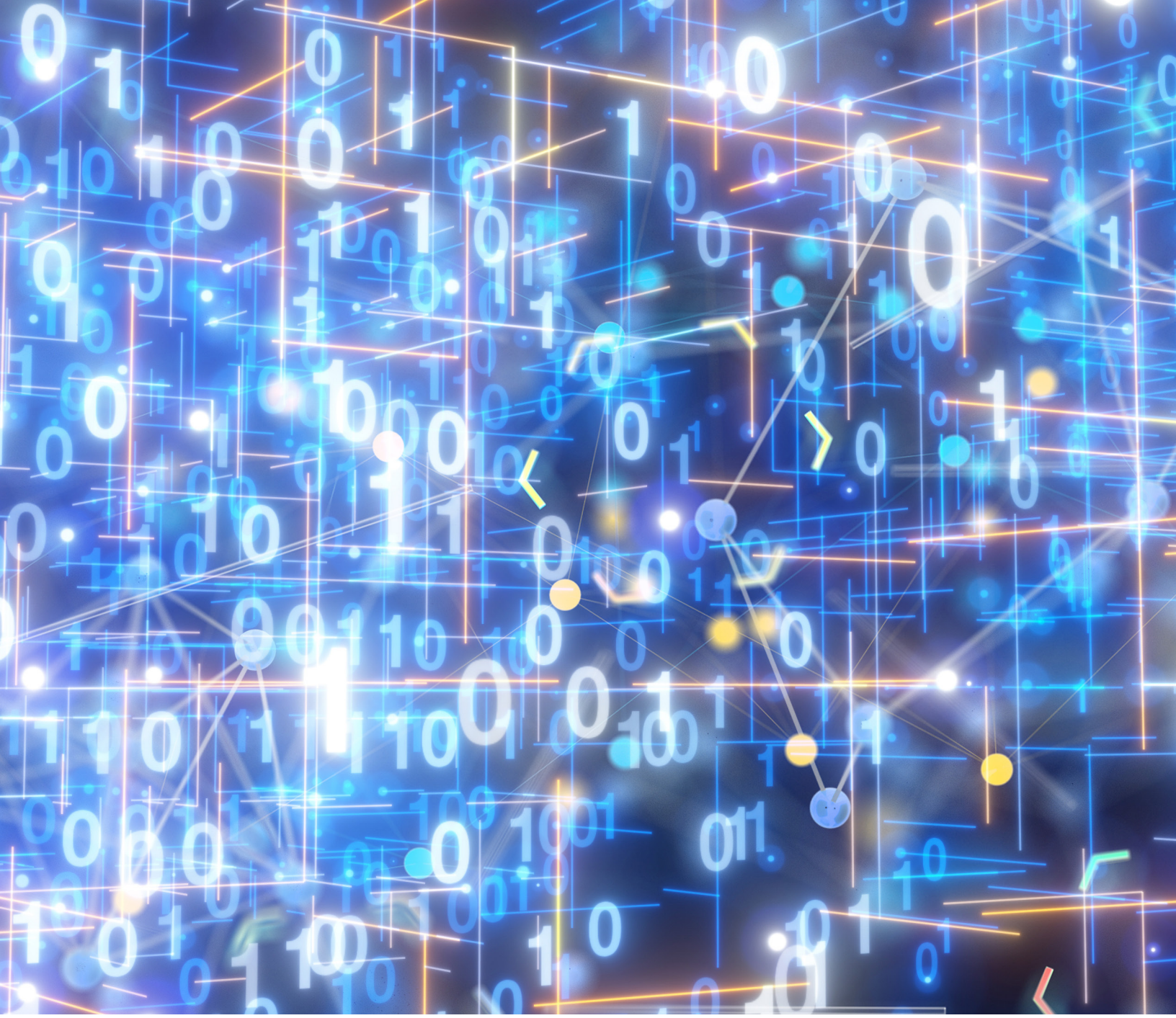

VIGILANT LEARN CJIS SECURITY COMPLIANCE GUIDE

MOTOROLA SOLUTIONS

OVERVIEW

Motorola Solutions offers to its law enforcement clients a hosted analytic solution known as Vigilant LEARN. The platform has two applications: Vigilant PlateSearchTM, and Vigilant FaceSearchTM. Unless on-premise deployment is required by the customer, all IT assets and software applications are hosted in colocation Infrastructure as a Service and Software as a Service configurations with Motorola Solutions' owned IT assets. Assets are located within Motorola Solutions' contracted data center. Physical and environment security controls are managed by Microsoft Azure. Information about the data center can be found at this link: Microsoft Azure Data Center. Plate images are stored separately at Amazon Web Services in Ashburn, VA.

