MOTOROLA SOLUTIONS

AICPA System & Organization Controls (SOC) 3 Report

Security, Availability, Processing Integrity, Confidentiality, & Privacy
Trust Services

Reporting on Motorola Solutions, Inc.'s (Motorola Solutions)
Development and Technical Support Operations of its
Critical Communications Products and Services
and the Suitability of Design and Operating Effectiveness of Controls
for the period of April 1, 2024, to September 30, 2024.

Motorola Solutions, Inc.

Chicago, Illinois (primary environment location); Asheville, North Carolina; Bangalore, India; Copenhagen, Denmark; Krakow, Poland; Penang, Malaysia; Plantation, Florida; Schaumburg, Illinois; Tel Aviv, Israel (facilitating environment [satellite] locations)

Prepared Pursuant to
Attestation Standards, Section 101 of the AICPA Codification Standards (AT Section 101)
by:

NDB

MOTOROLA SOLUTIONS

TABLE OF CONTENTS

I. INDEPENDENT SERVICE AUDITOR'S REPORT

Motorola Solutions, Inc. ("Motorola Solutions")
Corporate Headquarters
500 W. Monroe St.
Chicago, IL 60661

Scope

We have examined **Motorola Solutions'** accompanying assertion titled "Written Statement of Assertion provided by Motorola Solutions, Inc." (assertion) that the controls within **Motorola Solutions' Development and Technical Support Operations of its Critical Communications Products and Services** system in **Chicago, Illinois (primary environment location); Asheville, North Carolina; Bangalore, India; Copenhagen, Denmark; Krakow, Poland; Penang, Malaysia; Plantation, Florida; Schaumburg, Illinois; Tel Aviv, Israel (facilitating environment [satellite] locations)** were effective throughout the period of **April 1, 2024, to September 30, 2024**, to provide reasonable assurance that **Motorola Solutions'** service commitments and system requirements were achieved based on the trust services criteria relevant to **Security, Availability, Processing Integrity, Confidentiality, & Privacy** (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria.

The description 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.

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. In Section II, **Motorola Solutions** has 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 AICPA. 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 the following:

- 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 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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating 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 **Motorola Solutions' Development and Technical Support Operations of its Critical Communications Products and Services** were effective throughout the period of **April 1, 2024, to September 30, 2024,** to provide reasonable assurance that **Motorola Solutions'** service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

NDB

Tallahassee, Florida.
December 11, 2024.

Docusign Envelope ID: E16E4389-E2DF-4C33-AF01-1243E3F632CA

II. WRITTEN STATEMENT of ASSERTION provided by MOTOROLA SOLUTIONS, INC.

We are responsible for designing, implementing, operating, and maintaining effective controls within **Motorola Solutions, Inc.'s ("Motorola Solutions") Development and Technical Support Operations of its Critical Communications Products and Services** for the **Chicago, Illinois (primary environment location); Asheville, North Carolina; Bangalore, India; Copenhagen, Denmark; Krakow, Poland; Penang, Malaysia; Plantation, Florida; Schaumburg, Illinois; Tel Aviv, Israel (facilitating environment [satellite] locations)** throughout the period of **April 1, 2024, to September 30, 2024**, to provide reasonable assurance that **Motorola Solutions'** service commitments and system requirements were achieved based on the trust services criteria relevant to **Security, Availability, Processing Integrity, Confidentiality, & Privacy** (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria. Our description of the boundaries of the system is presented in section III and identifies the aspects of the system covered by our assertion.

The description 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. The description presents **Motorola Solutions'** complementary user entity controls assumed in the design of **Motorola Solutions'** controls.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period of **April 1, 2024, to September 30, 2024**, to provide reasonable assurance that **Motorola Solutions'** service commitments and system requirements were achieved based on the applicable trust services criteria. **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 section III.

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 were achieved.

We assert that the controls within the system were effective throughout the period of **April 1, 2024, to September 30, 2024**, to provide reasonable assurance that **Motorola Solutions'** service commitments and system requirements were achieved based on the applicable trust services criteria.

