

Vehicle Infrastructure Integration (VII)

Infrastructure Lexicon



February 26, 2007
Version 1.1

Booz | Allen | Hamilton

This report is confidential and intended solely for the use and information of the company to whom it is addressed.

Acceptance / Approval Page

// // _____ Reviewed by _____
David Cline Date
Quality Assurance

// // _____ Reviewed by _____
Mark Lawrence Date
Deputy Project Manager

// // _____ Approved by _____
Craig Pickering Date
Project Manager

// // _____ Approved by _____
Bill Jones Date
US Department of Transportation

DOCUMENT CHANGE HISTORY

Date	Author	Description
11/09/2006	Booz Allen Hamilton	1.0 Released as part of the SDN Subsystem Specification, Version 1.0
12/12/2006	Booz Allen Hamilton	VII Infrastructure Lexicon released as a separate document
12/19/2006	Booz Allen Hamilton	Added new term "Monitor" per ERB suggestion.
12/20/2006	Booz Allen Hamilton	Added new term "Delivery Instructions" per ERB suggestion.
02/01/2007	Booz Allen Hamilton	Added new terms "Remote Probe Data Message Subscription" & "Differential Correction Service"
02/09/2007	Booz Allen Hamilton	<ul style="list-style-type: none"> - Updated Security terms "Security Event", "Denial of Service", "Unauthorized Access", per ERB suggestion. - Added new Security terms: "IP Spoofing", "Password Attacks", "Man-in-the-Middle Attack", "Application Layer Attacks", "Network Reconnaissance", "Trust Exploitation", "Virus and Trojan Horse Applications", and "Initial Registration/Certification"
02/12/2007	Booz Allen Hamilton	<ul style="list-style-type: none"> - Added new terms "Services", "Nonpersistent Message Delivery", "Traffic Conditioning", "Political Boundary", "Performance Report", and "Capacity Report".

Table of Contents

1. INTRODUCTION	1
1.1 SCOPE	1
2. LEXICON	2

1. INTRODUCTION

This document, the *Vehicle Infrastructure Integration (VII) Infrastructure Lexicon*, is based on guidance and information provided by the United States Department of Transportation (USDOT), subsequent meetings and discussions, and agreed upon assumptions by the USDOT and Vehicle Infrastructure Integration Consortium (VIIC). Every effort has been made to ensure the content and approach in developing this document reflects available guidance from the USDOT and accurately reflects the overall scope and intent of VII's objectives.

1.1 SCOPE

This document details the formal definitions for terms used in the Subsystem Specifications and subsequent Design Documents for the VII infrastructure.

2. LEXICON

TERM	ACRONYM	DEFINITION
1609.2 Certificate		A type of digital certificate used to secure wireless communication within the VII system. [Source: IEEE 1609.2 Standard]
Abnormal Behavior		Behavior that does not conform to specifications defined for the interface or service concerned.
Access Control		Enables authorized use of a resource while preventing unauthorized use or usage in an unauthorized manner.
Accountability		The security goal that requires actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Accounting Management		Accounting management is the network management process responsible for gathering usage statistics for users and using the statistics to bill users and enforce usage quotas.
Active Advisory Message		Advisory Message which has reached its activation time and is unexpired
Advisory Message		A message sent from the VII traffic operator to provide an advice to the VII System User.
Advisory Message Distribution Service	AMDS	Service that delivers a Network User-supplied geographically-focused advisory message to Vehicles and Public Service Vehicles in specific geographic areas.
Advisory Message Request Type		Identifier indicating action associated with Advisory Message Payload
Application		Logical block of functions which may be combined to implement a VII use case. An application may include multiple pieces of application software.
Application Layer Attacks		Attacks on application-layer weaknesses. Generally, these attacks are aimed at design or implementation flaws of the application, with the intent of causing the application to behave in an unintended manner. Examples include cross-site scripting, denial of service and SYN attacks, SQL injection attacks and malicious bots.
Audit Trail/Log		A chronological record of system activities to ensure the reconstruction and examination of the sequence of security events and/or changes in a security event. In conjunction with appropriate tools and procedures, audit trails can provide a means to accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.
Augmented Map		A map that has been modified by analysis of probe data to provide more accurate information.
Authentication		Verifying the identity of a user, process, or device, as a prerequisite to allowing access to resources in an information system.
Authenticity		The property of being genuine and being able to be verified and trusted; confidence in the validity of VII transmission, VII message, or VII message originator. [Source: NIST Special Publication 800-53]

