td>DIGI-G102</td>
<td>$1.50</td>
<td>3</td>
</tr>
<tr>
<td>Battery Strap*</td>
<td>DIGI-BS1</td>
<td>$8.00</td>
<td>1</td>
</tr>
<tr>
<td>Battery Plug*</td>
<td>DIGI-DP1</td>
<td>$20.00</td>
<td>1</td>
</tr>
<tr>
<td>Battery Receptacle</td>
<td>DIGI-DR1</td>
<td>$15.00</td>
<td>1</td>
</tr>
<tr>
<td>Bottom Solar Plug*</td>
<td>DIGI-SP1</td>
<td>$45.00</td>
<td>1</td>
</tr>
<tr>
<td>Bottom Solar Receptacle*</td>
<td>DIGI-SR1</td>
<td>$45.00</td>
<td>1</td>
</tr>
<tr>
<td>3/16&quot; 34° 1/4&quot; Hex Bolt</td>
<td>DIGI-TC1</td>
<td>$2.60</td>
<td>4</td>
</tr>
<tr>
<td>#10-32 1/2&quot; Pan Head Screw</td>
<td>DIGI-TC4</td>
<td>$1.00</td>
<td>4</td>
</tr>
<tr>
<td>#10 Lockwasher</td>
<td>DIGI-TC5</td>
<td>$0.25</td>
<td>4</td>
</tr>
<tr>
<td>#10 Lockwasher</td>
<td>DIGI-TC6</td>
<td>$0.25</td>
<td>4</td>
</tr>
<tr>
<td>#10-32 Nut</td>
<td>DIGI-TC7</td>
<td>$0.25</td>
<td>4</td>
</tr>
<tr>
<td>#10-32 Wing Nut</td>
<td>DIGI-TC8</td>
<td>$0.25</td>
<td>2</td>
</tr>
</tbody>
</table>

IV. Contract Payments

a. For purchases and services pursuant to this contract, invoices shall be submitted as outlined in Attachment C: "Invoicing".

State of Utah / IT Contract - Digwest LLC - Attachment B
ATTACHMENT C

1. **Invoicing**

   Contractor shall submit invoices to State:

   **Utah Department of Transportation**
   **Traffic Operations Center**
   **cio Richard Shelley**
   **2060 S 2760 W**
   **Salt Lake City, UT 84104-4592**

   Or via email to Richard Shelley at the Utah Department of Transportation:
   rehelley@utah.gov

   The Contract number and PO number shall appear on all invoices and correspondence.

   Billings must be itemized identifying clearly all items, time and service fees. Invoices shall be submitted in a timely manner.

   The State reserves the right to adjust incorrect invoices. State will remit payment by mail or electronic commerce.

2. **Non-Compete Clause**

   The Contractor represents its officers and employees are free to contract with State and are not subject to restrictions by the terms of their present or past employment, including, but not limited to an agreement not to compete for a period of time unless disclosure has been made.

   Contractor must disclose to the State any possible conflicts in writing, before the contract is signed, and the State will evaluate whether to continue with contract execution. State may elect to terminate a contract immediately with a Contractor who is subsequently determined to be subject to such restrictions without liability to the State. If the State elects to terminate a contract for this reason, the State will supersede paragraph #13 in Attachment A – Standard Terms and Conditions and will not provide 60-day prior notice to the Contractor.

3. **Responsibility for Wages**

   Contractor is responsible for all applicable company wages in accordance with the Federal, State and local laws and ordinances.

4. **Confidential Information**

   To the extent work under this contract requires that the parties may be given access to confidential or proprietary business, technical or financial
information the parties shall, after receipt thereof, treat such information as confidential. Both parties shall maintain, as confidential, and shall not disclose to any person outside its employ, nor use for the purpose other than performance of this Contract, any specifications, drawings, blueprints, data, business information or other confidential information which is learned by virtue of this contract, except where required by law. The parties agree not to appropriate such information to their own use or disclose such information to their own use or disclose such information to other parties unless specifically authorized in writing. The foregoing obligations, however, shall not apply to:

* Information which, at the time of receipt by the Contractor, is public domain.
* Information which is published after receipt by the Contractor, or otherwise becomes part of the public domain through no fault of the Contractor.
* Information which the Contractor can demonstrate was already in the possession at the time of receipt, and was not acquired directly or indirectly from the State.
* Information, which the Contractor can demonstrate, was received from a third party who did not require the Contractor to hold such information in confidence.

6. Quality of Service

Contractor represents to State that it is experienced in and familiar with all aspects of the services required. Contractor will keep the State advised as to all new technology in all aspects of service. No changes in service provided by the Contractor under this Contract shall be made without the States prior written approval.

7. Assignment of Contract

The Contractor shall not sublet, assign or transfer any part of this contract without prior written approval from State. Neither shall the provision of monies due under this contract be assignable without prior written approval from State.

8. Intellectual Property Indemnity

Upon State's written notification to Contractor, Contractor shall defend, at its expense, any claim against State alleging the services, or any part thereof, infringement on any patent, copyright, trademark, trade secret, mask work or other intellectual property interest in any country and shall pay all costs and damages awarded. If an injunction against State use,
sale, lease, license, other distribution of services and product, or any part thereof, result in such a claim (or, if State reasonably believes such an injunction is likely), Contractor shall, at its expense, (and in addition to the contractor’s other obligations hereunder) and as State requests, obtain for State the right to continue using, selling, leasing, licensing or otherwise non-infringing but functionally equivalent. The provisions of this section shall not apply to any claim of infringement resulting solely from Contractor’s compliance with State’s detailed design specifications, were provided.