Sincerely,

Name:	Rebecca Streib Montee	Jeff Park
Title:	Director, Data Protection Compliance, Data Protection – Products	Sr. Manager, Data Protection Compliance, Data Protection – Products
Date:	September 30, 2024	September 30, 2024
Signature:	Signed by: Rebecca V Streib Montee C4A744D0D30C4BB...	DocuSigned by: Jeff Park AC7AA01A3B044E3...

III. DESCRIPTION of the SYSTEM provided by MOTOROLA SOLUTIONS, INC.

Company Overview

Motorola Solutions, Inc.'s ("Motorola Solutions" or "the company") mission is to solve for safer by connecting people through technology. Public safety and commercial customers around the world turn to Motorola Solutions innovations when they want highly connected teams that have the information they need throughout their workdays and in the moments that matter most to them.

Motorola Solutions' customers rely on them for the expertise, services, and solutions they provide, trusting years of invention and innovation experience. By partnering with customers and observing how Motorola Solutions' products can help in their specific industries, Motorola Solutions is able to enhance its customers' experience every day.

Motorola Solutions serves more than 100,000 public safety and commercial customers in more than 100 countries. Their wide-ranging product portfolio has the tools customers need to get the job done in any business.

As an industry leader, Motorola Solutions designs and develops mission-critical communications products, including radios and the infrastructure that supports them. Motorola Solutions' mission-critical design philosophy led to new capabilities in the area of cognitive research that helps Motorola Solutions develop products for first responders by working with them in crisis situations to study their communication needs. Motorola Solutions takes what they learn in the field and brings it back to the lab to create products that will function under extreme conditions and networks that will reliably support those products.

Working with their global channel partner community, Motorola Solutions reaches an extensive customer base, from small businesses to Fortune 500 companies. The company's focus is on developing integrated end-to-end solutions that deliver a clear return on investment. Motorola Solutions' products empower individuals through seamless connectivity.

Products & Services

Motorola Solutions Inc. is a global leader in mission-critical communications and analytics. Motorola Solutions Inc.'s technology platforms in mission-critical communications, command center software, video security & analytics, bolstered by managed & support services, help communities solve for safer and help businesses stay productive and secure. Motorola Solutions Inc. accomplishes this by building and connecting technologies to help protect people, property, and places, enabling critical collaboration between public safety agencies and enterprises for a proactive approach to safety and security.

Motorola Solutions Inc.'s Critical Communications invents, builds, delivers, and integrates innovative technology solutions to customers across industries. Whether it's a nationwide radio system securely connecting a country's first responders, a cutting-edge broadband network enabling Industry 4.0 automation, or a cloud-based, AI-driven voice assistant for public safety - our designers, engineers, programmers, and integrators work together to make sure it delivers the kind of performance our customers count on. Our rugged devices and resilient infrastructure support your communications needs. Critical Communications makes devices and networks that perform exceptionally in the harshest conditions. Motorola Solutions Inc. provides equipment and networks built to keep you connected in the field or the factory, in a burning building, or in a crowded shopping mall. Critical Communications solutions are organized into APX & ASTRO Products, MOTOTRBO™, Business & Commercial Radios, and WAVE PTX offerings.

APX & ASTRO P25 Products

APX & ASTRO P25 Product offers include:

1. *ASTRO P25 Radio Systems* - Reliable and secure wide-area communication, built for the safety of your personnel and your community with the ability to collaborate across multiple organizations.

    1. P25 Security System
    2. ASTRO Radio Systems
    3. ASTRO Radio Sites and RF Equipment

1. *CirrusCentral* - Cirrus Central provides ASTRO application services that simplify operations and increase resiliency. Cirrus Central delivers a system management app built for ASTRO radio systems to keep your network operating at peak performance and secondary core, safely removed from local events, can maintain communications between first responders and dispatch if your premise P25 core becomes unavailable.

    1. CirrusCentral Management
    2. CirrusCentral Core

2. *ASTRO Applications & Services* - Applications & services that simplify operations and increase resiliency.