TERM	ACRONYM	DEFINITION
Authorization		The granting or denying of access rights to a user, program, or process.
Authorized User		An individual who has appropriate approvals to access the VII information system and to access specified applications and data hosted on the VII System.
Availability		The readiness of the VII system for immediate and continuous use
Backbone		The sum of all Backbone Transport Interfaces throughout the VII System.
Backbone Gateway		A group of Network Devices and Security Devices handling all Backbone Transport Interfaces that terminate at a specific Network Access Point.
Backbone Transport Interface		A connection consisting of a communications link and its terminating endpoints at two different Backbone Gateways.
Border Gateway Protocol	BGP	Core routing protocol of the Internet which maintains a table of networks or "prefixes" that designate network reachability between autonomous systems. [Source: RFC 4271]
Business Management		Business Management is the layer of the Telecommunications Management Network which addresses the overall business being supported by the network- return on investment, market share, employee satisfaction, community and governmental goals
Capacity Report		A Capacity Report provides information on available port inventories, static bandwidth load, server licenses, etc, and is used to facilitate procurement and long term planning.
Carrier Sense Multiple Access with Collision Detection	CSMA/CD	The CSMA/CD protocol describes how data frames are placed onto the Ethernet transmission medium to manage collisions. [Source: IEEE 802.3 Standard]
Certificate		A set of data that uniquely identifies an entity, contains the entity's public key and possibly other information, and is digitally signed by a trusted party, thereby binding the public key to the entity. [Source: NIST Special Publication 800-21 [2nd Ed]]
Certificate Authority	CA	A trusted entity that issues and revokes public key certificates. [Source: Federal Information Processing Standard (FIPS)-201]
Certificate Management Authority	CMA	A Certification Authority (CA) or a Registration Authority (RA). [Source: NIST Special Publication-800-32]
Certificate Revocation List	CRL	A list of revoked but un-expired certificates issued by a CA. [Source: NIST Special Publication - 800-21 [2nd Ed]]
Certificate Validation		Verifies the binding between certificates and a valid issuing authority by verifying trusted certificate paths and if the certificate status is current and active. [Source: Federal Information Processing Standard (FIPS) 201]
Certification Practice Statement	CPS	A statement of the practices that a Certification Authority employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this Certificate Policy, or requirements specified in a contract for services). [Source: NIST Special Publication 800-32]
Cisco Internetwork Operating System	IOS	Cisco System's proprietary software used on Cisco routers and some Cisco switches.

TERM	ACRONYM	DEFINITION
Classes of Service		The concept of assigning different priorities to different messages and assigning higher priority messages to higher priority queues. This implies no assurance of a specific performance level, though higher classes of service will average better performance than lower classes of service.
Commercial Off-the-Shelf	COTS	Refers to products available for purchase from vendors, as opposed to custom-made products. [Source: Standard Industry Term]
Common Information Model	CIM	Describes the components of a managed computing and networking environment by using an object-oriented modeling approach. CIM is defined in the CIM Infrastructure specification. [Source: CIM Infrastructure Specification ver 2.3]
Common Management Information Service	CMIS	Standard that supports open distributed management. Uses the Common Management Information Protocol (CMIP) to issue requests for management services. [Source: RFC 1189]
Common Object Request Broker Architecture	CORBA	Standard that builds on the idea that software components, like hardware components, should ultimately be made interchangeable and reliable. Used in systems and applications management.
Communications Service	COMM	Service that provides data transport between Vehicles/Public Service Vehicles and Network Users.
Component		A level of functionality below the subsystem level.
Compromise		Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [Source: NIST Special Publication 800-32]
Confidentiality		(1) Assurance that information is not disclosed to unauthorized persons, processes, or devices. (2) Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control		Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against improper modifications prior to, during, and after system implementation. [Source: NIST Special Publication 800-53; Committee on National Security System Information (CNSSI)-4009]
Configuration Management		Configuration management is the network management process responsible for identifying, tracking and modifying the setup of Network Elements
Cooperative Intersection Collision Avoidance Systems	CICAS	Through the Cooperative Intersection Collision Avoidance Systems initiative, the USDOT is working in partnership with the automotive manufacturers and State and local departments of transportation to pursue an optimized combination of autonomous-vehicle, autonomous-infrastructure and cooperative communication systems that potentially address the full set of intersection crash problems. [Source: US DOT website]

