Public Safety Threat Alliance
Member Agreement

This Member Agreement ("**Agreement**") is entered into between Public Safety Threat Alliance, a registered ISO established by Motorola Solutions, Inc., with offices at 500 W. Monroe Street, Suite 4400, Chicago, IL 60661 ("**PSTA**") and _____, ("**Member**") with offices at _____. PSTA and Member will each be referred to herein as a "**Party**" and collectively as the "**Parties**". This Agreement is effective as of the date of the last signature (the "**Effective Date**").

Whereas, the Public Safety Threat Alliance was created to administer, collect and share cyber threat intelligence information with a focus on public safety systems and mission critical networks;

Whereas, the goal of the Public Safety Threat Alliance is to provide Members with cyber intelligence relevant to public safety, provide shared best practices, to raise cybersecurity awareness and increase cyber maturity of the entire public safety landscape through Public Safety Threat Alliance distributed content;

Whereas, Member desires to participate and contribute to the Public Safety Threat Alliance, and receive cyber threat intelligence information from the Public Safety Threat Alliance in accordance with the terms of this Agreement.

1. Definitions

"Affiliate" shall mean any company, corporation or other entity controlled by, in control of or under common control with Member and Member has authority to contractually bind the entity. For purposes of this definition, "control" means the ownership, legally or beneficially, directly or indirectly, of more than 50% of the voting shares or more than 50% of the assets of any company or corporation.

"Authorized Users" are Member's employees, contractors, and the entities (if any) specified in an Ordering Document, provided such entity is an Affiliate of Member or otherwise approved by PSTA in writing (email from an authorized PSTA signatory accepted), which may include affiliates or other Member agencies.

"Content Materials" are anonymized, aggregated and/or other generalized information obtained from PSTA Members, PSTA customers and other external sources relating to security threat intelligence and mitigation data generally. Such Content Material may include, but is not limited to: third party threat vectors and IP addresses, file hash information, domain names, malware signatures and information, information obtained from third party sources, indicators of compromise, as well as tactics, techniques, and procedures used, learned or developed in the course of addressing security incidents. Content Materials may include Service Use Data and Personal Data.

"Controller" means the entity who collects and determines the purpose and means of Processing of Personal Data.

"Data Protection Laws" means all data protection laws and regulations applicable to a Party with respect to the Processing of Personal Data under the Agreement.

"Data Subjects" means the identified or identifiable person to whom Personal Data relates.

"Metadata" means data that describes other data.

"PSTA Data" means data owned by PSTA and made available to Member as Content Material.

“Ordering Document” means solution descriptions, equipment lists, statements of work, schedules, technical specifications, and other ordering documents setting forth the Fees associated with the Public Safety Threat Alliance Subscription, additional options or cyber security services to be purchased by Member and provided by PSTA and additional rights and obligations of the Parties.

“Other Sources” means sources of Content Material other than Member such as other Public Safety Threat Alliance Members, PSTA customers, third parties and sources providing publicly available information.

“Personal Data” means any information relating to an identified or identifiable natural person transmitted to PSTA by, through, or on behalf of Member and its Authorized Users as part of Content Material. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

“Process” or **“Processing”** means any operation or set of operations which is performed on Content Material, including Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, copying, analyzing, caching, organization, structuring, storage, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

“Processor” means the entity which Processes Personal Data on behalf of the Controller.

“Security Incident” means an incident leading to the accidental or unlawful destruction, loss, alteration or disclosure of, or access to Personal Data, while processed by PSTA.

“**Service Use Data**” means data generated about the use of the Products and Services through Customer’s use or PSTA’s support of the Products and Services, which may include Metadata, Personal Data, product performance and error information, activity logs, and date and time of use

“Member Contact Data” means data PSTA collects from Member and its Authorized Users for business contact purposes, including without limitation marketing, advertising, licensing, invoicing and sales purposes.

“Sub-processor” means other processors engaged by PSTA to Process Content Material which may include Personal Data.

“Third Party Data” means information obtained by PSTA from publicly available sources or its third party content providers which may be aggregated with Content Materials and thereby become part of Content Materials made available to Member by PSTA.

2. Public Safety Threat Alliance Participation

2.1 Member Participation. As a Member participating in the Public Safety Threat Alliance, and as governed by the terms herein, Member agrees to: (1) PSTA’s collection of Content Material from Member, (2) the aggregation of such Content Material with Content Material derived from other sources, (3) the Processing, use and distribution of such Content Material to Other Sources and/or (4) PSTA’s other use of the Content Materials for lawful business purposes, including improving its products and services. In exchange for Member’s participation hereunder, PSTA will provide

Member access to and use of the Public Safety Threat Alliance Content Material subject to the terms and conditions set forth in this Agreement.

