APPENDIX F

INTELLIGENT TRANSPORTATION SYSTEMS (ITS) REQUIREMENTS

1. GENERAL REQUIREMENTS

1.1 The following general requirements pertain to the ITS Infrastructure and devices for the Bypass, which are conceptually illustrated in Figure 1 of this Appendix F.

Generally, for the ITS Infrastructure, including the hardware in the field and in the Data Management Centre as well as the application software, Project Co shall undertake detailed system design and prepare specifications for Ministry review in accordance with Schedule 9 – Review Procedure. Upon receiving a comment "Reviewed" or "Reviewed as Noted" pursuant to Schedule 9 – Review Procedure, the process shall be as follows:

1.1.1 For ITS hardware in the field, Project Co shall be responsible for procurement, testing installation, operation, maintenance and rehabilitation;

1.1.2 For ITS hardware in the Data Management Centre (DMC), which is comprised of the Data Hub and the Traffic Operations Hub, Project Co shall be responsible for preparing design and specifications and for procurement of the hardware which will be turned over to the Ministry. The Ministry shall at its cost be responsible for receiving the hardware, testing, installation, operation, maintenance and rehabilitation. Project Co shall provide assistance to the Ministry to ensure that the application software works properly on the hardware environment; and

1.1.3 For ITS application and specialized software, Project Co shall be responsible for development, testing, installation, operation, maintenance and rehabilitation (including updating software).

1.2 For all ITS devices, Project Co shall provide all required staff training (classroom and on-site) including quick reference user guides, installation documentation (electronic and hard copies) and operation and maintenance manuals.

1.3 All ITS devices must be compliant with the National Transportation Communications for ITS Protocol (NTCIP) which is a family of standards that enable "centre-to-field" and "centre-to-centre" device control. NTCIP provides data communications protocols that support integration and interoperability between centres and field devices. Specific NTCIP protocols that apply to the Bypass include but are not limited to:

- Traffic signals (NTCIP 1202);
- Variable message signs (NTCIP 1203);
- Environmental sensor stations (NTCIP 1204);
- CCTV cameras (NTCIP 1205);
- Vehicle count stations (NTCIP 1206); and
- Transportation sensor systems (NTCIP 1209)

In addition, the Data Management Centre (DMC) shall support "centre-to-centre" (C2C) communication with other agency centres. The design of systems in the DMC must comply with NTCIP C2C communication protocols.

Project Co is responsible to ensure that each device and the DMC on the Bypass are NTCIP compliant with respect to centre-to-field and centre-to-centre standards for the DMC.

1.4 For all ITS hardware devices in the field, Project Co shall prepare a formal test plan for Ministry review in accordance with Schedule 9 – Review Procedure. The hardware test plan will include all performance evaluation criteria as well as details of the following tests:

1.4.1 System Acceptance Test (SAT) prior to deployment to verify that the devices received from the manufacturer meet the required specifications. This SAT shall include a check that the devices are fully functional, complete and in good working order. This test shall be done under Ministry supervision; and

1.4.2 Field Acceptance Test (FAT) to evaluate the performance of the devices on a "production-like" system, prior to activation under simulated and realistic loads and conditions. The FAT shall test for factors including but not limited to accuracy, speed, reliability, scalability, usability, maintainability, configurability, and security. The FAT provides final contractual verification of the system's integrity and functionality. This test shall be done under Ministry supervision.

Upon successful completion of these tests, Project Co shall transfer the hardware devices from the test environment to the production (field) environment, under Ministry supervision.

1.5 Project Co shall ensure that the ITS devices and network are protected and secure with respect to intrusion and attack from unauthorized users. For the issue of cyber security, Project Co shall undertake the following tasks:

1.5.1 Cyber Security Audit - Project Co shall retain a qualified firm to undertake and complete a full Cyber Security Audit of the ITS Infrastructure, as designed, including all field devices, cabinets, supporting structures, wireless network, firmware, software drivers, firewalls and interfaces. The Cyber Security Audit shall apply to all hardware systems and technologies that will be designed as part of the Bypass. The cyber security firm will be responsible to supply all equipment or software including bandwidth and internet access to undertake any of the tests or tasks. Project Co may request approval from the Ministry for the cyber security firm to review and test the security of the systems by mimicking an attack.

The Cyber Security Audit shall address but not be limited to the following activities:

a. Identify the hardware or software item and describe details;
b. Identify the supplier (manufacturer or developer) of the product;
c. Document product warranties and firmware update requirements;
d. Field visits to device locations to determine vulnerabilities;
e. Follow up meetings/teleconference calls with supplier(s) if needed;
f. Assess vulnerabilities and risks of each device or product;
g. Determine possible impacts of an attack;

h. Assess impacts on the Data Management Centre;
i. Assess liability of damages due to an attack; and
j. Prepare recommendations to mitigate impacts of an attack.

The Cyber Security Audit shall provide an assessment of the current system as designed.

The recommendations of the Cyber Security Audit shall be used in the Cyber Security Plan;

1.5.2 Cyber Security Plan - For all ITS hardware devices in the field and software, Project Co shall complete and submit a formal Cyber Security Plan for Ministry review in accordance with Schedule 9 – Review Procedure. The Cyber Security Plan will provide a blueprint to deter attacks on the network and devices as well as prevent access to data from ITS Infrastructure that could be used to disrupt traffic flow, degrade safety, or support illegal activity. The Cyber Security Plan shall provide recommendations to prevent data from being accessed, stolen, modified or replaced with another dataset.

1.5.3 The Cyber Security Plan shall address the status of the devices and network going forward from Substantial Completion. The Cyber Security Plan shall address the following issues:

1.5.3.1 The Cyber Security Plan shall incorporate any security advisories issued up to the date of Substantial Completion by Canadian and US agencies including but not limited to Transport Canada, Industry Canada, USDOT, US Department of Homeland Security (DHS) and FHWA;

1.5.3.2 The Cyber Security Plan shall be complete and current as of the date of Substantial Completion and updated by Project Co at 2 year intervals during the Operational Term;

1.5.3.3 As part of the update, the Cyber Security Plan shall review the latest technologies and applications used in IT and security for consideration;

1.5.3.4 The Cyber Security Plan shall be coordinated with the Ministry including staff at the Data Management Centre (the Data Hub and the Traffic Operations Hub). The plan shall incorporate the Ministry's existing security protection systems installed at the Data Management Centre;

1.5.3.5 The Cyber Security Plan shall include an environmental scan of best practices in the industry to ensure that systems are safe and protected from intruders;

1.5.3.6 The Cyber Security Plan shall incorporate the results of input from Ministry staff including the DMC (Data Hub and the Traffic Operations Hub). Project Co may use email, teleconference calls and follow-up meetings to acquire the input;

1.5.3.7 The Cyber Security Plan shall consider various threat models including infiltration through the wireless and online networks. The threat models shall consider scenarios in which the attacker acquires physical access to the devices or cabinets as well as wireless and online access through the network;

1.5.3.8 The Cyber Security Plan shall identify the weakest security link in the network to focus improvements;

1.5.3.9 The Cyber Security Plan shall apply to all radio modems that will be designed as part of the Bypass including 5.8 GHz and 900 MHz (if used);

1.5.3.10 The Cyber Security Plan shall apply to all devices that provide remote or local access to the ITS Infrastructure including handheld terminals or laptops;

1.5.3.11 The Cyber Security Plan shall ensure that the system does not broadcast the SSID of the network to reveal it to unauthorized snoopers;

1.5.3.12 For 900 MHz radios, the 16 bit slave ID shall be selected as random values;

1.5.3.13 For traffic signal controllers, the Cyber Security Plan shall address the security of the debug port and consider disabling it unless used for non-operational purposes such as updates;

1.5.3.14 The Cyber Security Plan shall address the option of profile-based access control;

1.5.3.15 The Cyber Security Plan shall enable encryption of 5.8 GHz radios that interface to all ITS field devices;

1.5.3.16 The Cyber Security Plan shall address the use of pre-set default user names and passwords on all ITS devices. The plan shall develop a schedule to change the user names and passwords prior to Substantial Completion of the Bypass and at regular intervals. The user names and passwords with the schedule shall be sent to the Ministry for review in accordance with Schedule 9 – Review Procedure; and

1.5.3.17 The Cyber Security Plan shall provide a schedule to ensure that all firmware for ITS devices are updated prior to commissioning and at regular intervals during the Operational Term. Project Co shall be responsible for any and all firmware updates.

1.5.3.18 The Cyber Security Plan shall address the use of Virtual Private Networks (VPN) for service providers

1.5.3.19 The Cyber Security Plan shall address encryption of wireless data transfer using WPA-2 (personal and enterprise), WPA, WEP and other protocols.

1.5.3.20 The Cyber Security Plan shall address MAC address filtering for network interfaces.

1.5.3.21 The Cyber Security Plan shall include a penetration test wherein the firm assumes the role of an attacker to reveal weaknesses in the security readiness of the network and devices. The firm shall provide a report of the results to Project Co. Project Co shall be responsible to review the results of the penetration test with the Ministry and provide recommendations to address the issues.

1.5.3.22 Project Co shall submit the Cyber Security and Plan to the Ministry for review in accordance with Schedule 9, Review Procedure, prior to Substantial Completion.

Project Co and sub-contractors are directed to review and consider results of the paper entitled “Green Lights Forever: Analyzing the Security of Traffic Infrastructure” by Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex

Halderman (Aug.2014) from the Electrical Engineering and Computer Science Department at the University of Michigan. The paper appeared in the proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT'14), August 2014.

1.6 For all customized application software, Project Co shall submit a formal test plan, including all performance evaluation criteria, to the Ministry for review in accordance with Schedule 9 – Review Procedure prior to Substantial Completion. Customized application software refers to any new program developed by Project Co specifically for the Project or Commercial –Off-the-Shelf (COTS) software that is modified by Project Co for the Project. The test plan requirements apply to all software including generic and application programming interfaces (API). The test plan shall include (1) system performance testing of the software code and (2) user acceptance testing. All testing shall be performed by Project Co with Ministry attendance.

