Vigilant Solutions Security and Compliance Overview

Vigilant Solutions offers to its law enforcement clients a hosted license plate recognition (LPR) database and analytic solution known as LEARN. LEARN is hosted within Vigilant Solutions' data center managed by NTT Communications (http://www.us.ntt.com/en/resources/analyst-reports.html), a worldwide leader in providing hosted services and security. NTT is certified ISO 9001:2008, the internationally recognized standard for Quality Management Systems, and has been independently audited and verified for compliance under the Statement of Auditing Standards Number 70 [SAS70] Type II. The physical and network security employed at the Vigilant data center are exhaustive, and a full briefing document is available at http://vigilantsolutions.com/wp-content/uploads/2016/03/VS_LEARN-NVLS_Security_Document-Aug2015.pdf.

While license plate reader data contains no personal information inherently, it is linkable (through other sources such as DMV records and under permissible purposes defined by the Driver's Privacy Protection Act) to personally identifiable information (PII). Of greater relevance, law enforcement hotlist information such as NCIC is managed by Vigilant law enforcement customers within the data center, and may potentially contain Criminal Justice Information (CJI) as defined in 4.1 of the Policy. For these reasons, Vigilant has voluntarily implemented all changes necessary to fully comply with the relevant sections of FBI-CJIS Security Policy, Version 5.2.

Relevant Sections of FBI-CJIS Security Policy

Within the scope of this document, and as it pertains to FBI-CJIS Security Policy, Vigilant Solutions is a Non-Criminal Justice Agency (NCJA) as defined in 3.2.5 of the FBI-CJIS Security Policy document. Going beyond the minimum requirements for a NCJA as listed in Appendix J of the FBI-CJIS Security Policy, the following table highlights those sections of the FBI-CJIS Security Policy that are believed to apply to Vigilant's hosted solution:

Section & Title	Description	Notes
5.1 Information Exchange	Information Exchange Agreements outline the roles responsibilities and data ownership between agencies and any external parties	Vigilant's Enterprise Service Agreement and Terms and Conditions documents outline ownership of data collected by and hosted in an agency LEARN account.
5.1.1.5 Private Contractor User Agreements and FBI-CJIS Security Addendum	Private contractors who perform criminal justice functions for a CJA shall be be permitted to access CJI pursuant to an agreement between the CJA and the contractor that incorporates the FBI-CJIS Security	An executed FBI-CJIS Security Addendum and Hotlist Request Form is required from all agencies requesting Vigilant to use the agency's access to a

	Addendum approved by the Director of the FBI	hotlist containing CJI data to import that hotlist into their LEARN account.
5.1.1.6 Agency User Agreements	Fingerprint-based background checks and written agreement with the agency required.	The Vigilant development and support team, which has access to hotlist files for purposes of support and database maintenance only, has been subject to fingerprint-based background checks as part of an agency-requested fingerprint-based background check. These records are available upon request, and/or these employees will comply with any new requests made by agencies.
5.1.3 Secondary Dissemination	If data is released to another authorized agency and not part of primary information exchange agreement, this shall be logged.	All data sharing is logged and available for audit reporting.
5.2 Security Awareness Training	All personnel with access to CJI shall receive security awareness training within 6 months of assignment, and biennially thereafter.	Initial security awareness training conducted by Pete Fagan in September 2015 in Livermore CA.
5.2.2 Security Training Records	Records of security awareness training shall be kept current and maintained by a FBI-CJIS Security Officer (CSO).	Mark Rivera, retired Maryland State Patrol, is Vigilant's CSO and manages this process.
5.3.1.1 Reporting Structure and Responsibilities	Establishment of a primary POC for FBI-CJIS for incident handling and response.	Mark Rivera, retired Maryland State Patrol, is Vigilant's CSO and manages this process.
5.4.1.1 Events	Description of the events that must be logged within the system.	Windows tracking of unsuccessful login attempts; locks account after 5 unsuccessful attempts.

