Report on Motorola Solutions Inc.'s ActiveEye Managed Security Platform Relevant to Security and Confidentiality Throughout the Period April 1, 2025 to September 30, 2025

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Motorola Solutions Inc. ("Motorola Solutions")

Scope

We have examined Motorola Solutions' accompanying assertion titled "Assertion of Motorola Solutions Inc. Management" (assertion) that the controls within the Development and Technical Support Operations of its ActiveEye Managed Security Platform were effective throughout the period April 1, 2025 to September 30, 2025, to provide reasonable assurance that Motorola Solutions' service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Motorola Solutions, to achieve Motorola Solutions' service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Motorola Solutions uses subservice organizations to provide data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Motorola Solutions, to achieve Motorola Solutions' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Motorola Solutions' controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

Motorola Solutions is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Motorola Solutions' service commitments and system requirements were achieved. Motorola Solutions has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Motorola Solutions is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan

and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Motorola Solutions' service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Motorola Solutions' service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within the Development and Technical Support Operations of its ActiveEye Managed Security Platform were effective throughout the period April 1, 2025 to September 30, 2025, to provide reasonable assurance that Motorola Solutions' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Motorola Solutions' controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Louisville, Colorado
January 8, 2026

Section 2

Assertion of Motorola Solutions Inc. Management

Motorola Solutions, Inc.
500 W. Monroe
Chicago IL 60661

Assertion of Motorola Solutions Inc. (“Motorola Solutions”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Development and Technical Support Operations of the ActiveEye Managed Security Platform (system) throughout the period April 1, 2025 to September 30, 2025, to provide reasonable assurance that Motorola Solutions’ service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

The description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Motorola Solutions, to achieve Motorola Solutions’ service commitments and system requirements based on the applicable trust services criteria.

Motorola Solutions uses subservice organizations for data center colocation services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Motorola Solutions, to achieve Motorola Solutions’ service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Motorola Solutions’ controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2025 to September 30, 2025, to provide reasonable assurance that Motorola Solutions’ service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Motorola Solutions’ controls operated effectively throughout that period. Motorola Solutions’ objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period April 1, 2025 to September 30, 2025 to provide reasonable assurance that Motorola Solutions’ service commitments and system requirements were achieved based on the applicable trust services criteria.

Motorola Solutions Inc.

Attachment A

Motorola Solutions Inc.’s Description of the Boundaries of Its ActiveEye Managed Security Platform

Type of Services Provided

Delta Risk, a part of Motorola Solutions, Inc. (“the Company”), offers cloud security, Security Operations Center-as-a-Service, managed security, and professional services to commercial and public sector organizations. The Company provides visibility and controls for customers to enable effective cloud, endpoint, and network security.

ActiveEye Managed Security Platform, the Company’s proprietary platform, uses security orchestration automation and response (SOAR) to optimize and scale managed detection and response (MDR) capabilities across the enterprise. U.S. - based cyber security experts provide 24/7 monitoring, consulting, and guidance to customers. For additional information regarding Motorola Solutions’ public safety product suite, please visit https://www.motorolasolutions.com.

The Components of the System Used to Provide the Services

The boundaries of Motorola Solutions’ Development and Technical Support Operations of its ActiveEye Managed Security Platform are the specific aspects of the Company’s infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers or environments are not included within the boundaries of Motorola Solutions’ Development and Technical Support Operations of its ActiveEye Managed Security Platform.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes third-party cloud service providers to host the ActiveEye Managed Security Platform. The Company leverages the experience and resources of the third-party cloud service providers to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the ActiveEye Managed Security Platform architecture within the third-party cloud service providers to ensure the security and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools, suitable for supporting the ActiveEye Managed Security Platform’s operating systems, business functions, and production environments.

Software

Software consists of the programs and software that support the ActiveEye Managed Security Platform.

Software consists of the proprietary platform which utilizes SOAR software to optimize and scale the MDR capabilities offered by the ActiveEye Managed Security Platform. This software platform delivers several security capabilities, including providing user behavior analytics, detecting threat prioritization, and identifying misconfigurations or policy violations.