1.7 Upon Project Co receiving a comment "Reviewed" or "Reviewed as Noted" pursuant to Schedule 9 – Review Procedure to the test plan, Project Co shall undertake the system performance testing process which will include the following:

1.7.1 Detailed examination of the software programming code as well as a review of execution of the code under different loads, conditions, and the hardware for the systems on the Bypass;
1.7.2 The process shall test all software program functions for stability, reliability, and responsiveness;
1.7.3 The process shall test all software programs for security flaws and faults against unauthorized intrusion and attack;
1.7.4 The testing shall include but not be limited to documenting bugs, faults, coding errors, defects, and failures under load or specific conditions;
1.7.5 Project Co shall document the accuracy, reliability, speed and responsiveness of the data flows between the simulated loads and systems during the performance testing process;
1.7.6 Project Co shall prepare a test report of the results as well as the corresponding recommended fixes;
1.7.7 Project Co shall revise the software code for further testing until required performance thresholds are reached after which the software code shall be submitted to the Ministry; and
1.7.8 Project Co is responsible for version control during the testing process.

1.8 Upon submission of the software the software shall undergo User Acceptance Testing (UAT) in a simulated test environment by the Ministry, subject matter experts or designated users for a period of up to 6 months after Substantial Completion. The participants require prior approval by the Ministry. The UAT process shall include the following:

1.8.1 Identification of problems, coding errors, debugging, updates and final testing shall be documented and addressed during the testing period;
1.8.2 Upon acceptance of all modifications to the software and testing, Project Co shall submit a test report to the Ministry for review in accordance with Schedule 9 – Review Procedure; and

1.8.3 Upon receiving a comment "Reviewed" pursuant to Schedule 9 – Review Procedure of the final test report and delivery of the final software source code to the Ministry, the software shall be deemed to reach Final Completion.

1.9 Transfer of the final version of the software from the test environment into the production environment shall be done after:

1.9.1 Final Completion is reached under Ministry supervision; and
1.9.2 Acceptance testing has been completed.

1.10 The Ministry is responsible for all DMC hardware in the Data Management Centre in the data hub and the traffic operations hub. The Ministry is responsible for the DMC test and production servers, their hosting and bandwidth requirements during these test phases. Project Co will work closely with the Ministry during the testing phase to ensure that the field devices and application software work on the hardware platform in the Data Management Centre provided by the Ministry.

1.11 For the test and production environments, at all times, the data, the servers and other hardware must be physically located in Canada.

1.12 All hardware, software and equipment for the ITS Infrastructure shall become assets of the Province of Saskatchewan including all intellectual property ("IP") at the Expiry Date. Intellectual property refers to any and all work products that are created or produced for the Regina Bypass Project. Intellectual property includes all custom application software and source code developed for the Bypass. This requirement does not apply to products that Project Co or vendors have developed in their existing products, prior to their participation in the Project.

1.13 Not Used.

1.14 Not Used.

1.15 Project Co shall submit copies of all user guides, test results, source codes, warranties, documentation and licences to the Ministry.

1.16 The ITS data will be available to Project Co and will be accessible through any web browser, using the administrative portal. Project Co shall not rely solely on the data to make decisions on operations and maintenance.

1.17 Project Co shall be compliant with Government of Saskatchewan technical standards (http://www.highways.gov.sk.ca/business). The standards shall apply to all areas of the ITS Infrastructure for the Bypass including but not limited to hardware, software and applications. The standards will be followed by Project Co to tie into the Data Management Centre and Ministry systems. Project Co shall work closely with the Ministry to ensure the data from the field devices tie into the Data Management Centre.

2. SPECIFIC REQUIREMENTS

The Bypass includes ITS Infrastructure and devices that must be delivered by Project Co. The specific functional requirements for the ITS Infrastructure shall include the following:

2.1 Traffic Data Counter (TDC) Stations

Project Co shall design and install the Traffic Data Counter (TDC) stations on the Bypass mainline. The TDC stations shall provide traffic data to be used as input into the Ministry's incident management system, infrastructure planning and performance evaluation of the Bypass.

2.1.1 The TDC stations shall count traffic in real time and shall transmit the data via the wireless network and fiber optic connection to the Ministry's Data Management Centre (DMC) at the Data Hub located at 1 Research Drive, Regina, SK. The data will be monitored for possible highway incidents by DMC operators at the Traffic Operations Hub located at 1855 Victoria Avenue, Regina, SK.

2.1.2 The data will be stored at the DMC servers, located at the Data Hub, in archival format for future review and analysis by the Ministry and Project Co.

2.1.3 Each TDC station shall be a wireless, high resolution, microwave radar-based unit. Each data set shall contain the following parameters at each TDC location, lane by lane, by direction:

- Traffic volume by lane and direction
- Average traffic speed and length of each vehicle
- 85^{th} percentile speed
- Lane occupancy
- Average headway (time) and gap (distance) between vehicles
- Classification counts using a length-based measurement such as employed by the BC Ministry of Transportation and Infrastructure.

2.1.4 The data will be used by the Ministry's Advanced Traffic Management System (the "ATMS") software to detect and analyze traffic flows for potential incidents. The ATMS software will be provided by Project Co. a part of the application software in the DMC. Details of the ATMS software are in Section 2.7.11 of this Appendix F.

2.1.5 The TDC stations shall count all lanes simultaneously and be installed on a standard breakaway pole or an existing structure, that is accessible from the shoulder via maintenance vehicle. If possible, the poles shall be installed outside the clear zone, as per the Saskatchewan Uniform Traffic Control Devices Manual. If the poles are within the clear zone, Project Co shall provide the necessary protection. The TDC units shall be mountable at a height of between 2 to 15 metres.

2.1.6 The range of detection shall cover all lanes in the direction of travel including shoulders between 2 to 75 metres from the unit. Battery life expectancy shall meet or exceed 10 years.

2.1.7 Accuracy of the TDC stations should meet or exceed:

- 98% accuracy for volume counts
- +/- 5 km/hr. for average speed measurements
- 90% accuracy for classification
- 90% accuracy for occupancy by direction
- 80% accuracy for occupancy by lane
- A minimum gap between vehicles of 1.67 m (5.5 ft.) is required

2.1.8 The thresholds for accuracy shall be tested against "ground truth" data on a corridor or location approved by the Ministry. The tests shall be conducted in coordination with the Ministry and Project Co for a representative set of traffic conditions including peak, off-peak, mid-day and weekend scenarios.

2.1.9 The TDC units shall support and integrate with the Ministry's environment of Windows 7 operating systems or higher. Performance shall be met under all weather conditions including fog, ice, snow, wind, dust, freezing rain, rain, changing temperatures and lighting.

2.1.10 The TDC units shall be contained within a secure, outdoor, all-weather enclosed casing that is water-tight and sturdy. The TDC unit shall be resistant to sunlight, humidity, heat (within the specified range of temperatures), and frost.

2.1.11 A total of eight (8) TDC stations shall be installed on the following sections of the Bypass:

2.1.11.1 On the Bypass mainline north of Dewdney Ave in NB and SB directions;

2.1.11.2 On the Bypass mainline south of the Highway 1 interchange west of Regina in NB and SB directions;

2.1.11.3 Highway 6 south of the Bypass mainline in the NB and SB directions; and

2.1.11.4 On the Bypass mainline east of the Tower Road interchange in the EB and WB directions

The approximate locations of these units are illustrated in Figure 1 of this Appendix F.

2.1.12 Project Co shall determine the exact locations of the TDC stations, based on the detailed design and field conditions. Project Co shall be responsible for the procurement, installation, operation, maintenance and rehabilitation of the eight TDC units.

2.1.13 The TDC units shall include a wireless modem to transmit the data to a local receiver and then to the Data Management Centre.

2.1.14 Project Co shall prepare a functional and system design report of the TDC stations for review in accordance with Schedule 9 – Review Procedure, prior to procurement and installation.

2.1.15 The report shall include but not be limited to the following:

- An assessment of the available radar detection technologies;
- Network connectivity requirements;
- Maintenance and service requirements;
- System design drawings; and
- System and field acceptance test plans

2.1.16 Project Co shall include the TDC units as part of the Cyber Security Audit and Cyber Security Plan requirements in the "General Requirements" of this Appendix F.

2.1.17 If the TDC units are not sufficient to meet the coverage requirements of the Bypass, Project Co shall include recommendations in the report.

2.1.18 At a future date, the Ministry may add more TDC units to supplement the data capabilities of the system pursuant to Schedule 19, the Variation Procedure.

2.2 Closed Circuit Television (CCTV) Stations

Project Co shall design and install cameras that will be operational throughout the Project Term.

The CCTV cameras installed during the Construction Activities shall be portable and live, showing real time, broadcast quality images that are transmitted directly to the Highway Hotline and other media to show progress of the construction. Project Co shall install one HDTV image quality camera at each interchange location. The camera must be capable of providing time-lapse images directly to the Highway Hotline of each interchange and surrounding area during construction. Camera images will refresh at least once every 15 minutes. The specifications for the CCTV camera installed during the Construction Activities are as follows:

- HDTV 1080i r 720p regarding resolution, color fidelity, 16:9 format, and full frame rate
- 10X optical zoom
- 12X digital zoom and autofocus
- Pan and tilt function if installed with an optional pan/tilt motor
- Power over Ethernet, which eliminates the need for power cables
- Must be operational from -40 C to 45 C, and include a unique Arctic temperature control for powering up at very low temperatures following a power failure.