5.4.3 Audit Monitoring, Analysis and Reporting	Someone shall be responsible / appointed for review and analysis of audit records, at a minimum of once a week, to look for inappropriate or unusual activity.	Vigilant enables this for agencies through its auditing tools and report scheduler.
5.4.6 Audit Record Retention	Agency shall retain audit records for at least one year.	Audit records are held indefinitely.
5.5.2.1 Least Privilege	Agency shall approve individual access privileges and enforce the most restrictive set of rights/privileges needed by users for the performance of specified tasks. Logs maintains on access privilege changes maintained for minimum of one year or at least equal to the agency's record retention policy, whichever is greater.	LEARN provides the ability to specify an almost infinite number of user permissions and access controls through the creation of user profiles. Changes to rights / privileges are currently logged and available in audit records.
5.5.2.4 Access Control Mechanisms	One of the following must be employed: access control lists (users, groups, machines), resource restrictions (permission sets), encryption and strong key management, application level access control	LEARN uses Secure HTTP (https), allows for agency management of users, user profiles with permission sets, password policy management (character logic and change policy), and two-factor authentication.
5.5.3 Unsuccessful Login Attempts	5 Consecutive invalid attempts shall lock an account for a minimum of 10 minutes	5 unsuccessful attempts results in a two hour lock.
5.5.4 System Use Notification	The system shall allow a notification message to be displayed to users letting them know a) they are accessing a restricted system, b) usage is monitored, recorded and subject to audit, c) unauthorized use if prohibited and may result in penalties, and d) use of the system indicated consent to monitoring.	Vigilant allows agencies to monitor / record / audit, and have a notification tool in which users may also receive a pop-up notice upon login that is agency configurable.
5.5.5 Session Lock	The system shall prevent access via a session lock after a maximum 30 minutes of inactivity.	The system locks after 15 minutes, requiring re-entry of credentials.

5.5.7.3 Cellular	This section defines how agencies mitigate concerns surrounding BYOD	This appears to be an agency policy issue that doesn't drive any specific product requirements. Vigilant's mobile app uses the same user profile as configured within LEARN which controls all access and auditing.
5.5.6 Remote Access	Rules for monitoring and controlling remote access via the internet.	Audit of all logins includes IP tracking by user.
5.6.1.1 Use of Originating Agency Identifiers in Transactions and Information Exchanges	An FBI-issued ORI number shall be assigned at the agency level and attached to all activities by the agency's users.	ORI is captured at the agency level.
5.6.2.1.1 Password	This section details the requirements of passwords	Vigilant passwords follow the complexity and change requirements set forth.
5.6.2.1.2 Personal Identification Numbers	Best Practices on PIN use	LEARN uses two-factor authentication from SecureAuth to comply with this requirement.
5.6.2.2 Advanced Authentication	Defines Advanced Authentication requirements	LEARN uses two-factor authentication from SecureAuth to comply with this requirement.
5.6.3.1 Identifier Management	Requirements of agencies to manage user identifiers	User credentials that are inactive for a period of 6 months are disabled within the system, requiring an Agency Manager to re-activate the account.
5.7.1.2 Network Diagram	Requirements for a network topological diagram.	Available on request.
5.8 Media Protection	Requirements for security and protection of electronic and physical media.	Managed by NTT and documented in Vigilant's Data Center Security document referenced at the

		beginning of this document.
5.9 Physical Protection	Requirements for physical security and access controls around all hardware, software and media.	Managed by NTT and documented in Vigilant's Data Center Security document referenced at the beginning of this document.
5.10.1 Information Flow Enforcement	Prevent CJI from being transmitted unencrypted across the public network.	Secure HTTP (https) employed.
5.10.1.1 Boundary Protection	Ensure that failure of boundary protection mechanisms do not result in unauthorized release of information.	Industry standard Cisco inspection of all packets.
5.10.1.2 (1) Encryption	Minimum 128 bit	AES256 encryption.
5.10.1.3 Intrusion Detection Tools and Techniques	Specifies requirements for intrusion detection tools.	Automated monitoring via Cisco per security document.
5.10.3.1 Partitioning	Outlines requirements for partitioning of data.	Vigilant partitions web server, database server, user information, and more. Vigilant uses all four types of partitioning listed.
5.10.4.1 Patch Management	Requirements for management of software patches.	Centralized management on Vigilant's data center, with ample testing before install.
5.10.4.2 Malicious Code Protection	Virus Protection requirements	Microsoft System Defender employed.
5.10.4.3 Spam and Spyware Protection	Spam and Spyware Protection requirements	Cisco and Microsoft Security Essentials
5.10.4.5 Security Alerts and Advisories	Guidance for alerts and advisories.	Mechanisms in place to deliver alerts via agency notifications and agency manager emails.
5.12 Personnel Security	Fingerprint-based background checks and rules based on findings	Support team is screened and fingerprinted.

