REVISED JULY 2, 2020

VIGILANT LEARN SECURITY AND COMPLIANCE MEMORANDUM

OVERVIEW

Motorola Solutions offers the Vigilant LEARN platform to law enforcement clients as a hosted data capture and image analytics platform for license plate (Vigilant PlateSearch™) and face (Vigilant FaceSearch™) images to aid law enforcement in their day to day public safety mission. Unless on premise deployment is required by the customer, all IT assets and software applications are hosted in Co-Location Infrastructure as a Service and Software as a Service configurations with Motorola Solutions' owned IT assets. Our infrastructure is hosted in a Global NTT (NTT) data center in Ashburn, Virginia. Our secure data center vault in that facility is managed by NTT. The sister companies are worldwide IT leaders, providing Tier 1 hosted services and data security. The data center is certified ISO 9001:2008, the internationally recognized standard for Quality Management Systems. NTT is independently audited annually by a third-party firm for compliance under the Association of International Certified Professional Accountants (AICPA) Statement of Auditing Standards producing a Service Organization Controls (SOC) 2 Report. The SOC 2 is available under a Non-Disclosure Agreement. The physical and network security employed at the data center is exhaustive. Information about the physical security at the NTT data center can be found here: NTT Data Center. The data center has achieved FedRAMP Moderate control certification issued by DHS.

Motorola Solutions takes IT security seriously. We recognize that while license plate reader data inherently contains no Criminal Justice Information (CJI) or Personally Identifying Information (PII), it is linkable through other external sources such as DMV, NCIC or CHRI records. Of greater relevance, the law enforcement hot list information, such as NCIC, are managed by our law enforcement customers but in our custody. Additionally, end users can enter information that may potentially contain CJI or PII as defined in 4.1 of the CJIS Security Policy. This can occur when information from other sources is added in free text fields by the customer. For these reasons, Motorola Solutions has

voluntarily implemented the security controls necessary to adhere to the relevant sections of the policy. The current version of FBI-CJIS Security Policy can be found here: FBI-CJIS Security Policy. In regard to Vigilant FaceSearch™, images are either publicly available mugshot images or provided by customer agencies. All LPR and face images provided by the law enforcement customer are shared with other customers only as designated by customer enabled sharing controls. All activity is logged and can be audited.

Data Ownership – The Enterprise Service Agreement and Terms and Conditions documents outline ownership of data collected by and hosted in agency accounts. Customers own and control the data collected, entered, submitted and stored through Motorola Solutions applications. All customer owned data is classified by Motorola Solutions as Criminal Justice Data. Our Information Security Policy provides protection and handling instructions for employees. The policy encompasses rules for handling, storage, dissemination and disposal of customer owned data.

Data retention is the responsibility of the customer in accordance with any of their governing federal, state, local law, rule or policy. Data is deleted when the customer engages that action. Data is not mined, sold or shared beyond the sharing configurations established by the data owner. The data owner is responsible for submitting accurate, authorized, lawful and appropriate information through Motorola Solutions applications and ensuring they do so in accordance with any governing federal, state, local law, rule or policy.

Data Storage and Access – Law enforcement gathered Vigilant LEARN data is physically (geographically) and also logically separated from our sister subsidiary commercial LPR data partner DRN. Customers can acquire access to the commercial data, but it is a one-way share. We own the commercial data and what the customers can access. Law enforcement data is not shared with commercial customers and that option is not permissible for customers within the sharing configurations. Corporately, we do not share Vigilant LEARN customer data with anyone as we do not own the data. Our commercial customers do not have access to perform any query or analysis of Vigilant LEARN customer data.

PHYSICAL SECURITY

Physical protection mechanisms at the NTT facility in Ashburn, VA are consistent with, or greater than the FBI-CJIS Physically Secure Location criteria. They were last evaluated in December 2019 by Motorola Solutions staff with specific background and experience in FBI-CJIS Security Policy. The data center facility and staff are audited to AICPA standards using an independent third party auditor to validate the security controls. However, unless a Management Control Agreement is executed between the Contracting Government Agency and the Contractor(s), per the 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 and Motorola Solutions protocol is to encrypt data that may be considered sensitive, even if not CJI.