The CCTV cameras that are to be installed for the Operational Term shall be permanent and at designated locations on the Bypass mainline and shall transmit images and data to the Data Management Centre. All CCTV cameras will support the incident management and traveller information systems. The following sections pertain to the permanent CCTV cameras:

2.2.1 Incident management is a coordinated and systematic approach to minimize the duration of incidents through detection verification, response and restoration of the accident site to normal operations. The CCTV camera units installed by Project Co shall be part of the Ministry incident management system which will include the following sub-systems:

2.2.1.1 Incident detection – this is primarily done through the traffic detector units but can also be performed by operators who scan the corridor using the CCTV cameras as well as drivers and service patrols that report a problem. The traffic data is evaluated by the Data Management Centre's (DMC) Advanced Traffic Management System (ATMS) software to assess accident potential, before the DMC operators are alerted;

2.2.1.2 Incident verification – the operator will use the pan-tilt-zoom feature of the CCTV units to verify the details of the incident including but not limited to: location, number and types of vehicles, accident severity, possible injuries, environmental impacts, and lane closure requirements;

2.2.1.3 Incident response – the operator shall initiate an appropriate response to the incident and coordinate with the jurisdictions and emergency services during the process. In addition, the operator shall initiate alternate route plans and update traveller information systems that will advise motorists and divert traffic. Timely checking on progress using the CCTV camera units may be required; and

2.2.1.4 Incident clearance and site management/restoration – the operator shall ensure that the site is cleared of vehicles involved in the incident and is restored to normal operation. CCTV cameras may be used by the operator to confirm progress.

2.2.2 The permanent CCTV cameras and their images shall be available to the Ministry's Advanced Traveller Information System (ATIS). During Construction Activities, the CCTV images will be sent directly to the Highway Hotline. During the Operational Term, the permanent CCTV images will be sent to the DMC. The permanent CCTV camera images shall be screen shots that are refreshed every 120 seconds.

2.2.3 Advanced Traveller Information Systems provide access to the public about the real time traffic conditions on their journey. In addition, ATIS is an important tool for emergency service providers to ensure that their routes during their response are open and available. The information is provided in the following two formats:

2.2.3.1 Pre-trip information informs the traveller to make decisions prior to departure. The systems include but are not limited to traffic-related web sites, highway advisory radio, TV and other media; and

2.2.3.2 En-route information informs the traveller on real time traffic conditions throughout the journey. The systems can include radio, variable message signs (VMS), and in-vehicle navigation.

The ATIS information allows the traveller to make their best trip decisions which may include delaying their trip, changing modes, altering routes, travel times, or even cancellation of their journey.

2.2.4 Project Co shall design and prepare the ATMS software code with an Application Programming Interface (API) to install the required interfaces to the Ministry's Highway Hotline website. Alternate design approaches to providing the images to

the Highway Hotline may be submitted for consideration by the Ministry. The Project Co shall also design and prepare the ATMS software code with a generic API for other application interfaces. The generic API shall be customizeable by vendors and service providers, the Ministry and partner agencies in the future. These APIs must be submitted by Project Co to the Ministry for review in accordance with Schedule 9 – Review Procedure.

2.2.5 Each permanent CCTV camera unit shall include the following components:

- CCTV camera and lens
- PTZ mechanism
- Enclosure and shield
- Pole and foundation including concrete barriers, if necessary
- Roadside cabinet
- Power supply
- Wireless node or communications connection
- Controller/encoder

2.2.6 The CCTV cameras shall be full colour, digital high definition (HD) "IP" 1080 p units. The CCTV cameras shall provide colour images with a minimum of 470 lines of horizontal resolution while in daytime mode.

2.2.7 The CCTV units shall have high speed "pan-tilt-zoom" (PTZ) functionality with movement controlled from the Ministry Data Management Centre with a full 360 degree "pan" range and 220 degree of tilt. The camera shall have a 36x optical zoom and 12x digital zoom. The camera shall support at least 250 pre-set positions and be controlled by an input device at the Data Management Centre such as a joystick, mouse, or keyboard.

2.2.8 The iris on the CCTV camera shall be automatically controlled but will be able to switch to manual control. The iris shall automatically close in the event of a power outage

2.2.9 The CCTV cameras shall have the ability to switch from daytime to "night-vision" automatically. The units will be housed in a full metal enclosure, with heating, fan and air conditioning and will include a sunshield that is installed over the housing to protect it from over-heating due to sun and to provide shade to the lens. The sunshield will not interfere with the field of view at any focus setting. All cables shall enter the enclosure from the rear or bottom of the enclosure.

2.2.10 The enclosure shall include a temperature sensor that will provide thermostatically controlled heaters to prevent condensation from forming within the enclosure. The enclosure shall have a wiper to clean the lens remotely. The camera will be capable of operation in temperatures ranging from -50 degrees C to + 50 degrees C. The camera shall start up in extreme weather conditions within this range of temperature.

2.2.11 The CCTV cameras shall perform in all weather conditions including fog, ice, snow, wind, freezing rain, changing temperatures and lighting. The enclosures and the camera units shall be resistant to shock, dust, vibration, water, and temperatures within the specified range.

2.2.12 The CCTV camera shall include an encoder that will enable control all functions in the device from the DMC including PTZ, focal adjustments, iris control, and others.

2.2.13 The CCTV cameras shall have no streaks or peaks within the image during operation in day or night mode without noticeable lags. The CCTV camera shall not exhibit flares in the image at any focal length or during any period of night or day.

2.2.14 The CCTV cameras shall support MPEG-4 standards, as a minimum, including all parts or subsets of the standards. The cameras shall support 30 frames per second (60 Hz) for all resolutions. The cameras shall contain an additional memory slot that will support SD/SDHC/SDXC memory card expansion. Each camera shall also include a progressive scan charge coupled device (CCD) sensor. The CCTV cameras will include an electrical surge and lightning protection, based on approved Ministry suppliers.

2.2.15 The CCTV cameras shall be installed on a standard breakaway pole or an existing structure. If possible, the poles shall be installed outside the clear zone, as per the *Saskatchewan Uniform Traffic Control Devices Manual*. If the poles are within the clear zone, Project Co shall provide the necessary protection. The pole or existing structure must be acceptable in terms of vibrations, line-of-sight and field of view. The CCTV camera shall be mountable at a height of up to 15 metres. The camera shall be accessible for maintenance purposes from the shoulder using a standard Ministry vehicle ("bucket truck") with a lifting arm, controls and enclosure for a maintenance worker. The CCTV camera's diagnostics shall be accessible via the DMC or locally via a laptop computer.

2.2.16 Connectivity to the CCTV unit shall be via the wireless/fiber network from the DMC or locally through a USB, Ethernet or RS 232 port.

2.2.17 The CCTV cameras shall have the following features for image control:

- Backlight compensation;
- Electronic shutter;
- Image stabilization including software;
- "auto" and manual white balance; and
- Image rotation

2.2.18 All CCTV camera images from permanently located CCTV cameras will be transmitted in real time to the Ministry's Data Management Centre at the Data Hub located at 1 Research Drive, Regina, SK. The CCTV camera's functions shall be controlled and directed by the DMC Traffic Operations Hub located at 1855 Victoria Ave, Regina, SK.

2.2.19 A total of seven (7) permanent CCTV stations shall be installed at the following locations:

2.2.19.1 Highway 11 interchange;

2.2.19.2 Highway 1 interchange;

2.2.19.3 Highway 6 interchange;
2.2.19.4 Tower Road interchange;
2.2.19.5 Pilot Butte/Highway 1 interchange (north end);
2.2.19.6 Pilot Butte/Highway 1 interchange (south end); and
2.2.19.7 Road-Weather Information System (RWIS) station east of Tower Rd.

2.2.20 Project Co shall determine the exact locations of each CCTV unit within each interchange. In choosing the quadrant of the interchange for the CCTV camera, Project Co shall consider factors including but not limited to access to power and communications, field of view of traffic corridors for incident management purposes, and accessibility for maintenance vehicles. From each location, the cameras' unobstructed field of view should include all segments of the interchange ramps, corridors and surrounding area. The operator in control of the camera must discern details of possible incidents.

2.2.21 A CCTV camera is included as part of the Road-Weather Information System (RWIS) station to assess local visibility and weather conditions. This RWIS CCTV camera is described in Section 2.4 of this Appendix F.

2.2.22 The approximate locations of the permanent CCTV cameras are shown in Figure 1 of this Appendix F.

2.2.23 The CCTV cameras shall include a wireless modem to transmit data to a local receiver and then to the Data Management Centre.

2.2.24 Project Co shall prepare and submit the CCTV Assessment Report to the Ministry for review in accordance with Schedule 9 – Review Procedure prior to procurement and installation. The assessment report shall include photos and video images of each CCTV camera location based on the expected height of each unit within the interchange quadrant on the Bypass mainline. These photos and videos shall be recorded using a standard Ministry vehicle ("bucket truck") with a lifting arm, controls and enclosure for a maintenance worker

2.2.25 The assessment report shall include but not be limited to evaluation of the following factors:

2.2.25.1 Current available technologies – an environmental scan shall be performed of the currently available CCTV camera technologies. The scan shall also evaluate costs for capital, maintenance and operation;
2.2.25.2 Field of view – at the designated locations, the CCTV cameras shall have an unobstructed field of view and line of sight to the Bypass mainline. The camera shall be able to view the features of the interchanges including primary corridors, ramps and overpasses;
2.2.25.3 Range – with full zoom, the CCTV cameras shall have clear views at a minimum of 500 metres and up to a one-way range of 800 metres;
2.2.25.4 Geometry – the CCTV cameras shall be located to provide coverage at or near changes in the geometry of the Bypass mainline;
2.2.25.5 Topology – the CCTV cameras shall be located to provide coverage in areas in which there are changes in grade;

2.2.25.6 Exposure to light – the CCTV cameras shall be located and positioned to minimize interference from direct view into sunlight; and

2.2.25.7 Obstructions – the CCTV cameras shall be located to minimize interference of the views due to objects such as trees, signage, structures and landscaping.

2.2.26 Project Co shall include the CCTV devices as part of the Cyber Security Audit and Cyber Security Plan requirements in "General Requirements" of this Appendix F.

2.2.27 If CCTV camera locations are insufficient to meet the coverage requirements of the interchange and corridor, Project Co shall include recommendations in the report for Ministry review in accordance with Schedule 9 – Review Procedure.

2.2.28 During the Construction Activities Project Co shall procure and install mobile, temporary CCTV cameras at each interchange to capture progress on the project. The cameras shall be mounted on a secure structure that is stable but can be moved to another location. The images will be sent from the cameras in real time directly to the Highway Hotline via the wireless network. Project Co shall obtain the approval of the Ministry for the locations of the temporary CCTV cameras. At the Ministry's discretion, it may retain any or all of the temporary CCTV cameras in each location as a permanent CCTV camera.