TERM	ACRONYM	DEFINITION
Countermeasures		Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. [Source: NIST Special Publication 800-53; Federal Information Processing Standard (FIPS) 200; Committee on National Security System Information (CNSSI)-4009]
Data Integrity		The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit. [Source: NIST Special Publication 800-27A]
Dedicated Short Range Communications	DSRC	A high-speed radio communications standard that operates in the licensed frequency band of 5.8-5.9 Gigahertz (GHz), usually over a range of 300 meters or less. Also called 802.11p.
Delivery		Conveying a package, generally information in the VII context, to the target.
Delivery, Guaranteed		Conveying a package and providing acknowledgement of delivery.
Delivery Instructions		Delivery Instructions are the associated parameters indicating how, when, and where an Advisory Message should be distributed.
Denial of Service (DoS)		An attempt to make a computer resource unavailable to its intended users either by consuming its resources or obstructing the communication between the resource and its users.
Destruction		The physical alteration of information media or of information components such that they can no longer be used for storage or information retrieval.
Differential Correction Service		Service enabling improved radionavigation system accuracy by determining positioning error at a known location and subsequently transmitting the determined error, or corrective factors, to users of the same radionavigation system, operating in the same area.
Disruption		An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction). [Source: NIST Special Publication 800-34]
Domain Name Service	DNS	The system that translates domain names (computer hostnames) to IP addresses.
Driver		Occupant of the vehicle actively controlling the vehicle.
DSRC Communications Link		The wireless DSRC/WAVE communications for vehicle-to-roadside and vehicle-to-vehicle communications that implements IEEE 1609.
DSRC Industry Consortium	DIC	A group of manufacturers developing a radio in accordance with DSRC standard specifications.
DSRC Radio		Software and hardware components which implement the DSRC Communications link, and adhere to IEEE 1609.

TERM	ACRONYM	DEFINITION
Element Management		Element Management is the layer of the Telecommunications Management Network which addresses specific Network Elements. It covers the fault management and configuration management of the features and functions of a specific class of telecommunications network device by means of a software system (Element Management System) specific to the type of network element being managed (for example: CiscoWorks for Cisco equipment).
Encryption		Cryptographic transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
ENOC Server		A Server operating within the ENOC Subsystem, providing network VII Management Services and VII Security Services.
Enterprise Network Operation Center	ENOC	The ENOC is comprised of the Network Operations Center, Security Operations Center, Computer Security Incident Response Center, and the Help Desk.
Entity		A person, organization, hardware device, or software process.
External Access		The sum of all External Access Transport Interfaces throughout the VII System.
External Access Gateway		A group of Network Devices and Security Devices handling all External Access Transport Interfaces that terminate at a specific Network Access Point.
External Access Transport Interface		A connection between the VII System and an Administrative User, Network User or selected External Data Source, consisting of a communications link and its two terminating endpoints, with one endpoint located at a specific External Access Gateway and the other endpoint located at the site of a specific Network User or External Data Source.
Fault Management		Fault management is the network management process responsible for discovering the existence of a problem in the network; identifying the source of the problem and repairing the problem.
Fault-Management, Configuration, Accounting, Performance, and Security	FCAPS	A categorical model of the working objectives of network management. [Source: Whatis.com]
Federal Bridge Certification Authority	FBCA	The Federal Bridge Certification Authority consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability among Agency Principal Certification Authorities. [Source: NIST Special Publication 800-32]
Federal Information Processing Standard	FIPS	A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability. [Source: Federal Information Processing Standard (FIPS) 201]