Microsoft is a worldwide leader that provides hosted services and top-notch information security. Microsoft is certified ISO 9001:2015, 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 [SOC 2 Report]. The SOC 2 report is available under a Non-Disclosure Agreement. The public SOC 3 can be found here: SOC 3

The physical and network security employed at the Motorola data center are exhaustive.

The Microsoft Azure Data Center has been also certified as meeting FedRAMP medium security controls. While license plate reader data contains no personal information inherently, it is linkable through other sources or free text data fields that may enable the end user to input data that could be viewed as personally identifiable information (PII) or Criminal Justice Information (CJI) which is out of our control. Of greater relevance, law enforcement hot list information, such as NCIC and FaceSearch (mugshot) images, are managed by Motorola law enforcement customers and may potentially contain CJI as defined in 4.1 of the CJIS Security Policy. For these reasons, Motorola has voluntarily implemented security controls we believe are necessary to comply with the relevant sections. The current version of the FBI-CJIS Security Policy can be found here.

RELEVANT SECTIONS OF FBI-CJIS SECURITY POLICY

Within the scope of this document, and as it pertains to FBI-CJIS Security Policy, Motorola Solutions is a private contractor as defined in 5.1.1.5 of the FBI-CJIS Security Policy document. Going beyond the minimum requirements, the following table highlights those sections of the FBI-CJIS Security Policy that are believed to apply to the Motorola hosted solution:

5.1 Information Exchange

Information Exchange Agreements outline the roles, responsibilities and data ownership between agencies and any external parties.

Notes: Motorola's 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 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.

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 permitted to access CJI pursuant to an agreement between the CJA and the contractor that incorporates the FBI-CJIS Security Addendum approved by the Director of the FBI.

Notes: Motorola Solutions relevant staff will sign the executed FBI-CJIS Security Addendum when required by the client. Relevant User Agreements and contracts requiring Motorola Solutions signature will be reviewed and executed upon request.

5.1.1.6 Agency User Agreements

Fingerprint-based background checks and written agreement with the agency when required.

Notes: All Motorola staff have name-based background checks performed prior to final offer of employment. The Motorola development, networking and support teams which have access to hot list files, face images and other customer-owned criminal justice data for purposes of support and database maintenance only, have been subjected to fingerprint-based background checks as part of an agency-requested fingerprint-based background checks. Employees have successfully passed those background checks in several states. 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 a primary information exchange agreement, this shall be logged.

Notes: All data sharing and access is logged and available for audit reporting. There is a field that captures the entry of "on behalf of" searches.

5.2 Security Awareness Training

All personnel with access to CJI shall receive security awareness training within six months of assignment, and biennially thereafter.

Notes: Data Ownership - Motorola's 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, or 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.

5.2.2 Security Training Records

Records of security awareness training shall be kept current and maintained by a FBI-CJIS Security Officer (CSO).

Notes: Security Awareness Training records are retained and made available for review by customer agencies.

5.3.1.1 Reporting Structure and Responsibilities

Establishment of a primary POC for FBI-CJIS for incident handling and response.

Notes: The VP of Information Technology is the primary point of contact (POC) for the Incident Response Plan. Motorola Solutions has an Incident Response Plan.

5.4.1.1 Events

Description of the events that must be logged within the system.

Notes: Windows tracking locks account after 5 unsuccessful attempts. Application User Log-on and events associated with all user activities.

5.4.3 Audit Monitoring, Analysis and Reporting

Someone shall be responsible and appointed for review and analysis of audit records, at a minimum of once a week, to look for inappropriate or unusual activity.