2.3 Variable Message Signs (VMS)

Project Co shall design and install Variable Message Sign (VMS) units at the designated locations on the RBP corridor.

2.3.1 The Variable Message Signs (VMS) will inform motorists of incidents and weather-related events and will become part of the Ministry's traffic management system that is operated from the Data Management Centre. Each VMS unit shall include a wireless modem to send data to and receive instructions from the Ministry Data Management Centre (Traffic Operations Hub) via the wireless network. The VMS unit shall transmit the data over the wireless network to a local receiver and then via the fiber optic network to the Data Management Centre.

2.3.2 Each VMS unit shall display 3 lines of amber text to a maximum of 25 characters and spaces per line and be visible in low light and adverse weather conditions. The signs shall be designed to be visible and legible at the required sight distance for the design speed and geometrics of the corridor. The size, height, illumination, and style of font shall be consistent with:

- Ministry standards and guidelines for sign design; and
- Best practices based on human factors guidelines.

2.3.3 The VMS unit shall be installed on a standard breakaway pole or an existing structure. The poles shall be installed as per the *Saskatchewan Uniform Traffic Control Devices Manual*. The pole or existing structure

must be acceptable in terms of visibility, accessibility for maintenance, and structural capacity to support the sign. The VMS shall be accessible for maintenance purposes from the shoulder, or if necessary, from the travel lane with traffic management staff and signage, using a standard Ministry vehicle ("bucket truck") with a lifting arm, controls and enclosure for a maintenance worker.

2.3.4 The VMS shall be contained in an all-weather, metal enclosure and be capable of operation in a temperature range of -50 degrees C to + 50 degrees C. The VMS shall perform in all weather conditions including fog, ice, snow, wind, rain, changing temperatures and different lighting. The VMS units shall be resistant to shock, dust, vibration, water, and temperatures within the specified range.

2.3.5 Each VMS shall be configurable remotely and will include software for managing the VMS on the network. The software shall provide a standard library of messages and also support the creation of customized messages by the Ministry for any or all VMS, remotely or from the Ministry Data Management Centre at the Traffic Operations Hub. Any messages required by Project Co must be requested and approved by the Ministry.

2.3.6 The software shall include diagnostics that will monitor the status and operation of the unit and alert the Ministry of any malfunction, loss of functionality, power or communication. The software will support the continued development of a library of messages that can be used or edited for use on the VMS.

2.3.7 Project Co shall ensure that any software used to access the VMS unit, either remotely or via handheld devices, shall be protected against unauthorized intrusion or attack as per the "General Requirements" of this Appendix F. The VMS unit shall be part of the Cyber Security Audit and Cyber Security Plan requirements as per the "General Requirements" of Appendix F.

2.3.8 Project Co shall prepare an assessment report which includes functional and system design for the VMS units. The report shall include but not be limited to the evaluation of the following factors:

2.3.8.1 An environmental scan of all available VMS technologies and software including modularity, weight, energy efficiency, portability, ease of maintenance, resolution and intensity of the pixels, and mounting/ease of installation;

2.3.8.2 A review of each VMS location in terms of legibility, sight distance, visibility, geometry, topology and local weather;

2.3.8.3 A review of system components such as cabinets, solar panels, power, UPS, and communications;

2.3.8.4 Assessment of the structural and wind loading on the pole or mounting

mechanism;

2.3.8.5 Security issues and requirements of the VMS and any remote or handheld devices that communicate with the VMS units; and

2.3.8.6 Spare parts inventory requirements.

2.3.9 The VMS assessment report shall be submitted to the Ministry for review in accordance with Schedule 9 – Review Procedure.

2.3.10 The VMS units shall include the option of local control of the unit via a hand-held terminal or laptop. Maintenance staff shall have access to all message editing, diagnostic features and software through local control.

2.3.11 Connectivity to the hand-held terminal or laptop shall be through Ethernet, USB or RS 232 port. Connectivity to the Data Management Centre shall be via the dedicated wireless network.

2.3.12 A total of three (3) VMS shall be installed at the following locations:

2.3.12.1 EB on Highway 11, west of the Highway 11 interchange;

2.3.12.2 WB Highway 1, west of the Highway 1 interchange; and

2.3.12.3 EB on Highway 1, east of Tower Road on Highway 1.

2.3.13 An existing VMS is located east of the Highway 11 interchange on WB Highway 11, near the existing weigh scale. The vendor for this VMS is ADDCO Inc. The LED VMS is the ADDCO "Brick" DMS Model AFO-2s2A8-1340V. This VMS shall be integrated into the Ministry's VMS networks and traffic management system, operated at the Data Management Centre. Project Co shall review the existing VMS technology at this location and assess the operating software (driver) used by this VMS. Project Co shall prepare an assessment report for review in accordance with Schedule 9 – Review Procedure that includes the cost of design and implementation of an interface to the operating software to facilitate the integration of this VMS into the Ministry traffic management system. Project Co shall include replacement of the VMS as an option in the assessment report.

2.3.14 The existing VMS shall use a wireless modem to transmit data between the device and a local receiver, then via a fiber optic network into the Ministry Data Management Centre at the Data Hub located at 1 Research Drive, Regina, SK. Monitoring and messaging on the VMS shall be controlled from the Data Management Centre at the Traffic Operations Hub, located at 1855 Victoria Ave, Regina, SK. The VPN connection between the Data and Traffic Operations Hubs is discussed in section 2.7 of this Appendix F.

2.3.15 Project Co shall be responsible for selecting the exact location of each VMS structure, accounting for factors including but not limited to sight distance, local weather characteristics, key decision points on the Bypass, geometrics, topography and geotechnical soil conditions.

2.3.16 The approximate locations of the VMS units are shown on Figure 1 in this Appendix F.

2.4 Road-Weather Information System (RWIS) station

Project Co shall prepare a functional and system design for the Road-Weather Information (RWIS) station at the designated location on the Highway 1 corridor for review in accordance with Schedule 9 – Review Procedure.

2.4.1 The RWIS station shall house sensors and technology that monitor weather- related parameters including but not limited to:

2.4.1.1 Environmental variables such as ambient air temperature, barometric pressure, wind speed and direction, and relative humidity; and

2.4.1.2 Local factors such as current surface pavement temperature measured with optical sensors, freezing point of liquid on the surface, depth of snow and rain, and pavement conditions (slush, icy, etc.).

2.4.2 The RWIS station shall use these parameters to predict the formation of "black ice" on the corridor and adverse weather conditions that will require public advance warning and potential road closures. The RWIS station will also provide data to guide maintenance decisions including requirements for plowing and application of de-icing chemicals and sand.

2.4.3 The RWIS station shall be designed and installed on a concrete pad, in a secure, fenced enclosure. The equipment, including sensors, in the RWIS station shall be capable of full operation in temperatures ranging from – 50 degrees C to + 50 degrees C and will have power and communication 24 hours per day.

2.4.4 The RWIS station shall include a CCTV camera, installed on a high mast pole or an existing structure with a view of the corridor. The CCTV camera shall be as specified in Section 2.2 of this Appendix F and have PTZ functionality with a
field of view so that the operator can assess visibility, local conditions and other road-related factors on the corridor. The CCTV camera shall be located within the secure, fenced enclosure and be controlled by the DMC operators in the Traffic Operations Hub.

2.4.5 The RWIS station shall communicate with and be controlled from the Ministry Data Management Centre (Traffic Operations Hub) on a 24 hour basis. The RWIS station shall use the wireless network or a cellular modem connection to communicate with the Ministry Data Management Centre and transmit data. The data shall be sent from the RWIS station to a local receiver and then via a fiber optic network to the DMC. The Ministry data centre shall be able to interrogate
the RWIS station to acquire data on any single piece of equipment. The RWIS station will include central software and device drivers for all equipment that will support the data management of the RWIS station.

2.4.6 The software shall be scalable to permit additional RWIS stations to be added to the network in the future.

2.4.7 Project Co shall ensure that the RWIS station and all devices within the station are protected against unauthorized intrusion and attack. The RWIS station and all devices shall be part of the Cyber Security Audit and Cyber Security Plan as described in Section 1.5.2 of this Appendix F.

2.4.8 The RWIS station shall be located on Highway 1 east of the interchange between Tower Road and the Pilot Butte Access Road. The RWIS station shall be interfaced with the local VMS on Highway 1.

2.4.9 The approximate location of the RWIS station is illustrated on Figure 1 of this Appendix F.

2.4.10 Project Co shall be responsible for selecting the exact location of the RWIS station, considering local conditions including but not limited to availability of right-of-way, power, and communications, accessibility, and geotechnical soil conditions. The RWIS station will include a solar panel with a back-up battery for power.

2.5 Traffic Signals

Project Co shall design and install traffic signal controllers and signal heads at two locations (1) the Pilot Butte Access Road DDI and (2) the intersection of Highway 46 and Highway 364, north of Balgonie. The traffic signal systems at both locations shall include all detectors, wiring, conduit, cabinets, pedestals, poles, electrical and communications systems, advance signage, signal management software, modems and any special hardware as specified below.

2.5.1 At Pilot Butte DDI, Project Co shall review in accordance with Schedule 9 – Review Procedure the available traffic signal controller technologies, undertake an environmental scan and provide the Ministry with an assessment report and recommendations. The report shall consider the following:

- Control of EB to NB and WB to SB Highway 1 off-ramp traffic;
- Control of NB and SB through traffic;
- Raised median locations for the interchange;
- Phasing requirements for the interchange movements;
- Pedestrian and cycling requirements;
- Power and communications requirements;
- Controller standards including National Electrical Manufacturers Association (NEMA) TS-2, Advanced Transportation Controller (ATC) and Model 170;
- Controller types for the adjacent jurisdictions;
- NTCIP compliance;
- Signal coordination with adjacent jurisdictions;
- Signal pre-emption requirements for emergency vehicles;
- Cabinets and pedestal configurations; and
- Cyber security issues and recommendations.

More details are in Appendix H of Schedule 15-2 - Design and Construction.