TERM	ACRONYM	DEFINITION
Firewall		A security solution which segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic filtering rules.
Gateway		A group of interconnected Network Devices and Security Devices handling a specific set of Transport Interfaces within a Network Access Point.
Global Positioning System	GPS	The satellite-based system which allows a stationary or mobile device that is equipped with a GPS receiver to determine its geographical location (longitude and latitude).
Help Desk		The Help Desk is the point of contact for VII System operational inquiries, requests, or reports.
Human Machine Interface	HMI	Audio, visual, tactile interface between vehicle applications and vehicle occupants.
Identification		The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system. [Source: NIST Special Publication 800-47]
Incident		A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. [Source: NIST Special Publication 800-61]
Information Lookup Service	ILS	Provides RSE location, IP, and capability information to applications. Inputs are: Geographic boundary. Outputs are: RSE IP Addresses & GPS Coordinates & RSE capabilities.
Information Technology Infrastructure Library	ITIL	Framework that has gained broad industry acceptance for IT infrastructure management.
Infrastructure Server		A computer system, distinct from Network Device and Security Device, providing VII Services. For example, servers operating within the SDN Subsystem or the ENOC Subsystem.
Initial Registration/Certification		The process whereby an end entity first makes itself known to a CA or RA, prior to the CA issuing a certificate or certificates for that end entity. The end result of this process (when it is successful) is that a CA issues a certificate for an end entity's public key, and returns that certificate to the end entity and/or posts that certificate in a public repository. This process may, and typically will, involve multiple "steps", possibly including an initialization of the end entity's equipment. For example, the end entity's equipment must be securely initialized with the public key of a CA, to be used in validating certificate paths. Furthermore, an end entity typically needs to be initialized with its own key pair(s).
Integrity		Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Interface		The grouping of all the messages that two units send one another in performing a task. [Source: introduction]
Interface Requirements Specification	IRS	A document specifying technical requirements for an interface between subsystems of the VII System.
Internet Control Message Protocol	ICMP	A core protocol of the Internet protocol suite. It is chiefly used by networked computers' operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.

TERM	ACRONYM	DEFINITION
Internet Protocol	IP	Data-oriented protocol used for communicating data across a packet-switched internet.
Intrusion Detection System	IDS	Software that looks for suspicious activity and alerts administrators. [Source: NIST Special Publication 800-61]
IP Spoofing		The creation of IP packets with a forged (spoofed) source IP address.
Java Management Extensions	JME	Java technology that supplies tools for managing and monitoring applications, system objects, devices, and service-oriented networks.
Jurisdiction		The territorial range over which a VII Network User has been given access rights to a specific network asset or information about a specific asset.
Keepalive		A notification sent at regular intervals by/to a Managed Network Element indicating that the Managed Network Element is still functioning. The message ensures that a connection is still alive, and in some cases ensures that the connection does not get closed (e.g., if a firewall between the client and server automatically closes idle connections).
Key Management		The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization. [Source: Federal Information Processing Standard 140-2]
Lightweight Directory Access Protocol	LDAP	A networking protocol for querying and modifying directory services running over TCP/IP.
Local Safety System	LSS	Equipment and associated traffic applications which are physically close to the RSE and which are dedicated to performing vehicle and infrastructure safety and communicating over the DSRC Radio Link.
Local Safety System Interface	LSSI	The interface between the RSE and the Local Safety System.
Log		Denotes a chronological record of a specific set of events occurring within a system or network. Logs are composed of log entries each of which contains information related to a specific event that has occurred within the system or network. [Source: introduction]
Malicious Code		Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. [Source: NIST Special Publication 800-53 Rev 1; Committee on National Security System Information (CNSSI)-4009]
Malware		A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. [Source: NIST Special Publication 800-83]