Notes: Motorola enables auditing for agencies through its auditing tools and report scheduler. Motorola will assist clients with acquiring information that may be needed for their agency audits. Motorola audits their staffs' behavior for those authorized to access the software applications and data assigned to the support or development function.

5.4.6 Audit Record Retention

Agency shall retain audit records for at least one year.

Notes: Audit records are held indefinitely unless specified for deletion by the customer owner. Motorola executes retention routines established by the data owner. The metadata for transaction activity is retained for integrity and compliance audits.

5.5.2.1 Least Privilege

Agency shall approve individual access privileges and enforce the most restrictive set of rights and privileges needed by users for the performance of specified tasks. Logs maintain access privilege changes for a minimum of one year or at least equal to the agency's record retention policy, whichever is greater.

Notes: Vigilant LEARN provides customer-controlled functionality specifying tiered role-based access. The almost infinite number of user permissions and access controls through the creation of user profiles. Changes to rights and/or privileges are currently logged indefinitely and available in audit records.

5.5.2.4 Access Control Mechanisms

One or more 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.

Notes: Motorola uses ACL's to protect the database servers, firewalls and VPN and Vigilant LEARN software applications. Vigilant LEARN provides customer-controlled resource restrictions for the software application. Secure HTTP (https) for "data in transit." FIPS 104-2 certified for "data at rest" and "data in transit." Vigilant LEARN allows for agency management of role-based users, user profiles with permission sets, password policy management (character logic and change policy) consistent with FBI Security Policy.

5.5.3 Unsuccessful Login Attempts

CJIS Security Policy requires that after five consecutive invalid attempts, the account shall be locked out for a minimum of 10 minutes.

Notes: Motorola Solutions requires that five unsuccessful attempts result in a two-hour lockout.

5.5.4 System Use Notification

The system shall allow a notification message to be displayed to let users know a) they are accessing a restricted system, b) usage is monitored, recorded and subject to audit, c) unauthorized use is prohibited and may result in penalties, and d) use of the system indicated consent to monitoring.

Notes: Vigilant LEARN has a pop-up acknowledgment banner that must be affirmatively acknowledged prior to being granted access. That acknowledgment is logged by virtue of tracking system access by date, time and activity performed. The banner cannot be bypassed.

5.5.5 Session Lock

CJIS Security Policy requires that the system shall prevent access via a session lock after a minimum of 30 minutes of inactivity.

Notes: Motorola Solutions engages session lock after 15 minutes of inactivity, requiring re-entry of credentials.

5.5.7.3 Cellular

This section defines how agencies mitigate concerns surrounding bring your own device (BYOD).

Notes: This is an agency policy issue that doesn't drive any specific product requirements. Motorola'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.

Notes: 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.

Notes: ORI is captured at the agency level.

5.6.2.1.1 Password

This section details the requirements of passwords.

Notes: Motorola passwords follow the complexity and change requirements set forth in CJIS Security policy. Accounts are inactivated after 90 days without a password change and disabled after 120 days.

5.6.2.1.2 Personal Identification Numbers

Best Practices on PIN use.

Notes: N/A not used for Identification and Authentication.

5.6.2.2 Advanced Authentication

Defines Advanced Authentication requirements.

Notes: Vigilant LEARN uses optional two-factor authentication from SecureAuth to comply with this requirement. Client agencies may employ Advanced Authentication for physically non-secure locations. It can also be forced based upon customer requests.

5.6.3.1 Identifier Management

Requirements of agencies to manage user identifiers.

Notes: User credentials that are inactive for a period of 90 days are inactivated and disabled after 120 days within the system, requiring an Agency Manager to reactivate the account. Users and Agency Managers are notified with warnings during this process.

5.7.1.2 Network Diagram

Requirements for a network topological diagram.

Notes: Available upon request under an NDA.

5.8 Media Protection

Requirements for security and protection of electronic and physical media.

Notes: Motorola does not process or store electronic or physical media at Motorola headquarters or elsewhere unless being decommissioned. Comply with Media Disposal Policy by degaussing, secure overwrite and or physical destruction. Data at rest is encrypted during transit for decommissioning.