2.2 Invoicing and Payment for Membership. Fees and charges applicable to the Public Safety Threat Alliance Membership (the “Fees”) will be as set forth in the applicable Ordering Document. PSTA will invoice Member at the frequency set forth in the applicable Ordering Document, and Member will pay all invoices within thirty (30) days of the invoice date or as otherwise specified in the applicable Ordering Document. Late payments will be subject to interest charges at the maximum rate permitted by law, commencing upon the due date. PSTA may invoice electronically via email, and Customer agrees to receive invoices via email at the email address set forth in an Ordering Document.

2.2.1. Taxes. The Fees do not include any excise, sales, lease, use, property, or other taxes, assessments, duties, or regulatory charges or contribution requirements (collectively, “Taxes"), all of which will be paid by Member, except as exempt by law, unless otherwise specified in an Ordering Document. If PSTA is required to pay any Taxes, Member will reimburse PSTA for such Taxes (including any interest and penalties) within thirty (30) days after Member’s receipt of an invoice therefore. Member will be solely responsible for reporting the Subscription, additional option or service for personal property tax purposes, and PSTA will be solely responsible for reporting taxes on its income and net worth.

3. Member Obligations

3.1. Content and Data Sharing. Member agrees to (1) at its discretion, actively share with PSTA its own properly anonymized, aggregated or generalized information as relevant to the Content Material, and for proposed inclusion and distribution as Content Material for the Public Safety Threat Alliance; (2) authorize all Member’s Content Material for use and distribution under the terms of this Agreement and Addendum A Traffic Light Protocol (“TLP Designation”) Labeling; (3) designate any additional limitations or instructions on use and distribution of Member’s Content Material; (4) use and redistribute such Content Material only in accordance with the Agreement and the applicable TLP Designation that accompanied the Content Material and (5) to allow for processing of underlying security threat intelligence information as may be identified in any active monitoring or cyber related engagement between PSTA and Member. Member has no rights to de-identify the TLP Designation of Content Material.

3.2 License and Use of Public Safety Threat Alliance Content Material. PSTA grants Member a limited, non-transferable, non-sublicensable, and non-exclusive license to use the Content Material solely for the Member’s internal business purposes and only for security related functions. Except as it relates to the Member’s own information and subject to those rights granted under other agreements with PSTA, the Content Material, including any information contributed by other Members, PSTA customers or third parties, is or becomes the property of PSTA for the benefit of the Public Safety Threat Alliance and may be included in the Content Material. The Content Material is provided for the purpose of use by the Public Safety Threat Alliance and its Members. Member will not, and require it’s Authorized Users to not: (a) use the Content Material, or derivative information therefrom, for any purpose other than Member’s internal business purposes and only for security related functions; (b) disclose the Content Material, or derivative information therefrom, except in accordance with the TLP Designation. (c) “white label” the Content Material, or derivative information therefrom or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (d) use such Content Material, or derivative information therefrom, in violation of applicable laws; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the Content Material; or
(f) modify such Content Material, or derivative information therefrom, or combine any of it with Member’s own data or other data or use the data to build databases. Member acknowledges

having been advised that the Content Material, or derivative information therefrom, is protected in the U.S. and internationally by a variety of laws, including but not limited to, copyright laws and treaty provisions, trademark laws, patent laws and other proprietary rights laws. Member shall notify the Public Safety Threat Alliance immediately in the event of any use or redistribution of the Shared Data (i) in violation of the TLP Designation, or (ii) the terms of this Agreement.

3.3 Confidentiality of the Content Material. The Content Material and other information shared by Member and PSTA for the benefit of the Public Safety Threat Alliance is deemed to be confidential and "sensitive", in accordance with Addendum A. Members will: (i) maintain the confidentiality of the Content Material and not disclose it to any third party, except as authorized by hereunder, or by the PSTA in writing or as required by a court of competent jurisdiction; (ii) restrict disclosure of the Content Material to its employees who have a "need to know" and not copy or reproduce the Content Material; (iii) take necessary and appropriate precautions to guard the confidentiality of the Content Material, including informing its employees who handle the Content Material that it is confidential and is not to be disclosed to others, but those precautions will be at least the same degree of care that the Member applies to its own confidential information and will not be less than reasonable care. The Parties acknowledge that the Cyber Information Security Act of 2015 (Sections 1503(d)(4)(B) and 1504(d)(3).c.) exempts disclosure under any state, local, or tribal "sunshine law" or similar law requiring disclosure of information or records.