TERM	ACRONYM	DEFINITION
Man-in-the-Middle Attack		An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims.
Managed Entity		A person, organization, hardware device, or software process which is known by the VII System. Includes Network Users, Administrative Users, RSE Subsystem, ENOC Subsystem, SDN Subsystem, CA Subsystem, Reference Map Providers and Service Provider Management Systems.
Managed Entity Account		Identity and management data (including certificate) which is associated with a Managed Entity.
Managed Network Elements	MNE	A Managed Network Element (MNE) is a Network Element which is addressable and manageable by the Network Management System. An MNE collects and stores management information and makes this information available to the Network Management System. In VII, this includes RSEs, SDNs, and communications infrastructure. [Source: introduction]
Managed Security Elements		Denotes devices such as firewalls, virtual private networks, intrusion detection systems, etc. which are monitored and controlled via access to their management information. [Source: introduction]
Management Controls		The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security. [Source: NIST Special Publication 800-53; FIPS 200]
Management Information Base	MIB	Type of database used to manage the devices in a communications network used by SNMP.
Map		A collection of coordinates associated with specific features that together specify geographic aspects of a bounded area.
Mean Time Between Failure	MTBF	The reliability result of the reciprocal of a failure rate that predicts the average number of hours an item, assembly or piece part will operate within specific design parameters. (MTBF=1/(1)) failure rate, (1) failure rate = # of failures/operating time. [Source: NASA]
Mean Time Between Maintenance	MTBM	The mean (average) time between maintenance actions including both the corrective (MTBCM) and preventive (MTBPM) maintenance activities. The calculation of the MTBM is MTBM = MTBPM + MTBCM. [Source: NASA]
Message		Any instance of communication between two entities. [Source: introduction]
Message Format		Refers to the encoding of a message
Message Structure		Refers to the schema of a message
Message Values		Refers to the values of elements in a message
Micro-Map		A map that provides information only for a small area, for instance an intersection and surrounding areas within 100-300 meters.

TERM	ACRONYM	DEFINITION
Mobile Code		Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. [Source: NIST Special Publication 800-53; Committee on National Security System Information (CNSSI)-4009 Adapted NIST Special Publication 800-53; Committee on National Security System Information (CNSSI)-4009 Adapted]
Mobile User		The mobile, vehicle-based users of the VII Network, connecting via a DSRC radio-link.
Monitor		(In the usage of "monitor traffic") The act of inspecting network activity between System Services to apply filtering rules and detect security events for the purposes of incident prevention, handling, and response.
Multiprotocol Label Switching	MPLS	Data-carrying mechanism which emulates some properties of a circuit-switched network over a packet-switched network.
Network Access Point	NAP	An interconnected group of collocated Network Devices and Security Devices, providing internal and external communications.
Network Device		A device with transports data between networks or network segments. Examples of network devices include switches and routers.
Network Element	NE	A Network Element (NE) is a constituent part ("element") of an information communications system infrastructure ("network"). An NE is interconnected with other Network Elements in order to provide information communication services to a Network User. The term includes both hardware and software - routers, operating systems, communication ports, etc.
Network Management		Network management is the process of maintaining and administering ("management") an information communications system infrastructure ("network"). Network management contains five functional areas - Fault management, Configuration management, Accounting management, Performance management, and Security management. In a more restricted meaning, Network Management is the layer of the Telecommunications Management Network which address the network and systems that deliver services to customers, tackling issues such as capacity, diversity, and congestion.
Network Management Data		Network Management Data is data collected from Managed Network Elements in order to provide network management services.
Network Operations Center	NOC	The Network Operations Center is the location at which the VII Operating Entity personnel manage the VII network subsystem. It is a component of the Enterprise Network Operations Center (ENOC).
Network Reconnaissance		The overall act of learning information about a target network by using publicly available information and applications.

TERM	ACRONYM	DEFINITION
Network Service		In the context of VII, Network Service refers to one of the defined services which are being provided over the VII system, i.e. Information Lookup Service, Advisory Message Delivery Service, Probe Data Service, Map Element Distribution Service, Communication Service, Management Service, Security Service, and Positioning Service. It is synonymous with "System Service".
Network Subsystem		Network Subsystem refers to the communications infrastructure which enables messages to be transported between Roadside Equipment and users of the VII system.
Network Time Protocol	NTP	Protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks.
Network User		Public and private entities that distribute information through and/or receive information from the VII System.
Nonpersistent Message Delivery		Messages are not stored in memory for delivery at a later date. Therefore, incoming messages that are not able to be delivered to their destination are discarded.
Non-repudiation		Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information. [Source: NIST Special Publication 800-53; Committee on National Security System Information (CNSSI)-4009]
On-Board Equipment	OBE	A processing and communications capability resident in a vehicle, that provides an application runtime environment, positioning, security and communications functions, and interfaces to other vehicle systems including human machine interface elements.
Online Certificate Status Protocol	OCSP	An on-line protocol used to determine the status of a public key certificate. [Source: NIST Special Publication 800-63, FIPS 201]
Open Service Gateway Initiative	OSGI	Framework that defines an application life cycle model and a service registry.
Operating Entity		The entity in charge of managing and operating the VII Network. The Operating Entity will include participants from both USDOT and VIIC.
Operational Controls		The security controls (i.e., safeguards or countermeasures) for an information (sub) system that primarily are implemented and executed by people (as opposed to systems). [Source: NIST Special Publication 800-53; FIPS 200]
Original Equipment Manufacturer	OEM	Manufacturers of vehicles and providers of specialized services to owners of these vehicles.
Passenger		Occupant of the vehicle other than the driver.
Password Attacks		Password attacks can be performed using several different methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account or password. These repeated attempts are called brute-force attacks.