9. Facilities and Materials

The Contractor and all personnel working under this contract shall not acquire, borrow, copy or use in any manner software, documentation or data on any State data processing facility for use other than as required to complete this contract with the exception of items covered in the Scope of Work.

11. Right of Future Development

The State reserves all rights to future development of this system and is in no way required to obtain the services of the Contractor for these developments or release these developments to the Contractor.

12. Similar Products

Should the State independently design, develop or acquire ideas and concepts identical to those provided by or contained in the Contractor’s product, Contractor agrees this Contract shall not prevent State from using ideas or concepts to design, develop or acquire hardware or software for its use, provided the State does not copy the Contractor’s product.

13. Non-Performance

If, at any time, Contractor fails to demonstrate the required expertise (as represented in the Contractor’s proposal) or fails to meet acceptable standards of performance, the State reserves the right to require the Contractor to replace individual(s) with competent individual(s). The State Project Manager must approve this replacement. If the Contractor fails to provide competent individuals the contract may be cancelled immediately. If the State elects to terminate this contract for this reason, the State will supersede paragraph #13 in Attachment A- Standard Terms and Conditions, and will not provide 60 days prior notice to the Contractor.

14. Waiver
The failure of any party to enforce any of the provisions of this Agreement, or any rights with respect to it, or the failure to exercise any election provided for in it, will in no way be considered a waiver of such provisions, rights or elections, or in any way affect the validity of this Agreement.

STANDARD INSURANCE REQUIREMENTS

GENERAL INSURANCE REQUIREMENTS FOR ALL POLICIES

A. Any insurance coverage required herein that is written on a “claims made” form rather than on an “occurrence” form shall (i) provide full prior acts coverage or have a retroactive date effective before the date of this agreement, and (ii) be maintained for a period of at least three (3) years following the end of the term of this Agreement or contain a comparable “extended discovery” clause. Evidence of current extended discovery coverage and the purchase options available upon policy termination shall be provided to the Utah Department of Transportation.

B. All policies of insurance shall be issued by insurance companies licensed to do business in the state of Utah and either:

(1) Currently rated A- or better by A.M. Best Company; and
(1A) The insurer must also have an A.M. Best Company financial size category rating of not less than VII.

---or---

(2) Listed in the United States Treasury Department’s current Listing of Approved Surplus (Department Circular 370), as amended.

C. The Contractor shall furnish certificates of insurance, acceptable to the Utah Department of Transportation, verifying the foregoing matters concurrent with the execution hereof and thereafter as required.

D. In the event any work is subcontracted, the contractor shall require its subcontractor, at no cost to the Utah Department of Transportation, to secure and maintain all minimum insurance coverage required of the contractor hereunder.

E. In the event that governmental immunity limits are subsequently altered by legislation or judicial opinion, the Contractor shall provide a new certificate of insurance within thirty (30) days after being notified thereof in writing by the Utah Department of Transportation, certifying coverage in compliance with the modified limits or, if no new limits are specified, in an amount acceptable to the Utah Department of Transportation.
F. All required certificates and policies shall provide that coverage there under shall not be canceled or modified without providing 30 days prior written notice to the Utah Department of Transportation in a manner approved by the Assistant Attorney General for the Utah Department of Transportation.

REQUIRED INSURANCE POLICIES

The Contractor, all its own cost, shall secure and maintain during the term of this Agreement, including all renewal terms, the following minimum insurance coverage:

A. Worker’s compensation and employer’s liability insurance sufficient to cover all of the Contractor’s employees pursuant to Utah law. If covered by Workers Compensation Fund of Utah, then the A.M. Best rating is not required in this area
1. Including Coverage B. Employer’s Liability
2. $100,000 limit each accident
3. $500,000 limit per disease-policy limit
4. $100,000 limit per disease each employee

This requirement includes those who are doing business as an individual and/or as a sole proprietor as well as corporations and partnerships. In the event any work is sub-contracted, the Contractor shall require its subcontractor(s) similarly to provide worker’s compensation insurance for all of the latter’s employees, unless a waiver of coverage is allowed and acquired pursuant to Utah law.

The Utah Department of Transportation should not be an additional insured for workers’ compensation insurance.

B. Commercial General Liability
Commercial general liability (CGL) insurance with the Utah Department of Transportation as an additional insured, in the minimum amount of:
$1,000,000 per occurrence
$3,000,000 general aggregate
$3,000,000 products and completed operations aggregate

These limits can be covered either under a CGL insurance policy alone, or a combination of a CGL insurance policy and an umbrella insurance policy and/or a CGL insurance policy and an excess insurance policy. The policy shall protect the Utah Department of Transportation, the contractor, and any subcontractor from claims for damages for personal injury, including accidental death, and from claims for property damage that may arise from the contractor’s operations under this Agreement, whether performed by the contractor themselves, or subcontractor, or anyone directly or indirectly employed by either of them. Such insurance shall provide coverage for premises operations, acts of independent contractors, products and completed operations.
APPENDIX D—TRANSPORTATION AGENCIES RESPONDING TO THE SURVEY

Alabama Department of Transportation
Arkansas State Highway and Transportation Department
Arizona Department of Transportation
District Department of Transportation (Washington, DC)
Florida Department of Transportation
Indiana Department of Transportation
Maine Department of Transportation
City of Minneapolis–Public Works, Traffic & Parking Services Division
Missouri Highways and Transportation Commission
Montana Department of Transportation
North Dakota Department of Transportation
Ohio Department of Transportation
Oklahoma Department of Transportation
Oregon Department of Transportation
Rhode Island Department of Transportation
South Carolina Department of Transportation
Utah Department of Transportation