Further, the list below details the software functions used to build, support, secure, maintain, and monitor the ActiveEye Managed Security Platform:

- Remote access
- Ticketing system
- Source code control
- Secure electronic messaging
- System and event monitoring
- Single sign-on identity management
- Endpoint device management

People

The Company develops, manages, and secures the ActiveEye Managed Security Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for ActiveEye Managed Security Platform.
Information Security (InfoSec)	Responsible for managing access controls and the security of the production environment.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
Human Resources (HR)	Responsible for onboarding new personnel, defining the roles and positions of new employees, performing background checks, and facilitating the employee termination process.

The Executive Management team consists of the following individuals:

Greg Brown

Chairman and Chief Executive Officer

Greg Brown is chairman and chief executive officer of Motorola Solutions. Brown is in his 18th year as CEO of Motorola and Motorola Solutions. During Brown's tenure, he’s made over 50 acquisitions and achieved total shareholder return of over 1,200%. Today this almost 100-year-old global company is a leader in mission-critical networks in public safety and defense, 911 command center solutions and video security.

Under Brown’s leadership, Motorola Solutions has been named number one in its category on Fortune’s Most Admired list, named as one of the World’s Top Companies for Women by Forbes and one of the World’s Best Companies by Time Magazine, named to Newsweek’s Most Trustworthy Companies, named to Investor’s Business Daily’s 100 Best ESG Companies, and is considered one of the World’s Most Innovative Companies by Fast Company.

Brown was awarded the Yale Legend in Leadership Award in 2025. He was also named #1 underrecognized standout CEO of 2024 by Fortune as well as one of the top CEOs in America by Barron's in 2023. He is a member of the Pro Football Hall of Fame National Advisory Board and is also a member of The Business Council and the Council on Foreign Relations.

Brown served as Chairman of the Federal Reserve Bank of Chicago and Chairman of the Rutgers University Board of Governors, where he earned a bachelor's degree in economics and an honorary doctorate in humane letters. He also served as Midwest Chairman of the Navy Seal Foundation.

Jack Molloy

Executive Vice President and Chief Operating Officer

Jack Molloy is executive vice president and chief operating officer and leads global go-to-market operations. He oversees Motorola Solutions' global commercial strategy and day-to-day business operations, leading the teams responsible for sales, services, government affairs and marketing.

Molloy has held multiple leadership positions of increasing responsibility during his 31-year career with Motorola Solutions, including leading various sales organizations, systems integration, managed & support services and product development teams.

Molloy earned a bachelor's degree in marketing from Northern Illinois University and a master's degree in business administration from Loyola University.

Kathi Moore

Senior Vice President, Human Resources

Kathi Moore is senior vice president, Human Resources. She leads human resources for Motorola Solutions, as well as the Motorola Solutions Foundation.

Moore has held various human resources roles throughout her career and has deep knowledge of global rewards and talent, as well as a passion for employee engagement and retention.

Moore serves on the board for DuPage Pads Housing Solutions, a nonprofit organization serving individuals and families who are experiencing homelessness as the result of a disability.

Moore earned a bachelor's degree in business management from Benedictine University.

Rajan Naik

Senior Vice President, Strategy & Ventures

Rajan Naik is senior vice president, Strategy & Ventures, for Motorola Solutions. He is responsible for the corporate strategy organization, mergers and acquisitions, venture capital portfolio and competitive and market intelligence.

Prior to joining Motorola Solutions, Naik was senior vice president and chief strategy officer at Advanced Micro Devices and before that was a partner in the technology/media/telecom practice at McKinsey & Company.

Naik serves on the boards of directors for CSG and Evolv Technology.

Naik earned a bachelor's degree in engineering from Cornell University and a doctorate in engineering from the Massachusetts Institute of Technology.