TERM	ACRONYM	DEFINITION
Performance Management		Performance Management is the network management process responsible for measuring the performance of Network Elements, taking measures to optimize the network for maximum system performance.
Performance Report		A Performance report provides information on dynamic network data such as, throughput and peak loading, and resource utilization. It is used to facilitate network optimization and tuning, and is helpful in identifying resource deficiencies which feed into capacity planning.
Personally Identifiable Data		Data that is associated with living persons or that can be associated with living persons by deduction from personal identifiers in a data set.
Political Boundary		The borders of a governmental jurisdiction. In the context of VII, the organizational structure of the federal, regional, and local departments of transportation and their corresponding relationships.
Privacy Impact Assessment	PIA	An analysis of how information is handled: To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; To determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks
Private Key		The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data. [Source: NIST Special Publication 800-63]
Probe Data Elements		Individual data types packaged within probe data- for example Speed, or Location
Public Key		The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data. [Source: NIST Special Publication 800-63]
Public Key Certificate		A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. [Source: NIST Special Publication 800-63]
Public Key Infrastructure	PKI	A framework encompassing the laws, policies, standards, hardware, and software to provide and manage the use of public key cryptography on public networks.
Public Safety Agency		This role includes any agency that provides emergency notifications, including state and local police and fire departments and the National Weather Service.
Public Service On-Board Equipment	PSOBE	A processing and communications capability resident in a public service vehicle, that provides an application runtime environment, positioning, security and communications functions, and interfaces to other vehicle systems including human machine interface elements.
Publicly-owned Network Infrastructure		Local, state or federal government-owned network devices and media used for the purpose of transporting data traffic.
Quality of Service	QOS	Refers to the probability of the telecommunication network meeting a given traffic contract.

TERM	ACRONYM	DEFINITION
Real-Time		An operation is considered real-time if the time it takes to perform the operation is less than the maximum allowable delay to avoid undesirable consequences.
Reference Map		A map that serves as the baseline map for a given area.
Rekey a Certificate		To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key. [Source: NIST Special Publication 800-32]
Remediation		The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application. [Source: NIST Special Publication 800-40 Ver 2]
Remote Monitoring	RMON	A standard monitoring specification that enables remote network monitoring devices (often called monitors or probes) to exchange network-monitoring data with a network management system console.
Remote Probe Data Message Subscription		In a distributed broker architecture, the act of sharing subscription request information between PDS Brokers in order to fulfill a request for Probe Data Elements from a locally attached Network User.
Renew a Certificate		The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate. [Source: NIST Special Publication 800-32]
Repudiation		The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.
Request for Comment	RFC	A document which a standard-developing body, such as IEEE, uses to propose new technological standards in detail.
Revoke a Certificate		To prematurely end the operational period of a certificate effective at a specific date and time. [Source: NIST Special Publication 800-32]
Risk		The level of impact on VII operations, assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. [Source: NIST Special Publication 800-53; FIPS 200]
Risk Mitigation		Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. [Source: NIST Special Publication 800-30]
Road-Side Equipment	RSE	The equipment positioned along highways, at traffic intersections and other locations where timely communications with vehicles are needed. Each RSE includes a DSRC radio (also known as the Roadside Unit or RSU), a positioning system, processor, and router to send messages back through the VII Network.
RSE Backhaul		The sum of all RSE Backhaul Transport Interfaces throughout the VII System.
RSE Backhaul Gateway		A group of Network Devices and Security Devices handling all RSE Backhaul Transport Interfaces that terminate at a specific Network Access Point.