2.5.2 The unique operation of the DDI requires that CCTV cameras shall be installed by Project Co to monitor the operation of the interchange from the Data Management Centre. The CCTV cameras shall be full pan-tilt-zoom (PTZ) as specified in this Appendix F. The CCTV cameras shall be located such that all movements are visible to the DMC operator.

2.5.3 At Pilot Butte, the signal controllers and CCTV cameras shall transmit data to and from the Data Management Centre (Data Hub) via the wireless and fiber optic network. Project Co shall ensure that the traffic signal controllers, detectors, communication network and related technologies are protected against unauthorized intrusion and attack. The signal system and network shall be protected against any unauthorized operation of the signals, modifications or replacement of signal timing plans and parameters, and any access by non-authenticated users.

2.5.4 The Pilot Butte traffic signal controllers shall be part of the Cyber Security Audit and Cyber Security Plan as described in Section 1.5. of this Appendix F.

2.5.5 The Pilot Butte DDI shall have two signal controllers (north and south ends) and six traffic signal heads (3 each in the north and south ends) as per the "typical" DDI design.

2.5.6 At the intersection of Highway 46 and Highway 364, Project Co shall design and install the traffic signal controller and signal heads. Project Co shall submit for review in accordance with Schedule 9 – Review Procedure the available traffic signal controller technologies and provide the Ministry with an assessment report and recommendations for the signal at the intersection of Highway 46 and 364. The design and installation of the intersection signal shall include wiring, conduit, detectors, cabinets, pedestals, advance warning signage, flashers and poles. Project Co is responsible for any and all traffic engineering and analysis to ensure that the design of the intersection and signals provide a safe operating environment for drivers, pedestrians and cyclists, including the requirement for advance warning signage, barriers and flashers.

2.5.7 The traffic signal controller at the intersection of Highways 46 and 364 shall be remotely monitored, operated and controlled at the Data Management Centre with the ability to download changes and/or new signal timing plans and coordination schemes.

2.5.8 The Highway 46/364 traffic signal controller shall be part of the Cyber Security Audit and Cyber Security Plan as described in Section 1.5.2 of this Appendix F.

2.6 Wireless Network

The wireless network shall utilize SaskTel's "Long Term Evolution" network or "4G LTE" for data communications on the Bypass.

2.6.1 The ITS devices on the Bypass shall have wireless modems that will send

data to a receiver located on a local SaskTel tower. From the receiver, the data will be transmitted into a fiber network, sent to the SaskTel data centre and then to the Ministry Data Management Centre (Data Hub). Project Co is responsible to undertake any structural analysis and engineering, if required, to determine if the receiver may be safely installed on the Sasktel tower. Project Co shall be responsible for any upgrades or reinforcement to the structures, if required.

2.6.2 The wireless and fiber network shall be reliable and available 24 hours per day, and be capable of transmitting high quality video, data and voice over internet to and from the Data Hub located at 1 Research Drive, Regina, SK.

2.6.3 Project Co is responsible for all cyber and network security on any segment of the transmission between the devices and the Data Management Centre. Project Co shall provide any hardware and software for data security including encryption of the data sets.

2.6.4 The wireless and fiber network shall be part of the Cyber Security Audit and Cyber Security Plan, as described in Section 1.5.2 of this Appendix F.

2.6.5 Project Co is responsible to select the location of the receiver so that the signals from the ITS devices will transmit data at the required speed and quality. Project Co shall design, test and install the receiver and wireless network and shall link
all devices to the receiver, including all interfaces and multiplexing equipment, so
that data can be transmitted to the SaskTel data centre and the Ministry Data Management Centre.

2.6.6 Project Co shall be responsible for any and all legal, technical and financial agreements to obtain access to the local tower to install, operate and maintain the receivers and to obtain the use of the SaskTel fiber network and data centre. Project Co shall be responsible to arrange for the interface to the Ministry DMC from the SaskTel data centre.at each location, for review in accordance with Schedule 9 – Review Procedure. The report shall include but not be limited to evaluation of the following factors:

- Network signal strength;
- Signal loss;
- Bandwidth and speed;
- Repeater sites if required;
- Security requirements; and
- Access requirements for maintenance

2.6.7 Project Co shall prepare a test plan for the wireless network and the ITS devices at each location, for review in accordance with Schedule 9 – Review Procedure. The report shall include but not be limited to evaluation of the following factors:

- Network signal strength;

- Signal loss;
- Bandwidth and speed;
- Repeater sites if required;
- Security requirements; and
- Access requirements for maintenance

2.6.8 Project Co is responsible to ensure that the wireless network and devices that communicate and transmit data to and from the Data Management Centre are compliant with Canadian Radio-television and Telecommunications Commission (CRTC) regulations. Project Co shall obtain all necessary approvals and permits from the CRTC and other regulatory agencies.

2.6.9 Project Co shall communicate and coordinate with the Regina Airport Authority located at 1–5201 Regina Avenue, Regina, SK S4W 1B3 to ensure that there is no interference of the ITS technologies with airport navigation or guidance systems. Project Co shall be responsible to obtain any required approvals of the Regina Airport Authority and/or NavCanada during the design phase.

2.7 Ministry Data Management Centre

The central facility of the Bypass is the Ministry Data Management Centre (DMC).

2.7.1 For ITS devices on the Bypass, there are two data components:

2.7.1.1 Traffic operations component which will include data from ITS Infrastructure for traffic that will be shared with Project Co. The data will be shared through the administrative portal to provide access to Project Co staff from any web browser; and

2.7.1.2 Commercial Vehicle Enforcement component which will include goods movement data from the CVE pre-screening stations that will not be available to Project Co. This data will be strictly for the use of the Ministry staff via the work stations.

2.7.2 The Bypass ITS Infrastructure devices shall transmit their data over the wireless network to receivers inter-connected to the fiber network, through the SaskTel Data Centre and then to the Ministry DMC.

2.7.3 Project Co shall be responsible for preparing detailed system design of the DMC, DMC hardware specifications and procurement of the DMC hardware as well as for all ITS application software including device drivers and commercial off-the- shelf (COTS) software for the work stations. The Ministry will be responsible to provide the facility for both hubs, operator staff at the work stations in the traffic operations hub, and technical support in the data hub. The Ministry shall also be responsible for hardware, installation, operation, maintenance and rehabilitation (upgrading) in the DMC.

2.7.4 The Data Management Centre shall be comprised of two separate hubs, located in two different buildings as follows:

2.7.4.1 Data Hub (1 Research Drive)

The "Data Hub" is located at 1 Research Drive in Regina, SK. Data will be transmitted between all ITS Infrastructure field devices on the Bypass corridor via the wireless network, to the SaskTel 4G LTE fiber network and data centre and to the Ministry Data Hub. Project Co is responsible for any legal, technical and financial lease agreements to access and erect the receiver on the local towers, for power and communications connections to the receiver and access from the receiver into the SaskTel 4G LTE network, the SaskTel fiber optic network, and the SaskTel Data Centre. Project Co shall be responsible for all maintenance and any upgrades of the receiver and related software during the Works.

Project Co shall design the DMC hardware and software environment for the ITS Infrastructure on the Bypass and shall procure the DMC hardware, working closely with the Ministry, and turn over the DMC hardware to the Ministry after procurement. The Ministry shall review the final DMC design and specifications for hardware and shall install the DMC hardware after receiving it from Project Co. Upon receiving an endorsement "Reviewed" or "Reviewed as Noted" pursuant to Schedule 9, Review Procedure Project Co shall develop, test, install, maintain and update the ITS application software on the hardware environment provided by the Ministry. Project Co shall work closely with the Ministry to facilitate knowledge transfer for maintenance.

The data management Infrastructure shall be hosted at the Data Hub and will include at least four servers to handle the web applications, database and central software as well as a hot spare. The database server shall have sufficient storage to retain five (5) years of data, voice and video.

The real-time data flow shall be received as "incoming" into the DMC Data Hub where it will be simultaneously processed into real time and archived formats and sent to the following locations:

- Real time traveller information media including Highway Hotline and other ATIS applications. The real time status will be displayed in the DMC Traffic Operations Hub for assessment by operators; and
- Archived storage for future retrieval by the Ministry via a web-based administrative portal.

Project Co shall design and install the administrative portal, accessible by any web browser, to retrieve archived data on a 24 hour basis. Authorized users shall have access to the data including the staff of the Ministry and other departments of the Government of Saskatchewan,

Project Co, and partner agencies. The Ministry shall administer the list of authorized agencies and users that can access the portal.

The portal users shall have the ability to request customized queries that will retrieve data by the following parameters:

- Temporal – by time of day, day of week, month or year;
- Geographic – by corridor or location; and
- Geo-fencing – by municipality or region.

The queries shall include an "all data" option to request information that will be provided in any available format. The reports shall be available in a variety of formats including PDF.

Project Co shall submit the system design of the administrative portal to the Ministry for review in accordance with Schedule 9 – Review Procedure, including a test plan, prior to commissioning.

Project Co shall work with the Ministry Information Technology Office (ITO) staff to ensure that the system design and specifications for the Data Hub, including all hardware, software and devices, meet the Ministry requirements for network connectivity, security, redundancy, and disaster recovery processes and protocols. Project Co shall prepare the specifications and system design for Ministry ITO review in accordance with Schedule 9 – Review Procedure. Project Co shall procure, install, test, maintain and update the application software for the DMC under Ministry ITO supervision during the Project Term.

ITO is the inter-governmental group that provides information technology services and support to all Saskatchewan government departments and is housed in the building at 1 Research Drive in Regina, SK.

Project Co shall design the Data Hub, including all racks, wiring, harnesses and interfaces, within a secure temperature controlled environment for the communication and computer area. Project Co is responsible to determine if the available space within the building meets the requirement for a "secure, temperature controlled environment" through site inspection(s) and meeting(s) with ITO staff. If not, Project Co shall provide a separate enclosed area for the communication and computer racks.

Project Co will be provided with vacant space within the building. The Ministry will be responsible to provide operations staff following commissioning. The Ministry will also provide technical staff on a 24-7 basis for system support, operations and maintenance.

