I-95 HOV/HOT Lanes Project

Exhibit C

Technical Requirements

Attachment 1.10

Security Requirements for Concessionaire Operated Critical Infrastructure Facilities and Structures

Security Requirements for Concessionaire Operated Critical Infrastructure Facilities and Structures

The Department and the Concessionaire will mutually agree during the Construction Period to the requirements of the Security Management Systems (SMS) and protocols for the Express Operations Center which may include requirements and/or protocols listed below. All costs and funding associated with these requirements and protocols will be mutually agreed between the Department and the Concessionaire.

Definitions

1. "SMS" - Throughout this document the term Security Management Systems ("SMS") is intended to include all systems and equipment that directly and indirectly relate to the physical security of the facility, structure or compound the facility or structure is located on. Examples include but are not limited to Physical Access Control Systems (PACS), Cipher locks, security surveillance systems (CCTV), intrusion detection, security lighting, security related fiber optic and wireless communications systems and all associated hardware, security fencing, gates, gate operators, intercommunications, bollards and other forms of security systems and technology. SMS does not include standard door and/or office door knob locks and keys.

Documents

The Concessionaire shall adhere to the below listed policies, procedures, or laws pertaining to Criminal History Records Checks, Critical Infrastructure Information / Sensitive Security Information (CII/SSI), Freedom of Information Act requests and Records Retention pertaining to security.

1. The Department's Criminal History Records Check Policy (DPM 1-25)
2. The Department's Freedom of Information Act Policy (DPM 1-5)
3. The Department's CII/SSI Policy and Guide
4. Commonwealth of Virginia Records Retention Schedule(s) 108 and/or other applicable

Construction Period

1. The Department shall review and approve of all plans containing SMS components to determine the extent and type of needed SMS systems and potentially specific placement of components of the SMS. The Department shall

review the technical specifications and/or equipment to be used in order to ensure compatibility, interoperability, and integration with current systems utilized by the Concessionaire and the Department.

2. In general, through layered security, the following types (not all inclusive) of SMS will need to be incorporated into the facility or structure to mitigate common security vulnerabilities:
    a. Perimeter intrusion detection
    b. Vehicular and pedestrian access control (exterior)
    c. Access control (interior)
    d. Security camera system (exterior & interior)
    e. Security Lighting
    f. Security Network
    g. Interoperability with existing Department Security systems
    h. Other as determined necessary
3. The Concessionaire shall be responsible for any and all onsite security and security planning.

Operations Period

1. The Department shall have compliance oversight authority in order to ensure all SMS equipment, components and related security protocols are maintained at the Express Operations Center.
2. The Concessionaire shall allow the Department remote viewing and monitoring access to all security surveillance camera systems (CCTV) and shall allow the Department to extend this remote viewing capability to Department security consultants or local, state and Federal security partners who perform Homeland Security initiatives such as DHS, JTTF, USCG, VSP, etc.
3. The Concessionaire shall ensure all security surveillance camera systems (CCTV) operating platforms remain interoperable with security surveillance camera systems (CCTV) operating platforms utilized by the Department.
4. The Concessionaire shall be responsible for maintaining all SMS in accordance with manufacturer's recommendations and industry best practices, and will ensure all SMS is maintained in a functional and operational capacity.
5. The Concessionaire shall maintain a SMS preventative and corrective maintenance program, to include records documentation of all preventative and corrective maintenance activities.
6. The Concessionaire shall maintain and be responsible for all SMS monitoring and all associated SMS administrational functions.

7. The Concessionaire shall provide the Department a detailed inventory of all SMS installed to include location, SMS equipment documentation, including but not limited to as-builts, installation manuals, user manuals, programming manuals, training manuals, warranty documentation, etc.
8. The Concessionaire shall not remove, relocate, change, alter, disconnect or impede any piece of SMS equipment without the Department's prior review and approval, unless it's a direct replace in kind or upgrade.
9. The Concessionaire shall utilize, operate and incorporate all SMS into Concessionaire's daily operational protocols and procedures.
10. The Concessionaire shall ensure all staff is adequately trained in the use and operations of SMS equipment and protocols.
11. The Concessionaire shall designate an employee to serve as an onsite security representative. This representative shall be the Point of Contact (POC) with the Department responsible for coordinating security initiatives and programs with the Department.
12. The Concessionaire shall notify the Department of all security requests (i.e. requests for security information, assessments, and tours, to include foreign visitor's tour requests, etc).
13. All foreign visitor tour/site visit requests will be forward to the Department for processing in accordance with FHWA's Office of International Programs protocols.
14. The Concessionaire shall not release any security related information to include SMS information without the consent of the Department. FOIA requests for security information will be handled in accordance with the Department's FOIA policy and procedures; additionally the Concessionaire shall notify the Department of all security related FOIA requests.
15. The Concessionaire will notify the appropriate VDOT Traffic Operations Center of all suspicious activity, or criminal activity in addition to reporting to local authorities having jurisdiction.
16. The Concessionaire shall provide the Department, Department consultants or Federal security partners access to Concessionaire operated Operations Center(s), SMS equipment, components, systems and SMS maintenance records for the purpose of completing SMS compliance reviews to ensure SMS is being maintained in a functional and operational capacity. Adequate notice shall be given to Concessionaire, prior to any compliance review visit.
17. The Concessionaire shall support local, state and federal security initiatives involving the Express Operations Center and will allow deployment of equipment which supports security and or anti-terrorism operations, on the Express Operations Center at the discretion of the Department.
18. The Concessionaire in accordance with the Department's Criminal History Records Check Policy (DPM 1-25) shall ensure all persons to include the Department, contractor(s) and or subcontractor personnel working at, or having

unrestricted access to the Express Operations Center, or having access to designated CII/SSI information have been vetted through the Department's Criminal History Records Check process.

19. The Department reserves the right to require the Department's Criminal History Records Check on any Department, contractor and or subcontractor personnel.

20. The Concessionaire shall ensure all documents which are exempt from the FOIA under COV §2.2-3705.2., are marked in accordance with the Department's CII/SSI policy. Concessionaire shall consult the Department for any CII/SSI marking or handling guidance.

21. The Concessionaire shall develop and incorporate business continuity, resiliency, and emergency action planning as an element of their planning and operations at the Express Operations Center and HOT Lanes Project. It is the Concessionaire's responsibility, during the Construction Period and Operations Period to plan, develop, maintain and test these plans in accordance with Commonwealth of Virginia and federal requirements. The Department will have compliance oversight authority to verify that these elements do in fact exist, that they are maintained and tested according to industry best practices and that the level of preparedness will reasonably assure rapid recovery at minimum and continuous operation at best.

22. The Concessionaire shall ensure that all voice communications systems meet FCC requirements and are of such nature that will foster effective interoperability.

23. The Concessionaire shall ensure and document all employees, to include contractors working in an employee position, have completed the State's Terrorism and Security Awareness Orientation training or state equivalent versions. The Concessionaire shall initiate and maintain the same level of NIMS competency as equivalent Department staff positions.

24. The Concessionaire shall work directly with the Department to implement and maintain all security, NIMS, Emergency Response, Incident Management, programs, policies and procedures which may not have been addressed in all other associated contractual documents pertaining to the Express Operations Center and HOT Lanes Project, in order to maintain the same level of security, NIMS, and Emergency Response, Incident Management which the Department maintains.

25. The Department's Criminal History Records Check Policy (DPM 1-25) shall be followed, which may require background checks for those entities placing equipment on designated Critical Infrastructure facilities and structures or the right of way thereof, and therefore needing access to said equipment.