TERM	ACRONYM	DEFINITION
RSE Backhaul Transport Interface		A connection between an SDN Subsystem instance and an RSE Subsystem instance, consisting of a communications link and its terminating endpoints, with one endpoint located at a specific RSE Subsystem instance and the other endpoint located at a specific RSE Backhaul Gateway.
Safeguard		A technology, policy, or procedure that counters a threat or protects assets.
SDN Server		A Server operating within the SDN Subsystem, providing VII services
SDN Subsystem Facility		The physical location of the SDN Subsystem.
Secure Shell	SSH	Set of standards and an associated network protocol that allows establishing a secure channel between a local and a remote computer using public-key cryptography.
Secure Sockets Layer	SSL	A commonly used protocol for managing the security of a message transmission on the internet. SSL uses the public- and private-key encryption system, which includes the use of a digital certificate.
Security Control		Management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. (NIST Special Pub 800-53) [Source: NIST Special Pub 800-53]
Security Controls		The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information. [Source: NIST Special Publication 800-53; FIPS 200; FIPS 199]
Security Device		Hardware, with software running on it, providing the functionality of Security Control. Firewalls, intrusion detection systems and intrusion prevention systems are examples of security devices.
Security Event		An occurrence on a system that may be relevant to the indication of malicious activities such as IP spoofing, denial-of-service attacks, man-in-the-middle attacks, application layer attacks, network reconnaissance, trust exploitation, unauthorized access, virus and Trojan horse applications.
Security Incident		A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. [Source: NIST Special Publication 800-61]
Security Management		Security management is the network management process responsible for controlling (granting, limiting, restricting or denying) access to the network and its resources.
Security Operations Center	SOC	The Security Operations Center is the location at which the VII Operating Entity personnel manage the security of the VII System. It is a component of the Enterprise Network Operations Center (ENOC).
Sensitivity		From a security perspective, sensitivity is a measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection. [Source: NIST Special Publication 800-60]

TERM	ACRONYM	DEFINITION
Server Gateway		A group of Network Devices and Security Devices handling all Server Transport Interfaces that terminate at a specific Network Access Point.
Server Transport		The sum of all Server Transport Interfaces throughout the VII System.
Server Transport Interface		A network connection providing bi-directional transport of IP traffic between a Network Access Point and an associated Infrastructure Server.
Service Delivery Node	SDN	Equipment that hosts VII Public applications and services, to include the Event Notification Service (publish/subscribe), Location Based Services, Network Management System (NMS), Security Services, Advisory Message Distribution Service, and dynamic host configuration protocol services.
Service Management		Service Management is the layer of the Telecommunications Management Network which addresses the services being offered to customers over the network
Service-Level Fault		A Service Level Fault is an error condition recognized by the Network Management System when the monitored performance of a Managed Network Element fails to meet defined service-level performance thresholds.
Services		Functionality exposed by the VII System to external users and applications (including at a minimum Probe Data, Communications, and Advisory Message Distribution)
Session Data		A record of transactions between parties, typically storing source and destination IP addresses and ports, session start and end times, and counts of packets and bytes of data sent by source and destination. Session data is typically captured for connection-oriented TCP traffic, but sessions can be emulated for connectionless protocols like UDP and ICMP in a request-response model.
Storage		Denotes a repository of data. Storage can be written, read, deleted, or otherwise modified. Storage, being media independent (i.e., storage can take the form of compact disks, random access memory, files on a hard disk, a database system, etc.) can be volatile, non-volatile, or a combination of both. [Source: introduction]
Stratum [n]		The stratum levels define the distance from the reference clock and the associated accuracy. See also NTP.
Symmetric Key		A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code. [Source: NIST Special Publication 800-63]
System Integrity		The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. [Source: NIST Special Publication 800-27A; Committee on National Security System Information (CNSSI)-4009 Adapted]
System Operator		Denotes the administrative and engineering personnel who monitor the performance of the VII network subsystem and the RSE, run the day-to-day operations of these systems, and execute configuration changes to these systems.