    1. CommandCentral AXS Dispatch
    2. Critical Connect (Interoperability between land mobile radio (LMR) systems, broadband PTT, and applications to eliminate barriers and unify communications for all responders)
    3. SmartConnect
    4. WAVE PTX

3. *MOTOTRBO™* - (Professional DMR radios designed to the highest specifications)

    1. Professional Digital Mobile Radios and applications

4. *Business & Commercial Radios* - (Purpose-built analog, digital and LTE radios for customers without private radio systems)

    1. Unlicensed Business Radios
    2. Licensed Business Radios
    1. Business Radio Software

5. *WAVE PTX* - (Instantly connect your team across different devices, networks and locations)

    1. Broadband PTT Devices and wireless service
    2. WAVE PTX Mobile APP
    3. WAVE PTX Dispatch
    4. WAVE PTX Support

Organizational Structure

Executive Committee

Greg Brown | Chairman and Chief Executive Officer
Greg Brown is chairman and chief executive officer of Motorola Solutions. Brown is in his 17th year as CEO of Motorola and Motorola Solutions. Under Brown's tenure at Motorola Solutions, he has made over 40 acquisitions and achieved total shareholder return of over 1300%. Today this almost 100-year-old global company is a leader in public safety and enterprise 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 America's Best Employers for Diversity and one of the World's Top Companies for Women by Forbes, as 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 Chairman & CEO of Micromuse. He also served as the Chairman of the Federal Reserve Bank of Chicago, Chairman of the Rutgers University Board of Governors and Midwest Chairman of the Navy Seals Foundation. He currently serves as Co-Chair of Prium and is also a member of the Council on Foreign Relations. Brown is also a member of the Pro Football Hall of Fame Advisory Board.

Brown was named as one of the top CEOs in America by Barrons in 2023. He has also received the Eisenhower Award from Business Executives for National Security. Brown has served two American presidents as part of President Obama's Management Advisory Board and President George W. Bush's National Security Telecommunications Advisory Committee.

Brown earned a bachelor's degree in economics and an honorary doctorate in humane letters from Rutgers University.

Karen Dunning | Senior Vice President, Human Resources
Karen Dunning is senior vice president, Human Resources. She leads human resources, DEI, labor & employment, and the Motorola Solutions Foundation for the company.

Dunning has held several leadership positions in strategy, business operations and engineering throughout her career with the company.

Dunning serves as the executive champion for the company's LGBTQ+ business council.

Dunning earned a bachelor's degree in finance and a master's degree in business administration from Florida Atlantic University.

Mahesh Saptharishi | Executive Vice President and Chief Technology Officer
Mahesh Saptharishi is executive vice president and chief technology officer. He is responsible for the company's public safety software and video security & access control solutions. He also leads the chief technology office.

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 serves as the executive champion for the company's LatinX business council.

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

Jack Molloy | Executive Vice President and Chief Operating Officer
Jack Molloy is executive vice president and chief operating officer. He leads the worldwide sales and services organization as well as product development for the company's land mobile radio portfolio.

Molloy has held multiple leadership positions of increasing responsibility during his 30-year career with the company, including leading various sales organizations, systems integration, managed & support services and video security & access control product development.

Molloy serves as the executive champion for the company's Motorola Black Inclusion and Diversity Organization and Persons with Disabilities and Allies business councils.

Molloy earned a bachelor's degree in marketing from Northern Illinois University and a master's degree in business administration from Loyola 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 and he serves as the executive champion for the company's Motorola Asian Pacific Islander business council.

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

Jason J. Winkler | Executive Vice President and Chief Financial Officer
Jason Winkler is executive vice president and chief financial officer. He is responsible for the company's 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 the company's product and sales organization as senior vice president.

Winkler serves as the president of the Motorola Solutions Foundation and as a member of the executive board of the Chicago Police Memorial Foundation. He also serves as the executive champion for the company's Veterans business council.

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, Communications & Brand

Cynthia Yazdi is senior vice president and chief of staff. She leads global communications and brand for the corporation. She also leads the office of the chairman and CEO.