3.3.1. Use of Content Material. In compliance with the restrictions on the use of Content Material in this Section 3.3, Section 3.2 (License and Use of Public Safety Threat Alliance Content Material) and elsewhere in this Agreement, and in the spirit of cooperation and mutual benefit intended among Members, Member agrees that it shall not use Content Material shared in confidence by another Member to the competitive disadvantage of, or to obtain a commercial advantage over, the sharing Member.

3.4 Subscription Software License. Subject to Member's and its Authorized Users' compliance with the Agreement, PSTA hereby grants Member and its Authorized Users a limited, non-transferable, non-sub-licenseable, and non-exclusive license to use the Public Safety Threat Alliance service and the associated documentation, solely for Member's network enterprise defenses. The foregoing license grant will be limited to use in the territory and to the number of licenses set forth in an Ordering Document (if applicable), and will continue for the applicable Membership Term. Member may access, and use the Public Safety Threat Alliance service only in Member's owned or controlled facilities, including any authorized mobile sites; provided, however, that Authorized Users using authorized mobile or handheld devices may also log into and access the Public Safety Threat Alliance service remotely from any location. Member agrees to be bound by the terms of the web based and mobile application licenses accessible at login. No custom development work will be performed under this Agreement.

4. <u>Public Safety Threat Alliance - PSTA Obligations</u>

4.1 Public Safety Threat Alliance Content Material. PSTA will collect Content Material from Member and aggregate that Content Material with other Content Material collected from Other Sources. PSTA will share the Content Material with Member and Other Sources, subject to the terms of this Agreement.

4.2 Anonymization of Content Material. When pre-anonymized Content Material is provided by Member to PSTA for inclusion and distribution through the Public Safety Threat Alliance, PSTA shall have the right to use and distribute such Content Material without further anonymization. Notwithstanding the foregoing, PSTA reserves the right to further anonymize, generalize or aggregate any such provided information, in its sole discretion, prior to release and distribution as part of the Content Material. For avoidance of doubt, PSTA has the sole and absolute discretion

relating to the inclusion or exclusion of information from the Content Material and may edit, modify, revise, shorten or choose not to use proposed contributions of information offered from Member or Other Sources.

4.3 Grant of License to Content Material by Member Member grants PSTA, its subcontractors and Sub-Processors a royalty-free, worldwide, non-exclusive license to use, Process, host, cache, store, reproduce, copy, modify, combine, analyze, create derivative works from Content Material from Member and to sub-license, communicate, transmit, and distribute such Content Material to Other Sources in connection with furtherance of the purposes set forth in the Recitals to this Agreement..

5. PSTA Processing of Content Materials Including Personal Data

5.1 Roles of the Parties. The Parties agree that with regard to the Processing of Personal Data hereunder, Member is the Controller and PSTA is the Processor.

5.2 PSTA's Processing of Content Materials. PSTA and Member agree that PSTA may only use and Process Content Material, including the Personal Data embedded in Service Use Data, in accordance with applicable law and Member's documented instructions for the following purposes: (i) to perform under the Agreement including but not limited to as set forth in section 4 above; (ii) analyze Data to operate, maintain, manage, and improve the Public Safety Alliance; and (iii) create new products and services. PSTA and Member agree that this Agreement and Member's use of the Content Material are Member's complete and final documented instructions to PSTA for the Processing of Content Materials, including Personal Data. Any additional or alternate instructions must be agreed to in writing as an amendment to this Agreement. Member represents and warrants to PSTA that Member's instructions, including appointment of PSTA as a Processor, have been authorized by the relevant controller. Content Materials may be processed by PSTA at any of its global locations and/or disclosed to
Sub-processors. It is Member's responsibility to notify Authorized Users of PSTA's collection and use of Content Materials, including Personal Data, and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use. Member represents and warrants to PSTA that it has complied with the terms of this provision.

5.3 Details of Processing. All Personal Data processed by PSTA through the Public Safety Threat Alliance shall be for purposes described herein and only for the duration of the operation of the Public Safety Threat Alliance. The categories of Data Subjects and types of Personal Data are set forth on **Annex I** to this Agreement.