TERM	ACRONYM	DEFINITION
System Service		An implemented set of functionality which is provided to more than one application program.
System Usage Accounting		System Usage Accounting refers to the collection of statistical measurements which track the utilization of system resources by users of the system with a view towards billing the users for their consumption of resources.
System User		Users of the VII System, including Network Users, Vehicles, Public Service Vehicles and Administrative Users.
Tampering		An unauthorized modification that alters the proper functioning of equipment or a system in a manner that degrades the security or functionality it provides.
Telecommunications Management Network	TMN	Framework defined by the International Telecommunications Union–Telecommunications Services Sector (ITU-T) that proposes a model based on object-oriented principles and standard interfaces for communications between management entities in a network.
Temporary Address		A means of identifying a specific device or user that enables communications to that device or user, and is assigned to that device or use for a limited period of time.
Threat		Any circumstance, event, or act that could cause harm to the VII System by destroying, disclosing, modifying, or denying service to automated information resources.
Tolling Authority		This role is responsible for the management of toll road financial record-keeping and transactions.
Traffic Conditioning		Control functions performed by network devices to enforce traffic rules related to metering, marking, shaping and policing (See RFC 2475).
Transaction Service Provider	TSP	Public or private specialized traveler information service providers that provide value-added information to travelers.
Transmission Control Protocol	TCP	Transports data packets from one node to another over an IP network, with acknowledgements for received data. Re-sequences data after transmission.
Transportation Operations Center	TOC	State and local facilities that provide management of all local, state and interstate roadways, through the control of traffic signals, ramp meters, data collection equipment and data dissemination equipment, and the maintenance of roadway status, including work zones, special events, scheduled and unscheduled road closures and environmental conditions within a geographic extent.
Trust Exploitation		Although not an attack in and of itself, trust exploitation refers to an attack where an individual takes advantage of a trust relationship within a network.
Unauthorized Access		A state in which someone has gained access to information or privileges they should not have access to. Although unauthorized-access attacks are not a specific type of attack, they refer to most attacks executed in networks today. For example, in order for someone to brute-force attack a Telnet login, he/she must first get the Telnet prompt on a system.
Unauthorized Disclosure		An event involving the exposure of information to entities not authorized access to the information. [Source: NIST Special Publication 800-57; CNSI-4009 Adapted]

TERM	ACRONYM	DEFINITION
Unauthorized User		Is an individual who has not been granted the appropriate approval to access and the VII System and/or specific applications and data hosted on the VII System.
Uninterruptible Power Supply	UPS	A device which maintains a continuous supply of electric power to connected equipment by supplying power from a battery when utility power is not available.
Use Case		A description of a set of sequences of actions, including variants, that when performed by a system, yield an observable result to a system user.
User Datagram Protocol	UDP	Transports data from one node to another over an IP network, utilizing port numbers to distinguish one data flow from another and a checksum algorithm to verify that data did not become corrupted in transit.
Vehicle		A wheeled vehicle that carries its own motor. Different types of vehicles include cars, buses, trucks, vans and rail vehicles. Vehicle represents the common vehicle with specialized vehicles (e.g., Maintenance Vehicle) inheriting from Vehicle.
Vehicle Anonymity		A condition in which the vehicle cannot be uniquely identified (and its owner traced) using the data processed by the VII system.
VII	VII	Vehicle Infrastructure Integration
VII Network End User		The entire user community of VII System data including both public and private sector users.
Virtual Private Network	VPN	The extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks.
Virus		A self-replicating program that runs and spreads by modifying other programs or files [Source: NIST Special Publication 800-61]
Virus and Trojan Horse Applications		Viruses refer to malicious software that is attached to another program to execute a particular unwanted function on a system.
Vulnerability		A flaw or weakness in a system's security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
Web Service		A Web Service is a software component that is described via WSDL and is capable of being accessed via standard network protocols such as but not limited to SOAP over HTTP.
Web-Based Enterprise Management	WBEM	Systems management architecture initiative to unify the management of enterprise computing environments. WBEM allows the industry to deliver a set of standard-based management tools related to XML.
Wide Area Network	WAN	Computer network covering a wide geographic area.
X.509 Certificate		A type of digital certificate used for network communication within the VII system.
Zeroization		A method of erasing electronically stored data by altering or deleting the contents of the data storage to prevent recovery of the data. [Source: FIPS 140-2]