Motorola Solutions is responsible for the security, confidentiality and privacy of the data in its custody, and is accomplished through technical security controls consistent with the FBI-CJIS Security Policy. The NTT Data Center, as a colocation facility, provides physical security for the facility. NTT ensures that there is adequate physical security, reliable Internet, suitable staff, communications protection, power conditioning and HVAC. They are responsible for the confidentiality and privacy based upon those physical security controls at the data center. Motorola Solutions owns and maintains the physical equipment (servers). Data center staff have no authorized physical or logical access (GUI) to Vigilant LEARN, the infrastructure systems or data. Physical access to the equipment is controlled by Motorola Solutions. Data center staff are only permitted to access the equipment via a work order authorized by Motorola Solutions in exigent circumstances. When doing so, data center staff still have no access to the data or software applications. Unless there are exigent circumstances to power on or power off the equipment, only Motorola Solutions staff physically accesses the equipment at the data center and, only when a pre-arranged visit is established. As part of the physical security controls cabinets storing all servers, routers

and other equipment are unmarked and indistinguishable from other colocated data center clients. Authorized Motorola Solutions staff are provided a combination lock code to the equipment storage cabinets to perform any required maintenance. All access to the facility and cabinets is logged.

PERSONNEL SCREENING

When requested, Motorola Solutions Engineering and Support staff execute the FBI-CJIS Security Addendum, have state and national fingerprint-based background checks and complete bi-annual FBI-CJIS Security Awareness Training (Tier 4) through Peak Performance CJIS Online. If any barrier offense activity is discovered before or during assignment, Motorola Solutions suspends staff system access pending resolution and will notify those clients that require CJIS personnel screening procedures.

As stated previously regarding NTT, the policies, controls and procedures are equal to or greater than those for FBI-CJIS Security Policy, with one exception related to data center staff personnel screening. Not all data center personnel have undergone national fingerprint-based background checks as it is based upon customer need. Data center staff do not have logical access to unencrypted information and Motorola Solutions encrypts sensitive data at rest. All data center staff and security personnel have undergone name-based background checks and are evaluated for suitability by their management. Data center staff do not have authorized physical access to Motorola Solutions equipment and do not have access to unencrypted information. Additionally, data center staff have no administrator or user logical access privileges to any Motorola Solutions software applications, servers, firewalls or routers.

Data center staff do not manage Motorola assets or customer data. Customer data or IT assets are not co-mingled with any data center assets.

AUDITING AND ACCOUNTABILITY

Motorola Solutions' Vigilant LEARN applications have audit functions built in, enabling customers to view and audit user and transactional activity. Audit functionality is consistent with FBI-CJIS Security Policy and enables integrity audits to "increase the probability of authorized users conforming to a prescribed pattern of behavior." Audit functionality focuses on "events" and "content" as specified in Section 5.4.1. Motorola Solutions also audits its' staff to ensure adherence to our standards of acceptable use. Auditing user activity is a customer responsibility.

Auditing of the NTT facilities, processes, policies and procedures are accomplished by a third party auditing firm and onsite visits by our staff. The current auditor, Ernst and Young, evaluates the data center and staff using standards of the AICPA. The results of the evaluation are documented in SOC Type 2 & 3 reports. These evaluations are conducted annually to validate that processes, controls, and procedures are in place and performing as expected. The standards, based upon NIST 800-53 controls, are a superset of the CJIS Security Policy and are equal or greater than FBI-CJIS Security Policy control expectations. The data center security staff provide the SOC 2 Reports to Motorola Solutions upon completion under Non-Disclosure Agreement (NDA). The reports can be shared with clients under an NDA. Motorola Solutions analyzes the information for non-compliance. Additionally, Motorola Solutions has committed to visiting the data center annually to validate that the Physical Security controls are sustained.

The most recent period of audit was October 1, 2018 through September 30, 2019. The report was analyzed along with physical observations of the facility. A review of the SOC 2 consisted of reviewing data center

operational documents that describe operations, planning and training to physically protect Motorola Solutions assets as well as, ensure greater than 99% availability uptime. The annual reviews by our staff indicate no deviations from the described controls to protect the facilities and assets at the data center.