5.12.2 Personnel Termination	Terminated employees shall immediately have access terminated.	Comply.
5.12.4 Personnel Sanctions	Process for employees failing to comply with security policies.	Comply.

Narrative on FBI-CJIS Security Policy

Vigilant Solutions' LEARN web-based solution is exclusively available to law enforcement. All Vigilant agencies are ORI vetted police agencies that then manage the users they authorize. The data an agency collects can be shared to specific law enforcement agencies via MOU, can be shared to Vigilant's national law enforcement database, or can be exclusively retained for that client agency's use only.

As a company Vigilant Solutions specifies in several places, including on its website and in its Enterprise Service Agreement which is agreed to and signed prior to purchasing Vigilant Solutions' products and/or services, that the License Plate Reader (LPR) data collected by law enforcement deployed LPR systems remains the property of the collecting agency and Vigilant Solutions has no rights to it. Vigilant does not share, sell, or make use of law enforcement generated LPR data in any way. Furthermore, any data retention policy or the sharing of an agencies data would be fully in the control of the agency. Many different states, counties, and municipalities have legislation or guidance on this and LEARN allows for an Agency Manager within the department to make the necessary changes.

Vigilant Solutions uses technical controls and mechanisms within its suite of products that facilitate privacy controls on the data and restrict access to only those that are granted access by the agency.

Those technical controls include configurable access rights, agency controlled information sharing, logging user activity and access, periods of inactivity session locks, system access strong password criteria, encrypted data transport and, data storage in a facility that has criteria consistent with a FBI-CJIS Security Policy Physically Secure Location. Even though Vigilant Solutions has built-in tools to facilitate the Audit and Accountability controls criteria consistent with FBI-CJIS Security Policy, it is the client agency responsibility to perform the audit processes with the Vigilant Solutions product tools provided.

Additionally, in an effort to ensure the integrity of Vigilant's business relationships with clients and their data, as well as its purposes, Vigilant Solutions performs name-based background screening on all of its employees. When required by a client, all Vigilant Solutions staff directly supporting its agencies are subject to FBI-CJIS Security Policy Personnel Screening procedures. Vigilant Solutions cannot, by restrictions of federal law, independently perform fingerprint-based background check screening. Accordingly, it is within the jurisdiction and responsibility of the client agency to perform that screening if they believe it is required based upon the Criminal Justice Information provided by FBI-CJIS or access to FBI-CJIS Systems. Vigilant Solutions staff has, however, successfully completed FBI fingerprint-based background check screening by a FBI-CJIS System Agency in Texas. Only those employees that have passed the personnel screening process are allowed to provide technical system support or access the system in support of client agencies requests.

These employees have executed an FBI-CJIS Security Addendum. Copies are retained by Vigilant Solutions FBI-CJIS ISO along with records of Security Awareness Training that included topics on privacy, confidentiality and data security.

With the intention of meeting or exceeding the relevant aspects of the FBI-CJIS Security Policy, Vigilant Solutions has several administrative and technical controls to adhere to those criteria in response and to report a data breach within its control. Vigilant Solutions employs and manages malware and virus protection, patch management policies, intrusion detection and intrusion prevention systems to protect the customer owned data in LEARN. Vigilant Solutions has an incident response plan consistent with the FBI-CJIS Security Policy. A component of that plan is to communicate to impacted parties, in the event of any physical or technical breach, data loss, or misuse of data or systems through an incident reporting process. Vigilant Solutions uses these tools and processes to monitor for malicious activity and address any data breaches that may occur or traverse its communications entry and exit points or data storage facilities.