All space in the Data Hub shall be accessible and barrier-free as per the Saskatchewan Uniform Building and Accessibility Standards Regulations.

2.7.4.2 Traffic Operations Hub (1855 Victoria Ave.)

The "Traffic Operations Hub" is located at 1855 Victoria Avenue in Regina, SK. The Traffic Operations Hub will house the ITS Infrastructure related to operations including the traffic control room. Project Co shall prepare the detailed system design and specifications for the Traffic Operations Hub for Ministry review in accordance with Schedule 9 – Review Procedure. Project Co shall procure the hardware in the Traffic Operations Hub and turn it over to the Ministry. The Ministry shall be responsible for the testing and installation of the following in the traffic control room:

- Two work stations (on or before the Substantial Completion Date) equipped with computers, monitors, client software and internet access; (The Ministry may add, pursuant to Schedule 19, the Variation Procedure, up to three more (for a total of five) work stations,)
- One central high definition video wall display linked to both work stations;

Project Co shall design, install, test and maintain the following in the traffic control room:

- Central software to communicate with the ITS devices from the work stations; and
- Device drivers required to interface with the Bypass ITS devices.

The work stations shall be equipped with joy sticks or equivalent to manually control the CCTV cameras and other devices. Each work station shall have the ability to move files seamlessly to and from the video wall including still images, files or CCTV camera images. The work station computers shall be equipped with Windows 7 operating systems or higher, all required application software and a secure, login system to control access. Project Co shall have access to Bypass traffic data through this secure login system but not commercial vehicle pre-screening data. Project Co will provide design and specifications for the two work stations.

The video wall shall be located so that it is visible and clear to operators at all work stations. The video wall shall be scalable to support two work stations on the Substantial Completion Date and up to 5 work stations in the future.

Project Co shall design and procure and the Ministry shall install the two work stations prior to the Substantial Completion Date and the Ministry may add up to three more (to make a total of five) work stations pursuant to Schedule 19, Variation Procedure.

The video wall shall fit in approximately 5 feet by 20 feet of space on the wall facing the operator work stations and be configurable into any combination of between 1 and 10 separate images. The video wall may be comprised of separate units. The video wall units must be full high definition quality with an aspect ratio of 16:9, a display technology that can be properly cooled, and of a weight and size that can be structurally supported in the DMC. The video wall shall include video management software that allows and supports the configuration and transfer of images between the units.

A conceptual floor plan of the Traffic Operations Hub is shown in Figure 3 of this Appendix F. Project Co shall produce a final conceptual design and floor plan for approval by the Ministry ITO staff before design and construction, based on site visits, meetings with the Ministry and a review in accordance with Schedule 9 – Review Procedure of the available space allocated to this facility. The floor plan for the Traffic Operations Hub must accommodate the two work stations for the Bypass ITS operators. Space must be left available for installation of additional work stations that will be deployed by the Ministry for future expansion and the supervisor's work station. The floor plan shall also
accommodate the HD display area.

The Project Co shall not be given dedicated physical space in either the Data Hub or the Traffic Operations Hub. If Project Co requires access for maintenance of software, coordination shall be through the Ministry.

All space in the Traffic Operations Hub shall be accessible and barrier- free as per the Saskatchewan Uniform Building and Accessibility Standards Regulations.

2.7.5 The operational layout for each hub must fit within the available space in each building.

2.7.6 Project Co is responsible for any and all legal, technical and financial agreements to modify and occupy the current facility.

2.7.7 The Ministry shall use an existing "virtual private network" (VPN) connection to transmit the data between the two hubs (data and traffic operations). Project Co shall submit a test plan for Ministry review in accordance with Schedule 9 – Review Procedure of the VPN connection for data transfer between these two locations. Project Co shall conduct the test of the VPN connection under Ministry supervision which will include but not be limited to speed, available bandwidth, and latency. Project Co shall obtain approval of the Ministry to conduct the test and prepare a test report to be submitted to the Ministry for review in accordance with Schedule 9 – Review Procedure.

2.7.8 The DMC systems in both hubs shall be NTCIP compliant.

2.7.9 The Data Management Centre shall be scalable to add future corridors and

functionality. The Data Management Centre shall communicate with and support the following devices and facilities on the Bypass and integration of devices outside of the Bypass on the Substantial Completion Date:

- All devices on the Bypass including:
  - Traffic data counting stations;
  - CCTV cameras;
  - Variable message signs (VMS);
  - Road-weather information systems (RWIS);
  - Traffic signals, controllers and CCTV at the Pilot Butte interchange and the intersection of Highways 46 and 364; and
  - Commercial vehicle pre-screening stations.

- Additional devices in the Province outside of the Bypass , including:
  - Thermistors;
  - Over-height detectors;
  - Commercial vehicle inspection stations (VIS);
  - CCTV cameras;
  - VMS;
  - Traffic counters and classifiers;
  - WIM stations; and
  - Remote inspection stations.

Project Co shall ensure that the ATMS software discussed in Sections 2.7.10, 2.7.11 and 2.7.12 as well as the generic application programming interface (API) discussed in Section 2.2.4 can accommodate the integration of current and future devices.

2.7.10 The Data Management Centre shall include Advanced Traffic Management System (ATMS) central software that will monitor traffic flows on the Bypass on a 24-7 basis. The ATMS software shall continuously monitor the data from the Bypass ITS devices including speeds, volumes, headway (gap), and lane occupancy to determine the likelihood of an incident and alert the operators in the Traffic Operations Hub. Project Co is responsible for the provision, testing and commissioning of the ATMS software. Testing of the ATMS software shall be done with a simulated dataset due to the limited density of TDC units at Substantial Completion.

2.7.11 The ATMS software shall be comprised of several modules including incident management, traveller information and road-weather systems as follows:

- The incident management system module is described in Section 2.2of this Appendix F. The incident management system will be comprised of 4 sub- systems including incident detection, response, verification and clearance/site management. The ATMS software shall interface to the TDC, CCTV cameras and VMS devices on the Bypass. The incident management system shall use Advanced Traffic Management System (ATMS) software to assess traffic data, unusual patterns that indicate a high probability of a non-recurring incident, and alert the DMC operators in the Traffic Operations Hub through activation of the CCTV cameras for verification;

- The traveller information system module shall provide the DMC operators at the Traffic Operations Hub with access and interfaces to communication media. The operators shall have access to systems such as Highway Hotline, social media, VMS, traffic radio, and agency websites to provide information on road-related issues to the public and customers. The traveller information system module shall include all drivers and interfaces to the VMS network to permit operators to initiate messaging. As part of this module, Project Co shall consult with the Ministry and supply a list of available Content Management System (CMS) products to manage data and information for the web sites. Project Co shall provide the Ministry with an assessment of these currently available CMS products for Ministry evaluation; and

- The road-weather information system (RWIS) module shall provide the operator with direct access to the RWIS station data and information. The RWIS module will make recommendations to the operator on road closures, alerts and VMS messages. The RWIS module shall provide the operator with control of the RWIS CCTV camera that will allow assessment of visibility and local conditions. The RWIS module shall have interfaces to Saskatchewan emergency management and public safety agencies in the event of natural and local weather-related disasters. These agencies include but are not limited to provincial agencies, municipalities, RCMP, and Environment Canada. This module shall support the integration of other agency's RWIS stations into the ATMS software through the generic API.

2.7.12 The central ATMS software shall be scalable and support additional devices, corridors and functionality. As per Section 2.2.4, the ATMS software shall include a generic API for other application interfaces. The generic API can be customized by vendors and service providers, the Ministry and partner agencies in the future. These APIs shall be submitted by Project Co to the Ministry in accordance with Schedule 9, the Review Procedure. The software shall allow the addition or removal of devices and corridors via an interactive graphic user interface (GUI).

2.7.13 The displays shall be capable of showing a full GIS-based map of the network and Bypass, including the ITS devices represented by clickable icons. Clicking the icons will expand the device window and provide access to additional information on device status and data specific to that device. The central ATMS software shall be capable of managing the device data including video and incorporating them on the displays.

2.7.14 Project Co shall prepare a high level conceptual design, including system architecture, of the ATMS software for review in accordance with Schedule 9 – Review Procedure. The design shall incorporate all modules and systems in a test environment. The conceptual design shall use a simulated dataset to provide proof of concept of the ATMS software. Project Co shall submit a conceptual design report to the Ministry for review in accordance with Schedule 9 – Review Procedure.

2.7.15 The software and applications within the DMC shall be part of Project Co's Cyber Security Audit and Cyber Security Plan as described in Section 1.5.2 this Appendix F.

2.7.16 Upon receiving a comment "Reviewed" or "Reviewed as Noted" pursuant to Schedule 9 – Review Procedure of the conceptual design report, Project Co shall prepare a detailed system design that includes a formal test plan, including performance criteria, for Ministry review in accordance with Schedule 9 – Review Procedure. The test plan shall demonstrate the accuracy, reliability, and efficiency of each module. Project Co shall prepare a final test report for Ministry review in accordance with Schedule 9 – Review Procedure.

2.7.17 NOT USED

2.7.18 The Data Management Centre shall monitor the Bypass traffic as the corridor is designated as an over-height and over-dimensional route. Data and permitting documentation supporting over-height and over-weight trucks shall be directed and operated through the Data Management Centre.

2.8 Commercial Vehicle Pre-Screening Stations

Commercial vehicles travelling on the provincial highway system are randomly inspected and weighed by Highway Traffic Officers from the Ministry. Commercial vehicles travelling on the Bypass Infrastructure shall be inspected and weighed in a similar manner and frequency.

2.8.1 The commercial vehicles are subject to inspection at designated weigh scales and vehicle inspection stations. At these locations, the officers have the authority to check the following:

- Check for weight and size compliance;
- Conduct a check of the vehicle, on and off the highway;
- Check documentation and permits on all commercial vehicles;
- Conduct an inspection of all cargo, for contents and securement;
- Check the safety equipment on the truck and any inspection certificates;
- Check any dangerous goods that are being transported;
- Check the drivers licence and registration of the vehicle and carrier;

2.8.2 The officers can provide assistance to disabled commercial vehicles that enter the scale and enforce the Provincial and Federal rules of the road.