Yazdi has held a variety of leadership positions in strategy, marketing and operations roles during her 24-year career with the company. Most recently, she had responsibility for the Motorola Solutions Foundation. She also led product and business operations for the Asia Pacific and Middle East regions.

Yazdi serves as the executive champion for the company's Young Professionals Group and Women's business councils.

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

Jim Niewiara | Senior Vice President, General Counsel
Jim Niewiara is senior vice president & general counsel. He leads legal, government affairs, and ethics and compliance for the company.

Niewiara joined Motorola Solutions in 2008 and has held several law leadership roles. Most recently, he was responsible for overseeing the company's 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.

RELEVANT ASPECTS of INTERNAL CONTROL

Control Environment

Management's Role and Example
Motorola Solutions is dedicated to providing accurate and timely information to critical decision processes for all of their customers. Management instills a philosophy that enables all employees to share in the success and growth of the company. A highly skilled and diverse group of employees comprise the organization's management team; these individuals are ultimately responsible for the vision and direction of Motorola Solutions. These members meet on a structured, routine basis to discuss a wide range of topics, and are also responsible for establishing policy and addressing all operational, financial, and social aspects of the organization. Employees are looked upon by management as "team players" who are instrumental in shaping and building an organization with high ethical standards, coupled with a unique, successful business model.

Management's Communication
Furthermore, Motorola Solutions strives to build and foster a workplace environment which encourages communication and open forum discussions on a wide range of topics, ranging from technical issues for internal operations and client needs, to social discussions regarding ways to improve their internal corporate culture. Employees are routinely evaluated and given feedback from management regarding their professional skills, work habits, and attainment of goals.

Policy and Procedure Documents
Motorola Solutions' fundamental principles and ethical values are documented in the employee handbook, which employees must acknowledge via signature that they have received and understand the policies contained within the actual handbook.

Risk Assessment

Motorola Solutions has implemented a risk assessment policy which addresses issues and concerns throughout the entire organization. By fully understanding stated objectives and goals within each division, as well as the associated risks that may develop, Motorola Solutions feels it has actively embraced all levels of risk.

Sales/Marketing
With clearly defined goals and objectives, sales and marketing employees actively search for new business leads to help grow the organization. They communicate openly and frequently to all other members of the Motorola Solutions management team regarding business development and market penetration. Additional topics of discussion among these individuals and senior management may also include labor, capacity, and productivity measures, both short-term and long-term. Motorola Solutions actively assesses the risks faced with a potential decline or growth in sales, and how it may affect the organization as a whole.

I.T. Personnel
These employees are responsible for the entire Information Technology (I.T.) infrastructure for Motorola Solutions. Activities range from maintaining the security and availability of the company network, to assisting the needs of all employees regarding any computer-related and network-related needs. Management is fully aware of the risks attributed to their I.T. infrastructure, specifically regarding the security and the efficiency of the network. As a result, Motorola Solutions employees are highly skilled professionals who are constantly monitoring and improving the security infrastructure of the organization.

I.T. personnel are directly responsible for the following technology activities within Motorola Solutions:

- *Logical Security* – Access rights for users of all company-wide systems.
- *Network Security* – Core hardware and software components that constitute the organization's network and all activity associated with these components.
- *Computer Operations* – Help desk activities along with system incremental and full media back-up.
- *Data Processing* – Any activities resulting in processing of information via computerized transaction processing environments.
- *Development and Production Environments* – Any activities resulting in the development of new technology tools and the subsequent release to a production environment.

Additionally, Motorola Solutions I.T. personnel are instrumental in researching and developing ideas and thoughts that result in technology being used in a more efficient and resourceful manner for the organization. Management is keenly aware of the risks associated with developing and producing new technologies and makes a concerted effort to hire and retain talented, skilled, and productive employees.