Below are high-level descriptions of Vigilant Solutions enterprise efforts to address FBI-CJIS Security Policy areas.

Physical Security

The physical protection mechanisms at the NTT facility are consistent with the FBI-CJIS Physically Secure Location criteria were evaluated in June 2015 by Vigilant Solutions staff as well as an independent third-party security consultant with specific background and experience in FBI-CJIS Security Policy. Additionally NTT is SOC2 audited. Unless a Management Control Agreement is executed between the Contracting Government Agency and the Contractor(s), per FBI-CJIS Security Policy requirement for storage and maintenance of FBI Criminal Justice Information, a Cloud Service provider data center cannot be considered a Physically Secure Location. Vigilant Solutions Engineering and Support staff have executed the FBI-CJIS Security Addendum, have had fingerprint-based background checks and participated in FBI-CJIS Security Awareness Training during September 2015.

Vigilant Solutions is responsible for the security, confidentiality and privacy of the data through Technical Controls, consistent with the FBI-CJIS Security Policy, for the systems and data Vigilant Solutions hosts for client agencies. NTT provides physical security for the facility, communications infrastructure, power conditioning, HVAC, and is responsible for the confidentiality and privacy based upon those physical security controls. Vigilant Solutions provides the physical equipment (servers). NTT has no authorized access to the systems and data. Physical access to the equipment is controlled by Vigilant Solutions. NTT staff is only permitted to access the equipment via a work order authorized by Vigilant Solutions. Unless there are exigent circumstances, only Vigilant Solutions staff physically accesses the equipment at the NTT Data Center and only when a pre-arranged visit is established. Vigilant Solutions does not have card access to the NTT facility, nor the equipment rooms that store the Vigilant Solutions equipment. As part of the physical security controls at the NTT Data Center, Vigilant Solutions staff is provided unmarked keys to the equipment storage cabinets at time of service and escorted access after they arrive at the NTT Data Center to perform the scheduled visit to perform any required maintenance.

Auditing and Accountability

Vigilant Solutions' LEARN has audit functions built in for an agency to view and audit user and transactional activity.

Auditing of the NTT facilities, processes, policies and procedures are accomplished by a third party auditing firm paid for by NTT Data. The current auditing vendor, Ernst and Young produced the SAS 70 report until recently. The SAS 70 Report was the prior name for an evaluation and report for an audit process using standards of the American Institute of Certified Public Accountants (AICPA). Currently, the evaluation and report is named Service Organization Control (SOC Type 2 & 3). The SOC 2 & 3 evaluations have been conducted over the previous two years annually to validate that processes, controls, and procedures are in place and performing as expected. Those SOC 2 standards are validated more frequently and are equal to or greater than FBI-CJIS Security Policy control expectations. NTT Data supplies the SOC 2 Reports to Vigilant Solutions upon completion. Vigilant Solutions analyzes the information for compliance. Additionally, Vigilant Solutions has committed to visiting the NTT Data Center annually to validate that the Physical Security controls are sustained.

The most recent period of audit for NTT was October 1, 2014 through September 30, 2015. The previous year's report (October 1, 2013 through September 30, 2014) was analyzed along with physical observations of the facility. A review of the SOC 2 & 3 consisted of reviewing NTT operational documents and the SOC 2 & 3 reports that describe operations, planning and training to protect Vigilant Solutions assets. The SOC 2 and 3 Reports indicated no deviations from the described controls to protect the facilities and assets at the NTT facility. Additionally, the policies, controls and procedures are equal to or greater than those for FBI-CJIS Security Policy with one exception. Not all NTT Data staff has had fingerprint based background checks as it is based upon customer need. However as a general rule, NTT do not have authorized physical or logical access to the Vigilant Solutions equipment.