MSI utilizes the Azure GovCloud for its cloud offerings for infrastructure hardware. Microsoft employs strict policies to protect all media within the Azure GovCloud, is listed as CJIS compliant with 37 states, and maintains FedRAMP Moderate ATO for federal government use of the cloud. FedRAMP authorization by DHS ensures media protection and disposal policies that are consistent with the CJIS Security Policy and NIST 800-53 controls. Azure has a FedRAMP document to describe implementation of the policy controls which includes a third-party assessment.

The CJIS Security Policy requires customer agencies to implement appropriate policies for the retention, custody, and control of their digital or physical media. Accordingly, MSI and Microsoft do not maintain control over customer data accessed by the customer on endpoint devices. Each customer agency must maintain their own agency policy consistent with the CJIS Security Policy to control customer generated digital or physical media including retention, custody, control, and disposal.

MSI policy strictly prohibits employees from downloading or transferring customer data out of the production environment. MSI also requires all personnel to follow CJIS Security Policy for control of CJI within a production environment, including multi-factor authentication, least privilege, audit and accountability logging, vulnerability scanning, and mitigation.

MSI also has written policies and procedures governing this control area centered around data privacy that include data handling, media protection, disposal, and data breach provisions. MSI also has policies prohibiting the download of customer data. MSI creates no physical media with CJI.

5.9 Physical Protection

Requirements for physical security and access controls around all hardware, software and media.

Notes: Microsoft Azure Data Center and storage vault have been evaluated in 2018. The facilities exhibit extensive physical security controls that are in place and equivalent or greater than CJIS Physically Secure Location criteria. Physical security at the colocation data center is managed by Microsoft. They are responsible for physical security at that location that has been evaluated by Motorola Solutions staff and a third-party auditor.

Physical Protection for our Azure GovCloud environment is managed by Microsoft and, as indicated, has FedRAMP Moderate controls which have been validated with the Department of Homeland Security. Azure GovCloud has seven data centers to ensure the CJIS Security Policy requirements are met for data storage on U.S. soil. As a Trusted Provider in your state, Azure GovCloud has satisfied physical protection requirements to satisfy state CJIS System Agencies.

MSI uses stringent physical security controls for all its engineering facilities and has controlled areas for customer support and engineering staff. MSI buildings require credentialed card access from the exterior and for access to interior rooms that are classified as sensitive areas. Those sensitive areas have role-based credentialed access. All MSI facilities use visitor logs and have an escort policy. Any agency that would like to inspect our facilities can make arrangements to do so. Relevant physical security breaches will be reported to customers, as required by policy.

All MSI and Microsoft employees are required to use compliant Advanced Authentication for logical access to cloud resources or the MSI production environment.

5.10.1 Information Flow Enforcement

Prevent CJI from being transmitted unencrypted across the public network.

Notes: 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.

Notes: Industry standard Cisco inspection of all packets.

5.10.1.2 (1) Encryption

Minimum 128 bit.

Notes: Comply. FIPS-140-2 Certified. Certificates available upon request. Free text fields for data at rest.

5.10.1.3 Intrusion Detection Tools and Techniques

Specifies requirements for intrusion detection tools.

Notes: Automated monitoring via Cisco.

5.10.3.1 Partitioning

Outlines requirements for partitioning of data.

Notes: Motorola partitions web server, database server, user information, and more. Motorola uses all four types of partitioning listed.

5.10.4.1 Patch Management

Requirements for management of software patches.

Notes: Centralized management on Motorola's data center assets, with Change Management Plan, ample testing and roll back plans before install.

5.10.4.2 Malicious Code Protection

Virus Protection requirements.

Notes: Microsoft System Defender employed.

5.10.4.3 Spam and Spyware Protection

Spam and Spyware Protection requirements.

Notes: Cisco and Microsoft Security Essentials.

5.10.4.5 Security Alerts and Advisories

Guidance for alerts and advisories.

Notes: Mechanisms in place to deliver alerts via agency notifications and agency manager emails. Microsoft Azure has a Security Advisory alerting system that notifies the VP of IT, Director of IT and Field Support Manager in the event of a DDoS attack network and power outages.

5.12 Personnel Security

Fingerprint-based background checks and rules based on findings.