Finance and Accounting
These employees are responsible for a large array of issues, ranging from payments of organizational fixed and variable costs, building cash flow projection models, budgeting, and regulatory compliance, to collecting payments from clients and maintaining all other financial management activities. Risk assessment concerning cash flows and the ability to meet mandatory expenses is constantly monitored and evaluated. Issues such as lines of credit, cash

reserves, and other financial issues are discussed by senior management on a regular basis. Social issues are also studied and examined concerning employees, such as training, compensation, promotion, and the overall work environment of Motorola Solutions.

Control Activities

Motorola Solutions implements numerous policies and procedures that help ensure management directives are carried out, and implemented, and that appropriate actions are taken to address risks in achieving the organization's stated objectives. Control activities operate throughout Motorola Solutions at all levels, and in all functions. They include a range of activities, such as:

Authorizations
Permission or approval to conduct any activity (or activities) within the organization must follow a structured and regimented process. For new employees, access to systems and corporate facilities is granted based on one's assigned job duties and responsibilities. Users seeking a change or modification in access rights to systems and corporate facilities are required to go through a documented process, starting with a request to appropriate personnel, where changes for user access are undertaken. Authorizations for any type of change management activities within the organization must adhere to formal change policy procedures, with appropriate authorizations and approvals required for the change to ultimately take effect.

Verifications
User IDs and passwords are used throughout Motorola Solutions for ensuring that a valid verification process is in place. Logging and monitoring all critical organizational activities, ranging from security access points to network activity, can be conducted, if necessary, for ensuring a secure and continuous operation is in place that mitigates unauthorized or forced access.

Review of Operating Performance
Motorola Solutions enacts appropriate measures in reviewing, analyzing, and making recommendations pertaining to the organization's critical operational activities. Information systems, as well as all related hardware components and software applications, are routinely reviewed for ensuring maximum efficiency, along with validity and user appropriateness of all Information Technology components.

Security of Assets
Motorola Solutions employees who are assigned desktop computers, laptops, and/or any other company property are to use these devices for work activity only, and are not permitted to insert or download any software which has not been approved by the company. Anti-virus software is used on all computers for data protection.

Physical access to areas within the corporate facilities is limited to authorized personnel only, with access granted to these areas based on user appropriateness.

Segregation of Duties
Duties are segregated among employees to reduce the risk of error or inappropriateness. By creating effective barriers between duties, and continually assessing and making amendments to the definitions as these duties evolve, Motorola Solutions seeks to proactively address any matters before they become liabilities.

Whenever possible, Motorola Solutions enforces policies whereby an individual should not have responsibility for more than one of the three transaction components: authorizing transactions (approval), recording transactions (accounting), and handling the related asset (custody). Compensating controls are also used by Motorola Solutions

in situations where one person must conduct all of the business-related functions for a department. In occurrences such as this, additional personnel consisting of management will observe, review, and confirm the validity and completeness of transactions.

Information & Communication

Information

Documented policies exist for all critical activities of the organization's Information Technology infrastructure. Critical technology activities, along with all change management activities, are enacted through a formal process in accordance with company policy. Changes to existing systems, hardware, and software applications must be approved by management and aligned with the organization's business objectives and technology requirements. Motorola Solutions' business objectives are to have a synergistic alignment with goals of the organization, along with a realizable cost/benefit attribute. In addition, Motorola Solutions' technology objectives and requirements call for a secure configuration of all technology components with network and system reliability and maintenance.

Communication

Motorola Solutions embraces a belief that information should flow in an open forum environment, allowing discussion on a wide range of topics and subject matter by all employees. Management feels this will foster a true sense and understanding of the important role each employee plays in maintaining the security of the organization's infrastructure and the quality of internal control elements for their respective departments.

Motorola Solutions holds meetings on a routine basis. Additionally, effective communication with external parties, such as vendors, clients, brokers, consultants, and government entities enables Motorola Solutions to be proactive in addressing any issues before they become major constraints or liabilities.

Motorola Solutions' numerous policy and procedure documents are designed to adequately inform employees of policies and procedures relating to the workplace environment, and to one's professional conduct. Each department also has documented policies pertaining to their respective roles, duties, and how they should be carried out on a daily basis.