The NTT data center was visited in June of 2015 to observe NTT physical security controls and were found to be consistent or greater than the FBI-CJIS Security Policy criteria in a Physical Secure Location, including the protection of Vigilant Solutions assets.

The following FBI-CJIS Security Policy areas were observed to be functioning consistent with and exceeding FBI-CJIS Security Policy requirements:

5.9.1.1 Security Perimeter

5.9.1.2 Physical Access Authorizations

5.9.1.3 Physical Access Control

5.9.1.4 Access Control for Transmission Medium

5.9.1.5 Access Control for Display Medium - Does not apply. There is no logical access to the data, user interface or equipment in areas of NTT facilities that contain the Vigilant Solutions equipment. The configuration for the data storage is a Co-Location service arrangement with NTT Data. There is no user interface to Vigilant Solutions software applications. The equipment is secure and, cabinets storing Vigilant Solutions equipment are anonymously marked. Keys to the cabinets are only provided to equipment owners and NTT staff when contracted for service. Vigilant Solutions rarely engages this service.

5.9.1.6 Monitoring Physical Access

5.9.1.7 Visitor Control

5.9.1.8 Delivery and Removal

Evaluation of Compliance

Per FBI-CJIS Security Policy, facility compliance evaluation would be the responsibility of the Contracting Government Agency to assess. Vigilant firmly believes that the NTT Data Center meets the criteria, satisfying compliance with FBI-CJIS Security Policy criteria, and this belief is upheld by several independent reviews. Vigilant Solutions develops and designs its enterprise system to be adherent with the FBI-CJIS Security Policy. Vigilant Solutions has independently assessed the NTT Data center to inspect the facility and operations for physical security. It has also evaluated the Service Organization Report 2 audit report performed by an outside organization.

In further regard to certification; because different state, local and federal criteria may be required for different contract relationships, e.g., storing investigative, CHRI data vs. LPR data), those numerous variations of circumstances would not enable any cloud service provider to indicate that they are FBI-CJIS Security Policy Compliant nationally. Amazon Web Services literature states that indication.

> *https://aws.amazon.com/compliance/FBI-CJIS/ FBI-CJIS Compliance Summary and FAQ Page - "How is FBI-CJIS Compliance Determined?"*
>
> *Unlike many of the compliance frameworks AWS supports, there is no central FBI-CJIS authorization body, no accredited pool of independent assessors, nor a standardized assessment approach to determining whether a particular solution is considered "FBI-CJIS compliant". Simply put, a standardized "FBI-CJIS compliant" solution which works across all law enforcement agencies does not exist.*
>
> *Instead, each law enforcement organization granting FBI-CJIS authorizations interprets solutions according to their own risk acceptance standard of what can be construed as compliant within the FBI-CJIS requirements. Authorizations from one state do not find reciprocity within another state (or even necessarily within the same state); providers must submit solutions for review with each agency authorizing official(s), possibly to include duplicate fingerprint, and background checks and other state/jurisdiction-specific requirements.*
>
> *Each authorization is an agreement with that particular organization; something that must be repeated locally at each law enforcement agency. AWS will not claim to be something we are not, and that is why we won't make broad statements of being "FBI-CJIS compliant". Although a particular state or agency may have determined that AWS is FBI-CJIS compliant for their purposes, there is no one FBI-CJIS certification that applies across all law enforcement departments.*