Notes: Support team and IT networking and application development teams have successfully completed national and state FBI fingerprint-based background check screening by a FBI-CJIS System Agency in several states that require the screening. If

prohibitive barrier offenses or activity occurs after the fact, access rights are suspended pending court action and those agencies requiring CJIS Personnel Screening are notified.

5.12.2 Personnel Termination

Terminated employees shall immediately have access revoked.

Notes: Notices are sent to the Director of IT immediately in coordination with termination date to remove from Active Directory.

5.12.4 Personnel Sanctions

Process for employees failing to comply with security policies.

Notes: Rules of behavior, policy and procedures are in place to deal with violations from counseling to termination.

NARRATIVE ON FBI-CJIS SECURITY POLICY

Motorola Solutions' Vigilant LEARN web-based solutions are exclusively available to law enforcement. All Motorola agencies are ORI vetted police agencies that manage the users they authorize. The data an agency collects can be shared to specific law enforcement agencies via MOU, and can be shared to Motorola's national law enforcement database, or exclusively retained for that client agency's use only. This is accomplished by Agency Manager employing configurable resource restrictions and role-based access privileges.

As a company, Motorola Solutions specifies in several places, including on its website and in its Enterprise Service Agreement—which is agreed to and signed prior to purchasing Motorola Solutions products and/or services—that the Vigilant LEARN data collected or contributed by law enforcement remains the property of the agency and Motorola Solutions has no rights to that data. That information is shared based upon the sharing rules established by the data owner. Motorola further classifies all this information internally as Criminal Justice Data and has strong policies for handling, storage and destruction of this information.

Motorola does not share, sell, or make use of law enforcement generated Criminal Justice Data in any way. Furthermore, any data retention policy or the sharing of an agency's data is entirely in the control of the agency. Many federal, state, county, and municipal jurisdictions have legislation or guidance on appropriate legal or privacy rules. The Vigilant LEARN client application allows for the Agency Manager role, within the customer agency, to make the necessary changes to data sharing

and retention rules. However, it is the sole responsibility of the data owner to ensure that the data submitted, entered or shared is done so in recognition and legal authority of the customer agencies governing laws, regulations and policies. The data owner is responsible for establishing the sharing rules, retention and appropriate rules for data entry, along with the accuracy and timeliness of the data.

Motorola 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. Motorola Solutions only allows staff to access the data when performing customer support duties that are authorized by the customer. Remote access sessions to customer systems to assist a client are intended to be granted access and monitored (virtual escorting) during the customer support session by the customer and through the mechanism agreed upon.

Those technical controls include configurable access rights, agency- controlled information sharing, logging user activity and access, account inactivation for periods of inactivity, session locks, system access strong password criteria, encrypted data transport and data storage at a facility that has criteria consistent with a FBI-CJIS Security Policy Physically Secure Location.

Even though Motorola Solutions has built-in tools to facilitate the audit and accountability controls criteria consistent with FBI-CJIS Security Policy, it is the client agency's responsibility to perform the audit processes with the Motorola Solutions product tools provided. Motorola Solutions internally monitors activity for system availability, unauthorized access activity and system and data integrity.

Motorola Solutions internally monitors activity for system availability, unauthorized access activity and system and data integrity. If the customer deems additional events and content logging are required, we will work with customers to remediate any perceived gaps.

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

PERSONNEL SECURITY

In an effort to ensure the integrity of Motorola's business relationships with clients and their data, as well as its purposes, Motorola Solutions performs commercial name-based background screening on all of its employees prior to employment.

When required by a client, all Motorola Solutions staff directly supporting its agencies that may have access are subject to FBI-CJIS Security Policy Personnel Screening procedures (Section 5.12). Motorola 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 existence of Criminal Justice Information or access to agency infrastructure that may contain Criminal Justice Information provided by FBI-CJIS.

Motorola Solutions staff has, however, successfully completed FBI fingerprint-based background check screening by the FBI-CJIS System Agency in several states that require the fingerprint-based background checks. 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. If Motorola Solutions becomes aware of any prohibiting activity, those employees' access rights to LEARN or customer systems are suspended pending final resolution by the courts. In those states requiring CJIS screening, those CJIS System Agencies and clients are notified of activity and suspension of access.