The data center was visited in December 2019 to validate physical security controls. Conditions were equal to or greater than FBI-CJIS Security Policy criteria for a Physical Secure Location, including the protection of Motorola 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 Security gate, 12' fence, bollards, interior building access restrictions.

5.9.1.2 Physical Access Authorizations Pre-vetted credentials, visitors escorted, no–unanticipated visitors permitted. NTT employees have two factor credential access.

5.9.1.3 Physical Access Control Man-trap entry, proximity cards, iris biometric and credential card access to data vault, authorized visits for only pre-approved employees.

5.9.1.4 Access Control for Transmission Medium Underground private fiber - redundancy gateway routers

5.9.1.5 Access Control for Display Medium Does not apply. No logical access to the data, user interface or equipment in data center. Cabinets storing Motorola Solutions equipment are anonymously marked.

5.9.1.6 Monitoring Physical Access 24/7 security, alarms, face matching video – 30-day recording, access credentials, proximity cards.

5.9.1.7 Visitor Control Government ID check and recording of names, ID retained until credentials returned.

5.9.1.8 Delivery and Removal Controlled, monitored and logged. Separated secure storage space. Inventory control. Items not accepted without service ticket.

ENCRYPTION

In regard to encryption standards set by FBI CJIS Security Policy and the NIST FIPS 140-2 certification requirement for data security, we consider two items: "data in transit" and "data at rest." For data in transit, Motorola uses SSL/TSL with FIPS certified algorithms. For "data at rest" inside the Vigilant LEARN database at the data center, sensitive data (free text fields that may contain user appended Criminal Justice Information (CJI) or Personally Identifiable Information (PII)) is encrypted to the CJIS standard.

Within the ecosystem, there are several modes of encryption. From the initial detection prior to the data being sent via https, the data is not encrypted at the cameras. While the data is in transit to the Vigilant LEARN servers, the https protocols cited are used.

That protocol encrypts all data when it leaves the Vigilant CarDetector Mobile software application to the Vigilant LEARN software application and encrypts any responses sent to the end user, using the Internet to communicate to and from a Motorola Solutions owned and managed Microsoft Server 2012 R2. The Microsoft Server employs FIPS 140-2 certified 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 data center. Motorola Solutions uses Microsoft Windows Server 2012 R2 and the application module called Internet Information Services to enable the use of available certified encryption algorithms.

When a detection is matched to a hot listed plate in the Vigilant LEARN server (hot list supplied by client

agency via SFTP), the data leaves the Vigilant LEARN server, is encrypted via the Cisco router and traverses again via https back to the patrol vehicle that made the detection. The Vigilant CarDetector Mobile application in the patrol vehicle 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 and would be the responsibility of the customer when out of the car. Similarly, Vigilant FaceSearch™ information traversing the system and being stored on Motorola servers is encrypted.

The license plate field is left unencrypted to allow for rapid matching of inbound detection data against the hot list. All other sensitive fields are encrypted. License plate images are not encrypted and are stored at an Amazon Web Services facility in Ashburn, VA.

EVALUATION OF COMPLIANCE

Per FBI-CJIS Security Policy, facility compliance evaluation is the responsibility of the Contracting Government Agency to assess. Motorola firmly believes that the data center meets the Physical Security Controls criteria, satisfying compliance with FBI-CJIS Security Policy even if the data does not meet the FBI-CJIS definition. This belief is upheld by several independent reviews. Motorola Solutions develops and designs its enterprise system, including Vigilant LEARN applications, to be adherent with the FBI-CJIS Security Policy. Motorola Solutions has independently assessed the data center to inspect the facility and operations for physical security. We also evaluate annual SOC 2 Reports performed by third-party AICPA auditor. The NTT Data Center has FedRAMP Moderate certification issued by DHS.

Motorola Solutions designs for compliance whether it is required or not to provide the security and privacy controls the customer needs to make assurances to others that your service provider takes information security seriously.

Questions? Contact VigilantSupport@motorolasolutions.com
or call 925-398-2079.

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. **motorolasolutions.com**

MOTOROLA, MOTO, MOTOROLA SOLUTIONS and the Stylized M Logo are trademarks or registered trademarks of Motorola Trademark Holdings, LLC and are used under license. All other trademarks are the property of their respective owners. © 2020 Motorola Solutions, Inc. All rights reserved. 07-2020