Monitoring

Motorola Solutions' internal control systems are continually monitored with ongoing procedures and activities, which occur in the course of operations. Any control deficiencies are immediately reported upstream to management, whereby corrective action is to be taken. Matters of a more serious nature are reported to top-level management.

Critical monitoring activities over internal controls for Motorola Solutions include the following areas:

- Sales/Marketing
- I.T. Personnel
- Finance and Accounting
- Daily Operations and Transaction Processing Environment

Applicability of Report

This report has been prepared to provide information on **Motorola Solutions' Development and Technical Support Operations of its Critical Communications Products and Services** that may be relevant to the requirements of its customers to meet the Trust Services Criteria for **Security, Availability, Processing Integrity, Confidentiality, & Privacy**. The report has been prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system which each customer may consider important. This report is limited to the controls in operation to support the services as defined in **Motorola Solutions' Development and Technical Support Operations of its Critical Communications Products and Services**. Additionally, the authorized users of the system providing these services are limited to **Motorola Solutions** personnel.

IV. GENERAL I.T. CONTROLS

General controls are the vital framework of any organization, as they provide the needed guidance and security measures that allow for the establishment of a secure, reliable, and continuous operation. These controls are the processes, policies, and procedures that relate to the organization's operations, Information Technology security, software and hardware infrastructure, transaction processing environments, and all other essential corporate activities and guidelines vital to Motorola Solutions' success.

The following general I.T. control areas are included within the scope of this System & Organization Controls (SOC) 3 report:

Change Management
Change management for information system resources consists of the policies, procedures, and all related activities involving changes to production systems as a whole. Change management must ensure that changes are authorized, tested, approved, properly implemented, and documented. For change management to be effective, a number of operational, I.T., and business initiatives are aligned within Motorola Solutions, such as having documented, formal processes in place and strict requirements for following the applicable processes and procedures, along with competent, well-skilled personnel involved in the entire change process itself. Motorola Solutions utilizes a formalized change management process, for which all policies, procedures, and related change functions are effectively documented accordingly.

Logical Security
Logical security elements outline the activities of valid computer users by controlling the resources they can access and the type of access permitted regarding applications and other related I.T. systems. Logical security can be enforced by the use of identification (authorization) and authentication practices. Motorola Solutions utilizes Role Based Access Control, whereby defined roles are identified and categorized accordingly in all systems to which employees have access. Furthermore, employees are only given the access needed to perform one's roles and responsibilities, as this helps ensure the safety and security of Motorola Solutions systems. Additionally, only authorized users are allowed to access Motorola Solutions systems, and terminated users are promptly removed from all company-wide access.

In summary, Motorola Solutions' user identity, provisioning, and access rights lifecycle is a series of administrative, operational, and technical activities. Related procedures are adopted, implemented, and undertaken for creating identities (identification), authenticating to system resources (authentication), assigning users certain access rights (authorization), and employing effective segregation of duties, while also undertaking various auditing, monitoring, logging, and reporting functions (accounting) for a given entity's distributed information systems environment. Furthermore, the user identity, provisioning, and access rights lifecycle management process should always strive to advocate security, scalability, and flexibility, along with the continued adoption of emerging technologies to meet its needs.

Network Security
Network security elements ensure the protection of networks and their services from unauthorized modification, destruction, intrusion, or disclosure. Network security provides assurance that a network performs its critical functions correctly, efficiently, and without any interference. Its primary goal is to provide a reliable and secure platform, designed specifically so that users and programs perform only the actions that are permitted.

Motorola Solutions has in place various information security and operational-specific policies and procedures discussing controls in place for ensuring the confidentiality, integrity, and availability of the entire organizational

network. Additionally, monitoring processes are in place for effectively monitoring critical systems, along with having comprehensive anti-virus measures also in place.

Noted elements of Motorola Solutions' network security infrastructure consist of the following:

1. Firewalls: Along with being properly provisioned, access to firewalls is only allowed by authorized personnel. These devices produce alerts and logs, along with periodically being updated with the latest vendor-required security upgrades. Furthermore, firewalls are configured to ensure that all traffic is properly inspected, so as to not allow direct connections between the untrusted internet and any internal hosts, such as databases and other critical servers. Only essential ports, protocols, and services are allowed, with all others being denied for helping ensure the safety and security of Motorola Solutions' network infrastructure.