These employees, in addition to others, have executed and will upon request, execute the FBI-CJIS Security Addendum. Copies are retained by Motorola Solutions FBI-CJIS ISO along with records of Security Awareness Training that included topics on privacy, confidentiality and data security. Motorola Solutions staff performs security awareness training through CJIS Online, which has been accepted by all states requiring the CJIS Security Awareness Training. Security addenda are also posted there.

INCIDENT RESPONSE PLANNING

With the intention of meeting or exceeding the relevant aspects of the FBI-CJIS Security Policy, Motorola Solutions has several administrative and technical controls to adhere to those criteria in response to and subsequent reporting for cyber security events within its control. Motorola Solutions employs and manages malware and virus protection, patch management policies, intrusion detection and intrusion prevention systems to protect the customer-owned data in Vigilant LEARN. Motorola 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. Motorola 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.

Azure GovCloud has been evaluated in the approved states for an incident response plan and meets FedRAMP Moderate authorization. MSI and Microsoft will agree to report breaches of the provider boundary or internal network access controls to the affected customer Local Agency Security Officer (LASO) once verified.

PHYSICAL SECURITY

The physical protection mechanisms at the Microsoft Azure Government facility are consistent with, or greater than the FBI-CJIS Physically Secure Location criteria. They were evaluated in December 2019 by Motorola Solutions' staff with specific background and experience in FBI-CJIS Security Policy and do so annually. Additionally, Microsoft undergoes auditing by an independent third party auditor at the colocation facility. The data center also had FedRAMP Moderate certification approved by DHS. It must be noted that 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. To date, no law enforcement agency in the U.S. has required such agreements.

As part of meeting physical security requirements, Motorola Solutions Engineering and Support staff adhere to the personnel screening requirements, having executed the FBI-CJIS Security Addendum, submitting to fingerprint- based background checks and complete CJIS Security Awareness Training.

Motorola Solutions is responsible for the security, confidentiality and privacy of the data in their custody. That is accomplished through technical controls, consistent with the FBI-CJIS Security Policy, for the systems and data Motorola Solutions hosts for client agencies. Microsoft and Microsoft America, as a colocation facility. Microsoft only provides physical security for the facility, communications infrastructure, firewalls, reliable internet, power conditioning, HVAC, and is responsible for the confidentiality and privacy based upon those physical security controls. Motorola Solutions provides the physical equipment (servers, firewalls, etc.) and software that hosts the data and thus is responsible for those technical security controls.

Microsoft and Microsoft Azure staff have no authorized logical access (GUI) to Vigilant LEARN applications or physical access to the infrastructure systems or data in our secure server cabinets. Physical access to the equipment is controlled by Motorola Solutions. Only Microsoft Azure staff are permitted to access the equipment at the Virginia data center via a work order authorized by Motorola Solutions and, only in exigent circumstances. When doing so, Microsoft staff still have no access to the data for the applications. Unless there are exigent circumstances to power on or off the equipment, only Motorola Solutions staff can physically access the equipment at the Microsoft Azure Data Center. Access approvals are only when a pre-arranged visit is established.

As part of the physical security controls at the data center; cabinets storing the servers, routers and other equipment are unmarked and indistinguishable from other colocated clients. The Microsoft Azure center has multimodal biometric access protections that include face, iris, credential card and pin to access the interior portion of storage vaults and our storage cabinets. Once being granted access to the vault the unmarked cabinets are further protected by a unique combination lock on each cabinet.

The data center was visited in December 2019 to observe Microsoft physical security controls. Conditions were equal 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. Microsoft employees have two factor credential access.

5.9.1.3 Physical Access Control

Man trap entry, proximity cards, pre-authorized visits for only pre-approved employees.

5.9.1.4 Access Control for Transmission Medium

Secure private fiber underground with redundancy in gateway routers in secure remote space.

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 Microsoft facilities that contain the Motorola Solutions equipment. The configuration for the data storage is a colocation service arrangement with Microsoft Azure. There is no user interface to Motorola Solutions software applications. The equipment is secure and cabinets storing Motorola Solutions equipment are anonymously marked. Keys to the cabinets are only provided to equipment owners and Microsoft staff when contracted for service.