2.8.3 Project Co will not be permitted to construct pull-out areas along the Bypass mainline which is defined in the Technical Requirements.

2.8.4 The Ministry will prepare a Commercial Vehicle Enforcement (CVE) Strategy which may provide recommendations on enforcement infrastructure. The Ministry and Project Co shall work closely to ensure that the CVE strategy recommendations are implemented prior to Substantial Completion.

2.8.5 Project Co shall be responsible for the design and construction of four pre-screening sites for commercial vehicle enforcement. Each pre-screening site shall have the following ITS Infrastructure:

2.8.5.1 A weigh-in-motion (WIM) scale using bending plate load cells. Equivalent technology such as quartz will require Ministry approval;

2.8.5.2 Licence plate reader (LPR) software integrated with the CCTV cameras;

2.8.5.3 Traffic classifier;

2.8.5.4 Four (4) CCTV cameras (side shot on each door, front plate and back plate) to capture views of the truck; and

2.8.5.5 One (1) CCTV camera showing the truck within the full field of view, separate from the 4 cameras in section 2.8.5.4. This camera shall be a full pan-tilt-zoom (PTZ) unit with 360 degree rotation as described in Section 2.2 in this Appendix F;

2.8.6 The pre-screening sites shall be remotely linked to and controlled at the Data Management Centre, Traffic Operations Hub, for coordinated remote operation, analysis and support.

2.8.7 Project Co shall be responsible to ensure that all devices and software used in the pre-screening sites are protected against unauthorized intrusion or attack. Project Co shall provide any necessary software and hardware to provide cyber security to prevent unauthorized users to access, modify, remove or replace data from the pre-screening sites.

2.8.8 The pre-screening sites shall be part of Project Co's Cyber Security Audit and Cyber Security Plan as described in Section 1.5. of this Appendix F.

2.8.9 Project Co shall prepare a system design and test plan for Ministry review in accordance with Schedule 9 – Review Procedure including each device and integration into the DMC. The test plan will include but not be limited to accuracy and reliability of the equipment, including WIM, LPR, CCTV, credentialing and classification technology.

2.8.10 The pre-screening sites shall be located at:

- Highway 11, northwest of the Highway 11 interchange (median);
- Highway 1, west of the Highway 1 interchange (median);
- Bypass mainline, west of Highway 33 (WB traffic only); and
- Bypass mainline, east of Highway 6 (EB traffic only).

2.8.11 The median pre-screening sites will cover 4 lanes of traffic (2 lanes in each direction). The WB and EB pre-screening sites will cover 2 lanes of traffic.

2.8.12 The approximate locations of the pre-screening sites are denoted on Figure 2 of this Appendix F.

2.8.14 Project Co shall be responsible for selecting the exact location of the pre-screening sites, based on the local geotechnical, topographical and geometric conditions.