2. Provisioning and Hardening: Motorola Solutions' information systems are properly provisioned, hardened, secured, and locked down for ensuring their confidentiality, integrity, and availability. Because improperly or poorly provisioned systems can often result in network exploitation by hackers, malicious individuals, and numerous other external and/or internal threats, the following provisioning and hardening procedures are applied as necessary when deploying critical systems:

    1. Vendor-supplied default settings are changed.
    2. All unnecessary accounts are eliminated.
    3. Only necessary and secure services, protocols, and other essential services are enabled as needed for functionality.
    4. All unnecessary functionality is effectively removed.
    5. All system security parameters are appropriately configured.

3. Remote Access: All access to Motorola Solutions information systems initiated outside the organization's trusted network infrastructure is considered "remote access," and as such, only approved protocols are used for ensuring that a trusted connection is initiated, established, and maintained. Specifically, all users utilize approved technologies, such as IPsec and/or SSL Virtual Private Networks for remote access, along with additional supporting measures, including Secure Shell.

4. Anti-Virus and Anti-Malware: Malicious software (malware) poses a critical security threat to Motorola Solutions' information systems; thus, effective measures are in place for ensuring protection against viruses, worms, spyware, adware, rootkits, Trojan horses, and many other forms of harmful code and scripts. Motorola Solutions has anti-virus (AV) solutions deployed on all information systems, as applicable, with the AV being the most current version available from the vendor, enabled for automatic updates, and configured for conducting periodic scans, as necessary. Because strong and comprehensive malware measures are not just limited to the use of AV, additional tools are employed as necessary for eliminating all other associated threats, such as those discussed. The seriousness of malware, and the growing frequency of attacks within organizations, requires that all I.T. personnel within Motorola Solutions stay abreast of useful tools and programs that are beneficial in combating harmful code and scripts.

5. Patch Management: All necessary system patches and system updates to Motorola Solutions' information systems (those defined as critical from a security perspective) are obtained and deployed in a timely manner as designated by the following software vendors and/or other trusted third-parties: (1) Vendor websites and email alerts. (2) Vendor mailing lists, newsletters and additional support channels for patches and security. (3) Third-party websites and email alerts. (4) Third-party mailing lists. (5) Approved online forums and

discussion panels. Effective patch management and system updates help ensure the confidentiality, integrity, and availability of systems from new exploits, vulnerabilities, and other security threats.

Additionally, all patch management initiatives are documented accordingly, which includes information relating to the personnel responsible for conducting patching, the list of sources used for obtaining patches and related security information, the procedures for establishing a risk ranking for patches, and the overall procedures for obtaining, deploying, distributing, and implementing patches specifically related to critical Motorola Solutions information systems.

6. Encryption: When necessary and applicable, appropriate encryption measures are invoked for ensuring the confidentiality, integrity, and availability of Motorola Solutions' information systems, as well as any sensitive data associated with them. Additionally, any passwords used for accessing and/or authentication to the specified system resource are encrypted at all times, as passwords transmitting via clear text are vulnerable to external threats. As such, approved encryption technologies, such as Secure Sockets Layer | Transport Layer Security, Secure Shell, and many other secure data encryption protocols are utilized when accessing the specified system resource.

7. System Monitoring: Motorola Solutions employs the following system monitoring initiatives for its information systems. (1) Event monitoring, such as user access. (2) Performance and Utilization monitoring, such as CPU capacity, disk utilization, etc.

8. Incident Response: Motorola Solutions has in place a documented global incident response plan, which include provisions for effectively preparing, detecting, responding, and recovering from an incident, along with initiating post-incident activities and awareness.