5.9.1.6 Monitoring Physical Access

24/7 Alarms, face search video and 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 a service ticket.

AUDITING AND ACCOUNTABILITY

Motorola Solutions' Vigilant LEARN applications have audit functions built in for an agency to view and audit user and transactional activity. The customer available audit functionality is consistent with those identified in the FBI-CJIS Security Policy. It was designed to enable integrity audits to increase the probability of authorized users conforming to a prescribed pattern of behavior. It focuses on "events" and "content" as specified in Section 5.4.1. Motorola Solutions audits its staff to ensure they adhere to our standards of acceptable use.

Auditing of the data center facilities, processes, policies and procedures are accomplished by a third-party auditing firm. The current auditing vendor, Ernst and Young produced the Service Organization Controls (SOC) 2 report. The SOC 2 is 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 are conducted to validate that processes, controls, and procedures are in place and performing as expected. Those SOC 2 AICPA standards are validated annually and are equal to or greater than FBI-CJIS Security Policy control expectations. The SOC 2 report is supplied to Motorola Solutions upon completion under Non-Disclosure Agreement (NDA) and can be shared with clients under NDA. Motorola Solutions analyzes the information for compliance. Additionally, Motorola Solutions has committed to visiting the data center annually to validate that the physical security controls are sustained. Note: SOC 2 reports are not an acceptable equivalent for the FBI-CJIS audit. Even though they provide valuable insight to security controls, they are not accepted in lieu of an audit by a CJIS agency.

The most recent period of audit for Microsoft was April 1, 2021 through March 31, 2022. The previous year's report (October 10, 2020 through March 31, 2021) was analyzed along with physical observations of the facility. A review of the SOC 2 & 3 consisted of reviewing operational documents and the SOC 2 & 3 reports that describe operations, planning and training to physically protect Motorola Solutions assets, as well as to ensure greater than 99% availability uptime. The SOC 2 and 3 Reports indicated no deviations from the described controls to protect the facilities and assets at the facility.

The Microsoft Azure Data Center also has undergone third party attestation leading up to FedRAMP moderate certification issued by DHS. This rigorous assessment process is based upon NIST 800-53 controls.

As stated, the policies, controls and procedures at the data center are equal to or greater than those for FBI-CJIS Security Policy, with one exception. Most data center personnel have not undergone national fingerprint-based background checks as it is based upon customer need and legal authority. But, data center staff do not have physical or logical access to unencrypted information. All data center staff have undergone name-based background checks and evaluated for suitability. Data center staff do not have authorized physical access to Motorola Solutions equipment and do not have access to unencrypted information. Those data center employees have no authorized administrator or user logical access to any Motorola Solutions software applications, servers, firewalls or routers. Data at rest is in a physically secure location and the free text fields that may contain CJI or PII are encrypted to the FIPS 140-2 NIST Certification. All data in transit is encrypted to FIPS 140-2 NIST Certification.

Customer data is not co-mingled with any data center assets.

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 Microsoft Azure Data Center meets the physical security controls criteria, satisfying compliance with FBI-CJIS Security Policy. This belief is upheld by several third- party independent reviews. Motorola Solutions develops and designs its enterprise system 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. The data center has been evaluated through the Service Organization Report 2 audit report performed by an outside organization for this policy area that is available for review.

Our parent company, Motorola Solutions complements our process with their own rigorous information security requirements that further enhance Motorola Solutions products.

FBI-CJIS CERTIFICATION VS. COMPLIANCE

In regard to certification. Because different state, local and federal agencies can have additional requirements or similar but different security controls for each of their contract relationships, e.g., storing investigative, CHRI data vs. PlateSearch, FaceSearch and data; those numerous variations of circumstances would not enable any cloud service provider to indicate that they are FBI-CJIS Security Policy compliant nationally. Even within a state, the state must designate if a solution is acceptable statewide. Amazon Web Services (AWS) literature also states this explicitly, so do not be misled.

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 fingerprints, 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 Web Services, services provided by Motorola Solutions and its colocation partner, Microsoft Azure, can only meet compliance through an analysis of the product by a government entity. There is no blanket compliance or certifications issued to a vendor or cloud service provider by a state or 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.