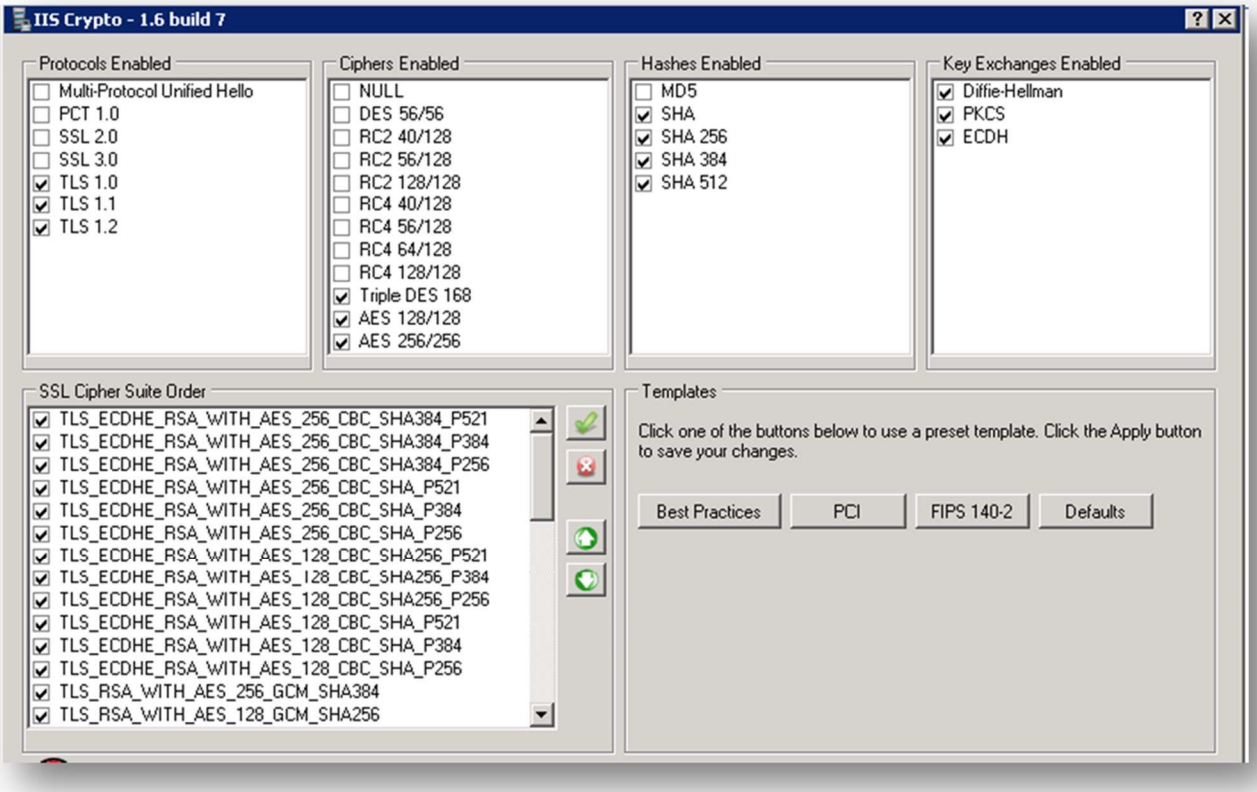
Much like Microsoft Cloud and Amazon Cloud, services provided by Vigilant Solutions and its' data partner NTT Data can only meet compliance through a government entity. There is no blanket compliance or certifications issued to a

vendor or cloud service provider by the FBI-CJIS Division. Being FBI-CJIS Security Policy compliant is accomplished through an individual evaluation and assessment by the government agency that contracts for that service. As cited, Cal DOJ went through the process of determining FBI-CJIS Security Policy compliance for FBI-CJIS Security Policy with Microsoft for that entity alone (Cal DOJ).

The cloud providers cited, including Vigilant Solutions, can only have the administrative, technical and policy controls in place to be evaluated by the government entity, often with the assistance of the FBI-CJIS Information Security Officer staff, to enable meeting the FBI-CJIS Security Policy compliance criteria when a government entity has a desire to enter into the contracted government relationship for that particular government service. In this case, it would be for the storage and access of the LPR Data and Hotlists if the information is considered FBI-CJIS Security Policy defined Criminal Justice Information.

FBI-CJIS Security Policy dictates that a location/facility or entity that houses or processes defined FBI Criminal Justice Information and used or arranged in a contracted relationship with a government entity for handling of Criminal Justice information can only be a considered a Physically Secure Location if it is under Management Control of the Contracting Government Agency and formalized with a Management Control Agreement. The Management Control Agreements or other agreements need to be evaluated for execution based upon the information or service being employed.