Jim Niewiara

Senior Vice President, General Counsel

Jim Niewiara is senior vice president & general counsel. He leads legal, ethics and compliance for Motorola Solutions.

Niewiara joined Motorola Solutions in 2008 and has held several law leadership roles. Most recently, he was responsible for overseeing Motorola Solutions' commercial legal teams as well as litigation and intellectual property. Prior to Motorola, he spent 15 years as a commercial litigator in Chicago.

Niewiara earned a bachelor's degree in political science and economics from the University of Illinois at Urbana-Champaign and a law degree from Harvard Law School.

Mahesh Saptharishi

Executive Vice President and Chief Technology Officer

Mahesh Saptharishi is executive vice president and chief technology officer. He is responsible for Motorola Solutions' global product organization, overseeing product development for critical communications, video security and command center.

Saptharishi joined Motorola Solutions in 2018 through the acquisition of Avigilon, a video security solutions company, where he served as senior vice president and chief technology officer. Prior to Avigilon, he founded VideoIQ, a video analytics company that was acquired by Avigilon, as well as Broad Reach Security, which was later acquired by GE.

Saptharishi earned a doctoral degree in artificial intelligence from Carnegie Mellon University.

Jason J. Winkler

Executive Vice President and Chief Financial Officer

Jason Winkler is executive vice president and chief financial officer. He is responsible for Motorola Solutions' financial strategy and leads all financial functions as well as supply chain and information technology.

Since joining Motorola in 2001, he has held a number of financial leadership positions supporting investor relations, global channel management, mergers and acquisitions and product operations. Prior to this role, he led finance for Motorola Solutions' product and sales organization as senior vice president.

Winkler is the president of the Motorola Solutions Foundation and serves on the board of The Goodyear Tire & Rubber Company.

Winkler earned a bachelor's degree in business administration from Valparaiso University and a master's degree in business administration from the University of Chicago's Booth School of Business.

Cynthia Yazdi

Senior Vice President, Chief of Staff to the Chairman and CEO

Cynthia Yazdi is senior vice president and chief of staff, leading the office of the chairman and CEO.

Yazdi has held a variety of leadership positions in strategy, marketing and operations roles during her 25-year career with Motorola Solutions. Most recently, she had responsibility for the communications and brand function, and prior to that, global marketing and the Motorola Solutions Foundation. She also led product and business operations for the Asia Pacific and Middle East regions.

Yazdi earned a bachelor's degree in civil engineering from Concordia University.

Procedures

Procedures include the automated and manual procedures involved in the operation of the ActiveEye Managed Security Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. The procedures align with the Company's information security policies and are updated and approved annually, or whenever business changes require it.

The following table details the procedures as they relate to the operation of the ActiveEye Managed Security Platform:

Procedures	
Procedure	**Description**
Logical and Physical Access	How the Company restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical and physical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the ActiveEye Managed Security Platform production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for the transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest and enabled for cloud service provider environments.

Subservice Organizations

The Company uses subservice organizations for data center colocation services. The Company's controls related to the description does not extend to the colocation services for IT infrastructure provided by the subservice organizations.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Controls are expected to be in place at subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organizations' physical security controls should mitigate the risk of

unauthorized access to the hosting facilities. The subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews subservice organizations' SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to subservice organization management.

Complementary User Entity Controls

Complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Motorola, to achieve Motorola's service commitments and system requirements based on the applicable trust services criteria.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of the ActiveEye Managed Security Platform. Commitments are communicated in the Data Processing Addendum, Privacy Policy, and Professional Services Agreement.

System requirements are specifications regarding how the ActiveEye Managed Security Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to the ActiveEye Managed Security Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• The Company will ensure system access is granted to authorized personnel only. • The Company will protect data at rest and in transit, including implementing access controls. • The Company will identify and remediate security incidents and events.	• Logical access standards • Physical access standards • Encryption standards • Incident management Standards
Confidentiality	• The Company will maintain all customer data as confidential and will not disclose information to any unauthorized parties without written consent	• Data classification • Retention and destruction standards