For example, in California, the state CJIS System Agency, California Department of Justice (Cal DOJ), went through the process of determining FBI-CJIS Security Policy compliance for use of the Enterprise Microsoft 365 product for that entity alone, by Cal DOJ agencies for that narrow scope purpose. Cal DOJ still requires analysis for any other enterprise or client application, such as LEARN, that is used for law enforcement or criminal justice agencies that will access data provided by them or CJI provided by the FBI-CJIS Division.

If a contracting government agency (law enforcement or criminal justice agency) has a desire to enter into the contracted government relationship for particular government services involving CJI, such as using cloud services, the cloud providers cited—including Motorola Solutions—can only provide the government entity documentation related to the administrative, technical, physical and personnel policy controls to demonstrate the controls are in place.

This information then needs to be evaluated and validated by the government entity to determine if what a service provider states meets compliance requirements and will stand up to the test of a FBI-CJIS Security Policy compliance audit. This analysis often will occur, if CJI is in the scope of the project, with the assistance of the FBI-CJIS Information Security Officer staff to enable meeting the FBI-CJIS Security Policy compliance criteria. In this case, it would be for the storage and access of the PlateSearch, FaceSearch and data, and first determine if the information is considered FBI-CJIS Security Policy defined Criminal Justice Information. Then, determine what parts of the CJIS Security Policy apply – all or some.

The evaluation of the documentation, clear contracts and agreements that set expectations, vendor reputation and trust are ultimately the way that information security control compliance is achieved regardless of the standard body that controls the requirements. You need a vendor you can develop and sustain a trusted relationship with.

FBI-CJIS Security Policy dictates that a location, facility or entity that houses or processes defined FBI Criminal Justice Information and used in a contracted relationship with a government entity for handling of Criminal Justice Information can only be considered a physically secure location if it is under management control of the contracting government agency. That requirement is formalized with a Management Control Agreement or similar document. The Management Control Agreement or other Information sharing 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. Or similarly if staff are connected to or accessing systems that may contain CJI. To be consistent with FBI-CJIS Security Policy, an agency needs to fully evaluate the information provided for a solution to determine compliance.

ENCRYPTION

All Vigilant LEARN "Notes" or free text fields stored "at rest" within Vigilant LEARN servers are encrypted to the FIPS 140-2 certification. All data "in transit" transmitted is encrypted as well using Microsoft Server 2019 FIPS 140-2 certificates.

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, Motorola Solutions uses encryption for transmitted data to and from servers deploying Secure Socket Layer/Transport Layer Security protocols.

That encryption protocol encrypts all data when it leaves the Car Detector Mobile software application Vigilant LEARN software application. The LEARN application encrypts all responses sent to the end user, using the Internet to communicate to and from a Motorola Solutions owned and managed Microsoft Server 2019. The Microsoft Server employs FIPS 140-2 certified algorithms during data transit and at rest. The server(s) are used to manage traffic as well as store and process data transactions on the servers located at the Microsoft Azure Data Center.

Motorola Solutions uses Microsoft Windows Server 2019 and the application module called Internet Information Services to enable the use of available encryption algorithms.

When a detection is matched to a hot listed vehicle in the Vigilant LEARN server (hot list could be 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 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. However, the free text field used by the end user that could contain sensitive information is 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, Motorola uses SSL/ TLS with FIPS certified algorithms. For data at rest (data inside LEARN databases at the data center), sensitive PII or potential CJI data is encrypted to NIST FIPS 140-2 certified standard.

HOW SECURE IS YOUR DATA CENTER?

The Microsoft Azure GovCloud data center is classified as a Tier 1 facility. That classification mitigates against would be attacks/ disclosure from people physically inside a secure facility or environmental or natural disasters. Furthermore, Motorola employees granted specific work access to a Motorola Solutions secure server have been subjected to national and state fingerprint background checks. Any instance of physical access to Motorola Solutions servers is first authorized by Motorola Solutions Director of IT and is documented at the Microsoft site. Microsoft staff do not have authorized physical or logical access to software or hardware. Motorola Solutions firmly believes we are a trusted partner you can trust to protect your data.

Additional questions can be referred to your Motorola Solutions representative.

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