In this instance, FBI-CJIS Security Policy only applies to that information defined as FBI Criminal Justice Information and being sourced and or accessed to or from the FBI Criminal Justice Information Services Division. To be consistent with FBI-CJIS Security Policy, an agency needs to fully evaluate the information provided for a solution to determine compliance. For more information on this, please see our whitepaper on cloud solutions and compliance with FBI-CJIS Security Policy at http://vigilantsolutions.com/wp-content/uploads/2016/03/lpr-data-cjis-compliant-whitepaper.pdf.



Encryption

Within the system, there are several modes of encryption. From the initial detection prior to the data being sent via https, the data is not encrypted. While the data is in transit https protocols are used. Vigilant Solutions uses encryption for transmitted data to and from servers deploying Secure Socket Layer/Transport Layer Security protocols. That protocol encrypts all data when it leaves the Car Detector Mobile software application or LEARN software application and encrypts any responses sent to the end user, using the Internet to communicate to and from a Vigilant Solutions owned and managed Microsoft Server 2012. The Microsoft Server employs FIPS approved algorithms during data transit. The server(s) are used to manage traffic as well as store and process data transactions on the servers located at NTT Data Center.

Vigilant Solutions uses Microsoft Windows Server 2012 and the application module called Internet Information Services to enable the use of available encryption algorithms. As indicated these are FIPS approved algorithms.

The data at rest inside the LEARN server is not encrypted. When a detection is matched to a hot listed vehicle in the LEARN server (hot list could be supplied by client agency via SFTP) the data leaves the LEARN server, is encrypted via the Cisco router and traverses again via https back to the patrol vehicle that made the detection which would then see the alert. As per FBI-CJIS Security Policy, the patrol vehicle is considered a physically secure location and would not require encryption to that end. It would be possible through the Vigilant Solutions engineering team to discuss options for obfuscation of the data and to what end if required.

Currently, the LEARN server is using SQL Server database and is using the following settings in its IIS Crypto: Protocols enabled; TLS 1.0, TLS 1.1, TLS 1.2 – Ciphers Enabled; Triple DES 168, AES 128/128, AES 256/256 – Hashes Enabled; SHA, SHA 256, SHA384, SHA512 – Key Exchanges Enabled; Diffie-Hellman, PKCS, ECDH. SSL Cipher Suite Order is in part as follows: TLS_ECDHE_RSA_WITH AES_256_CBC_SHA384_P521, TLS_ECDHE_RSA_WITH AES_256_CBC_SHA384_P384, TLS_ECDHE_RSA_WITH AES_256_CBC_SHA384_P256, TLS_ECDHE_RSA_WITH AES_256_CBC_SHA_P521, TLS_ECDHE_RSA_WITH AES_256_CBC_SHA_P384, TLS_ECDHE_RSA_WITH AES_256_CBC_SHA_P256, TLS_ECDHE_RSA_WITH AES_128_CBC_SHA256_P521, TLS_ECDHE_RSA_WITH AES_128_CBC_SHA256_P384, TLS_ECDHE_RSA_WITH AES_128_CBC_SHA256_P256 and so on. Additional information as to the additional suite order can be directed to Vigilant Solutions' CSO.

The level of security that are associated with hotlists differs slightly, as this is data that may potentially contain CJI. All hotlist data is encrypted both in transit and also at rest to protect this potentially sensitive data. The license plate field is left unencrypted to allow for rapid matching of inbound detection data against the hotlist. All other fields are encrypted.

With regard to the standards set by FIPS/NIST as to data security standards and access, there are two items to consider here: data in transit and data at rest. For data in transit, Vigilant uses SSL with FIPS approved algorithms. For data at rest (data inside LEARN databases at the NTT datacenter), this data is not encrypted when stored INSIDE the data center. The data center is a SOC2 facility such that what you are mitigating against would be attacks/disclosure from people physically inside a secure facility. Furthermore, employees (Vigilant and NTT) that would be granted specific work access to a Vigilant Solutions secure server have been fingerprint and background checked. Any instance of physical access to Vigilant Solutions servers is first authorized by Vigilant Solutions Vice President of Engineering and is documented at the NTT site.