Computer Operations

Computer operations elements consist of daily activities that help facilitate core operational components of any organization. Computer operations provide assurance that an organization performs critical functions relating to tape/media, system monitoring, patch management, and other ancillary activities. As such, Motorola Solutions has in place comprehensive data backup policies, procedures, and supporting processes for ensuring all environments are backed up in a timely, accurate, and complete manner. Furthermore, any incidents relating to backups, such as backup failures, are corrected immediately for ensuring the integrity of the data.

Data backup and storage procedures for Motorola Solutions' information systems are initiated by authorized I.T. personnel consisting of documented processes and procedures that include the following initiatives: (1) The type of backup performed. (2) The date(s) and time(s) for the designated backup processes to commence. (3) The appropriate reporting procedures and related output for confirmation of backups (i.e., log reports, email notification, etc.). (4) Incident response measures in place for backup failures and/or exceptions. (5) Retention periods for all data backups as required by management, customers, and all necessary regulatory compliance mandates. Additionally, when data has been compromised due to any number of reasons, appropriate restore procedures are to be enacted that allow for complete, accurate, and timely restoration of the data itself.

V. COMPLEMENTARY USER ENTITY CONTROLS

Motorola Solutions' description of the controls of its **Development and Technical Support Operations of its Critical Communications Products and Services** system was designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at user organizations is necessary to achieve the stated criteria within the applicable trust services criteria that are included in the scope of the AICPA SOC 3 report. This section describes additional controls that should be in operation at user organizations to complement the controls within Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services** system. The user control considerations should not be regarded as a comprehensive list of all controls which should be employed by user organizations. There may be additional controls that would be appropriate for the processing of user transactions not identified in this report.

Clients utilizing Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services** system should be fully aware of the user controls listed below, and should endeavor to implement them to their fullest extent. Routine reviews of these controls should be conducted as part of the client's normal course of business, or as situations change, thus demanding additional review.

Additionally, in order for user organizations to rely on the controls reported herein, each User Organization must evaluate its own internal control structure to determine if the identified user control considerations are in place. The User Organization control considerations listed in this section do not purport to be and are not a complete list of the controls, as it is ultimately the responsibility of each said User Organization to identify their corresponding user control considerations.

Identified below is a list of general user control considerations that should be initiated by each respective User Organization:

- Implementation of sound and consistent internal controls regarding general I.T. system access and system usage appropriateness for all internal User Organization components associated with Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services**.

- Timely removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services**.

- Transactions for user organizations relating to Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services** system are appropriately authorized and transactions are secure, timely, and complete.

- For user organizations sending data to Motorola Solutions, data must be protected by appropriate methods for ensuring confidentiality, privacy, integrity, availability, and security.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services**.

- User organizations should report to Motorola Solutions in a timely manner regarding any material changes to their overall control environment that may adversely affect services being performed by Motorola Solutions' description of its **Development and Technical Support Operations of its Critical Communications Products and Services**.

- User organizations are responsible for contacting Motorola Solutions in a timely manner regarding any changes to personnel directly involved with services performed by Motorola Solutions. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Motorola Solutions.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Motorola Solutions.

- User organizations are responsible for developing, and if necessary, implementing a Business Continuity and Disaster Recovery Plan that will aid in the continuation of services provided by Motorola Solutions.

1. Additionally, user organizations are responsible for any actions undertaken by their users that may impact the confidentiality, integrity, and availability of the services being offered by Motorola Solutions. Ultimately, this requires that user organizations have in place comprehensive policies, procedures, processes, and best practices relating to the following core information security domains, as well as other relevant security and operational areas:
    1. Network Security
    1. Security Planning
    2. Security Categorization
    3. Physical Security
    4. Security Awareness Training
    5. Provisioning and Hardening
    6. Information Security Reference Material
    7. Time Synchronization
    8. Network Architecture
    9. Firewall Configuration and Rulesets
    10. Documented Business Needs
    11. Review and Auditing
    12. Access Rights
    13. Change Control | Change Management
    14. Patch Management
    15. Backup and Storage
    16. Encryption
    17. Event Monitoring
    18. Configuration and Change Monitoring
    19. Logging and Reporting
    20. Incident Response