Figure 1: ITS Infrastructure Approximate Locations

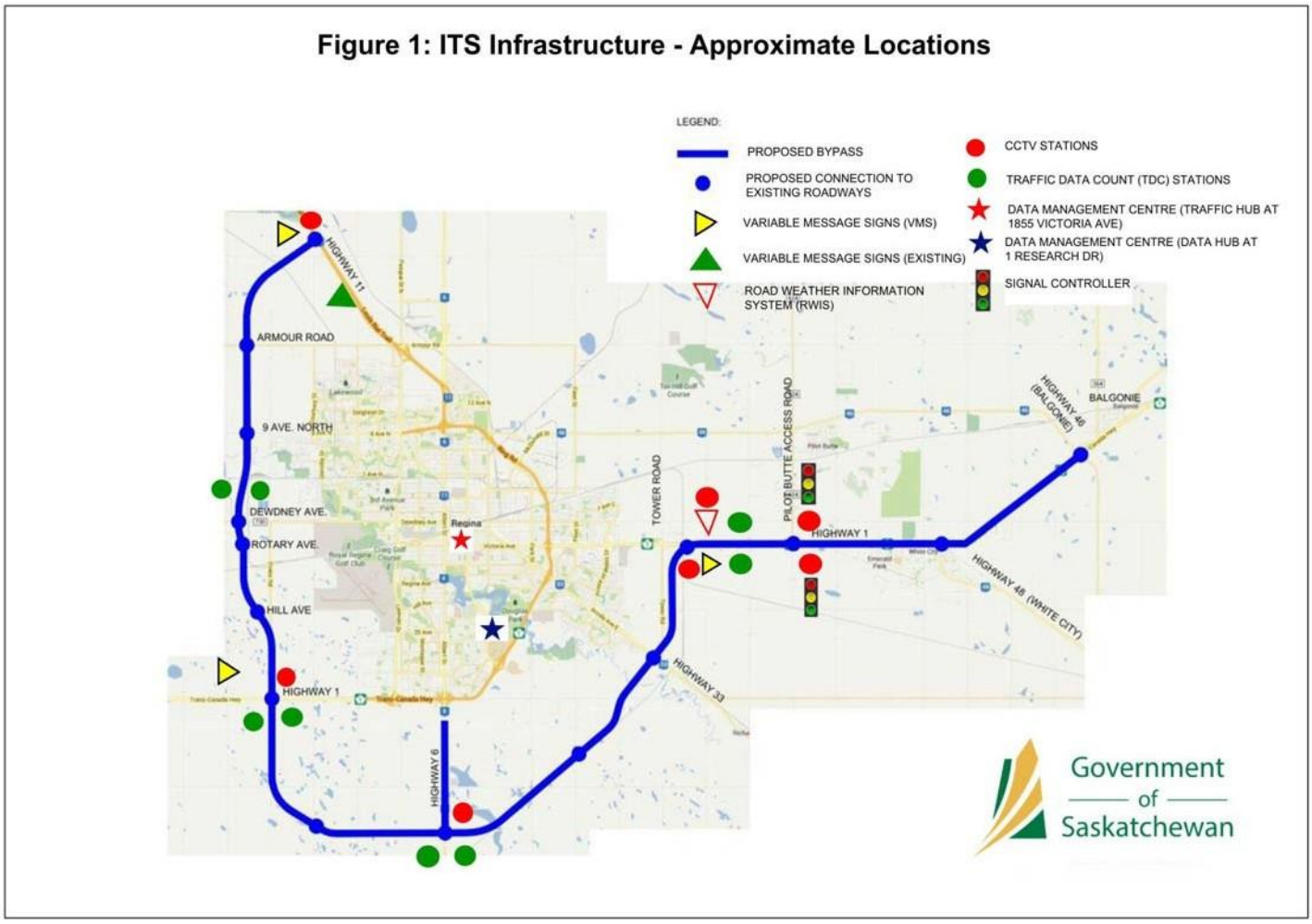


Figure 2: Regina Bypass Project (RBP) Truck Pre-Screening Sites

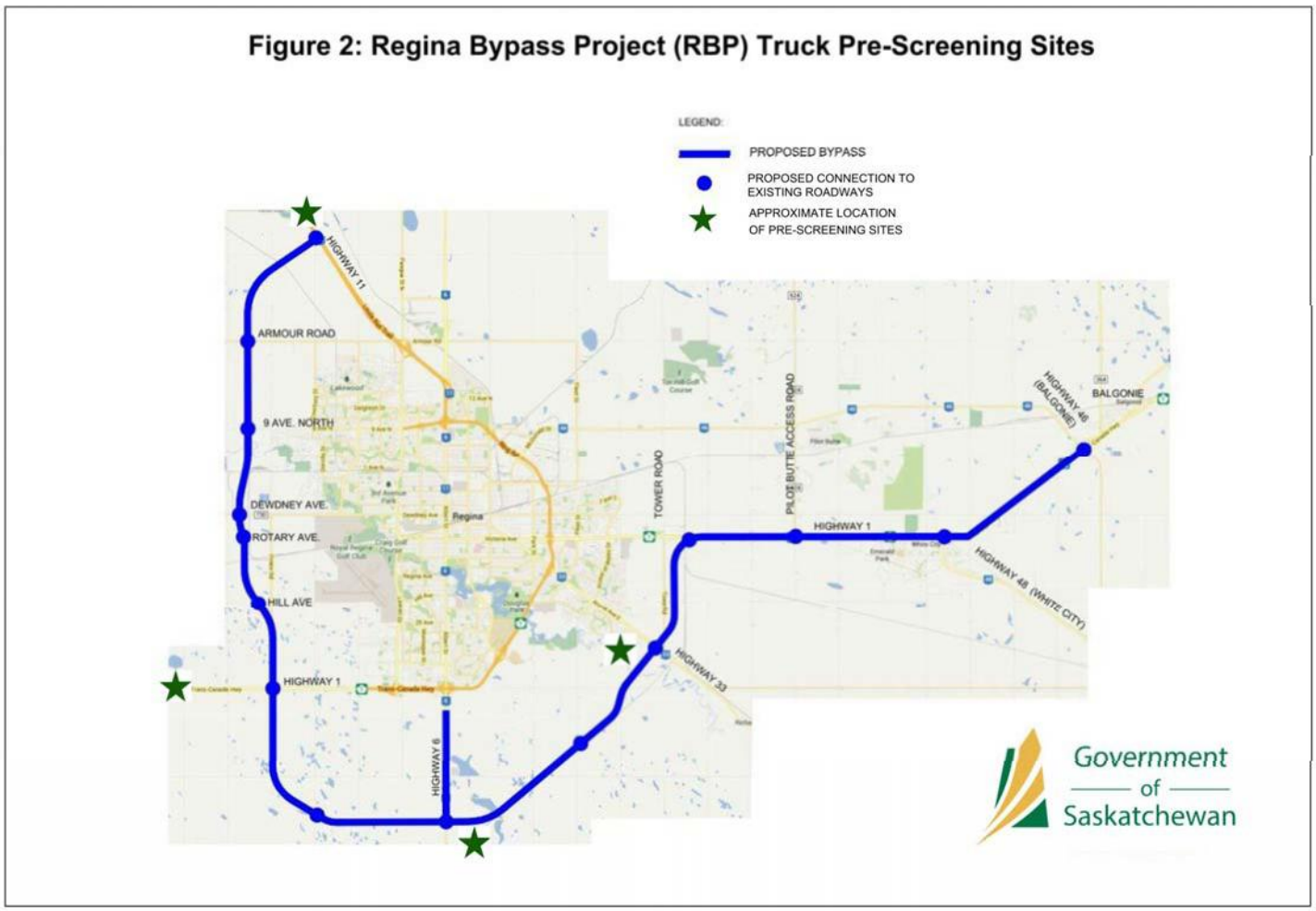
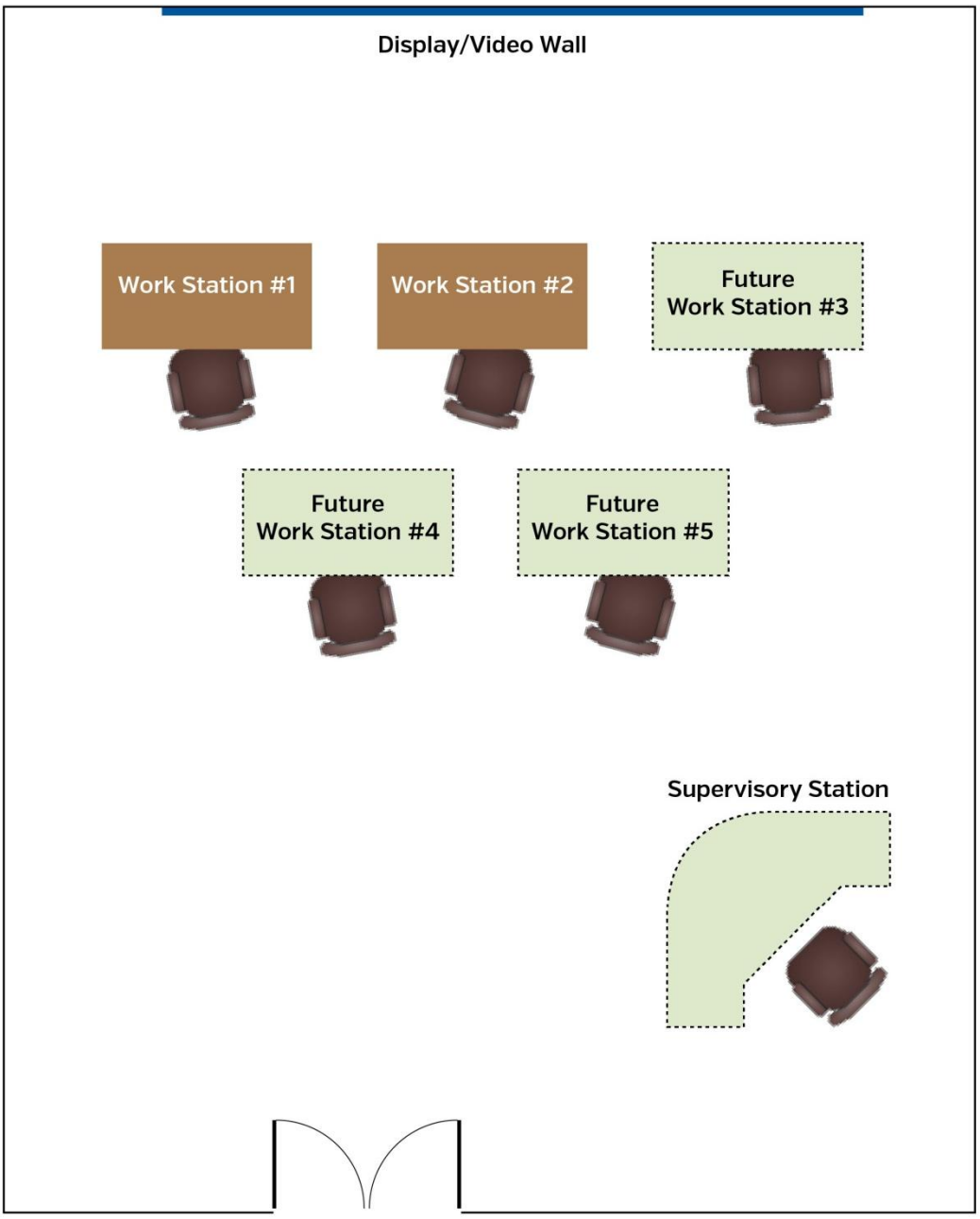


Figure 3: Conceptual Floor Plan for Data Management Centre, Traffic Operations Hub



Note: Computer/Communications equipment to be housed in a secure, temperature-controlled enclosure.in the Data Hub.

The work stations and video wall will be housed in the Traffic Operations Hub.

Attachment 1: Regina Bypass ITS Design Criteria

Regina Bypass ITS Design Criteria November 6, 2014

1. General

The general requirement for the Regina Bypass will be for a high speed, free flow corridor. This document discusses the needs and recommended elements of the Intelligent Transportation System (ITS) components of the Regina Bypass.

It should be noted that the "needs assessment" for the area was addressed through the development of a Provincial ITS Technical Strategy which was undertaken in 2014 by the Saskatchewan Ministry of Highways and Infrastructure (MHI). The needs assessment process involved meetings and discussions with 14 internal departments as well as responses to a questionnaire sent to 14 external agencies. In addition, a review of the background documentation including modelling results, interviews with staff that worked on the project to date, a key meeting held with the Saskatchewan Ministry of Highways and Infrastructure (MHI) on August 6, 2013, a cost estimate workshop held on August 13, 2013 and numerous other meetings and discussions assisted this process. The needs of MHI for the basic elements of ITS infrastructure on the Regina Bypass were refined, confirmed and integrated into the Provincial ITS Technical Strategy.

2. Assumptions

The following assumptions were used as a guide for the ITS recommendations:

- Design speed is 130 km/h and posted speed is 110 km/h;
- Traffic volumes are consistent with the forecast in "West Regina Bypass Functional Planning Study", June 2013;
- Design vehicle is the WB-20;
- Population is 300,000;
- The Global Transportation Hub (GTH) will, in the future, achieve full "build out" with forecast external trips of 6,426 daily;

3. Description

A review of previous planning documentation shows clearly that a high volume and percentage of trucks are expected to use the corridor. To the west of the Bypass, the GTH is a unique and important generator of traffic. As the GTH develops, the truck trips will also increase and will need to be supported by the ITS infrastructure. The West Regina Bypass Traffic Forecast, prepared by AE for MHI on November 2012, predicted significant inbound and outbound truck trips. Table 6.28 on Page 6-20 shows that the GTH is predicted to generate the following trip volumes:

Daily Traffic	*AM Peak Hour*			*PM Peak Hour*		
GTH	*Total*	*Inbound*	*Outbound*	*Total*	*Inbound*	*Outbound*
6,426	366	246	120	427	150	277

4. ITS Requirements – Basic

In terms of the basic ITS infrastructure, the following requirements have been identified:

a. Traffic Data Stations for traffic counting and classification

Traffic data stations are required for several purposes:

(1) To provide real time traffic flow data incident management purposes;
(2) Provide a historical record of the general purpose (GP) and truck traffic on the Bypass; and
(3) To measure the equivalent single axle loads (ESAL) being supported by the Bypass;

The data stations are cost effective and will provide invaluable information to support the content needs of the VMS system, incident management for MHI, and planning information for future development.

The data station locations were discussed with MHI at the August 6 1 meeting and August 81 workshop as well as in additional meetings. The following locations are part of the basic package:

Location	*Direction*	*Number of Stations*
North of Dewdney on Bypass	SB and NB on Bypass	2
South of Highway 1 west on Bypass	SB and NB on Bypass	2
Highway 6 south of Bypass	SB and NB on Highway 6	2
Highway 1 east of Tower Road	EB and WB on Highway 1	2
	TOTAL	8

Data stations can utilize different technologies. Loop detectors are generally the most reliable and cost effective but are prone to failure in areas of extreme weather and heavy truck traffic. These loops are difficult to replace during periods of poor weather outside of the construction season. Wireless technologies such as radar and beam sensors are not affected by weather or traffic loads and can operate reliably, although they are more costly.

A typical radar data station will include a detector on a pole, connected to a server in a weather-proof cabinet. The data will be transmitted from the cabinet via the wireless network to a receiver that will send it to the Ministry Data Management Centre. The radar detector can count across multiple lanes in real time and can also measure other parameters such as classification (truck) counts, headway, lane occupancy and speed. The detector is directional and if data is required in both directions, two units will be required.

b. Variable Message Signs (VMS)

Variable Message Signs (VMS) serve a number of functions in any ITS program. VMS are an important component of any enroute traveller information system to advise motorists of real time traffic conditions, alternate route choices, and adverse weather conditions.

The permanent new VMS structures used on the Bypass will have 3 lines of text, a standard library of messages as well as the ability to create custom messages. They will be mounted on cantilevered structures and remotely connected to and controlled at the MHI Data Management Centre via a wireless network. The VMS can also be controlled via a handheld terminal or a laptop.

VMS are typically located prior to key decision points in the network, depending on the posted speeds, about 300 to 500 m in advance. The VMS can display up to 3 lines of text, usually with 25 to 30 characters each, including spaces. A total of three (3) new VMS locations and one (1) existing location have been identified as part of the basic ITS package for the Bypass. The locations are as follows:

Location	*Direction*
Highway 11 West of Bypass	EB Highway 11
Highway 1 East of Tower Road	EB Highway 1
Highway 1 West of Bypass	WB Highway 1
Highway 11 near weigh scale (integration work) *see "Note" below	WB Highway 11

*Note: The existing VMS on H1ghway 11 for northbound traffic (near the weigh scale) will be integrated into the VMS system. Work is required to support a review of current technology, installation of a wireless node, software work and site inspection.

c. CCTV Stations

Typically, CCTV cameras on a major highway support several functions:

(1) As part of an incident management system, CCTV cameras are used to verify accident locations, severity and extent in real time. Typically, these cameras have "pan-tilt-zoom" (PTZ) functionality with remote control