5,4 Disclosure of Processed Data. Member agrees PSTA may disclose and share any Content Materials with Other Sources, in PSTA's discretion, to further the purposes of the Public Safety Threat Alliance. In the event a government or supervisory authority demands access to Content Material, to the extent allowable by law, PSTA will provide Member with notice of receipt of the demand to provide sufficient time for Member to seek appropriate relief in the relevant jurisdiction. In all circumstances, PSTA retains the right to comply with applicable law. PSTA must ensure that its personnel are subject to a duty of confidentiality with respect to Personal Data, and will contractually obligate its sub-processors to a duty of confidentiality, with respect to the handling of Personal Data contained in Content Materials.

5.5 Member's Compliance Obligations. Member is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Member must not use the Public Safety Threat Alliance Content Material in a manner that would violate applicable Data Protection Laws. Member must have sole responsibility

for (i) the lawfulness of any transfer of Personal Data to PSTA, (ii) the accuracy, quality, and legality of Personal Data provided to PSTA; (iii) the means by which Member acquired Personal Data, and (iv) the provision of any required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Member takes full responsibility to keep the amount of Personal Data provided to PSTA to the minimum necessary for PSTA to perform in accordance with the Agreement.

5.6. PSTA as a Controller or Joint Controller. In all instances where PSTA acts as a Controller it must comply with the applicable provisions of the PSTA Privacy Statement at https://www.PSTAsolutions.com/en_us/about/privacy-policy.html#privacystatement as each may be updated from time to time. PSTA holds all Member Contact Data as a Controller and must Process such Member Contact Data in accordance with the PSTA Privacy Statement. In instances where PSTA is acting as a Joint Controller with Member, the Parties must enter into a separate addendum to the Agreement to allocate the respective roles as joint controllers.

5.7 Sub-processors.

5.7.1 Use of Sub-processors. Member agrees that PSTA may engage Sub-processors who in turn may engage Sub-processors to Process Content Materials, including Personal Data in accordance with this Agreement. A current list of Sub-processors is set forth at **Annex II** When engaging Sub-processors, PSTA must enter into agreements with the Sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this Agreement.

5.7.2 Changes to Sub-processing. The Member hereby consents to PSTA engaging Sub-processors to process Member Data provided that: (i) PSTA must use its reasonable endeavors to provide prior notice of the addition or removal of any Sub-processor, which may be given by posting details of such addition or removal at a URL provided to Member in **Annex II;** (ii) PSTA imposes data protection terms on any Sub-processor it appoints that protect the Personal Data to the same standard provided for by this Agreement; and (iii) PSTA remains fully liable for any breach of this clause that is caused by an act, error or omission of its Sub-processor(s). The Member may object to PSTA's appointment or replacement of a Sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, PSTA will either appoint or replace the Sub-processor or, if in PSTA's discretion this is not feasible, the Customer may terminate this Agreement.

5.8. Data Subject Requests. PSTA must, to the extent legally permitted, promptly notify Member if it receives a request from a Data Subject, including without limitation requests for access to, correction, amendment, transport or deletion of such Data Subject's Personal Data and, to the extent applicable, PSTA must provide Member with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Member must respond to and resolve promptly all requests from Data Subjects which PSTA provides to Member. Member must be responsible for any reasonable costs arising from PSTA's provision of such assistance under this Section.

5.9. Data Transfers. PSTA agrees that it must not make transfers of Personal Data under this Agreement from one country's jurisdiction to another unless such transfers are performed in compliance with this Agreement and applicable Data Protection Laws. PSTA agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit PSTA to transfer Personal Data to its affiliates and Sub-processors. PSTA agrees to amend as necessary its agreement with Member to permit transfer of Personal Data from PSTA to Member. PSTA also agrees to assist the Member in entering into agreements with its affiliates and Sub-processors if required by applicable Data Protection Laws for necessary transfers.

5.10. Security. PSTA must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects..

5.10.1. Security Incident Notification. If PSTA becomes aware of a Security Incident involving Personal Data provided by Member, then PSTA must (i) notify Member of the Security Incident without undue delay, (ii) investigate the Security Incident and apprise Member of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of PSTA. Notification of a Security Incident must not be construed as an acknowledgement or admission by PSTA of any fault or liability in connection with the Security Incident. PSTA must make reasonable efforts to assist Member in fulfilling Member's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

5.11. Data Retention and Deletion.

Except for anonymized Personal Data, or as otherwise provided under the Agreement, PSTA will delete all Personal Data provided by Member no later than eighteen (18) months following termination or expiration of this Agreement unless otherwise required to comply with applicable law.

5.12. CCPA and CPRA. If PSTA is Processing Personal Data within the scope of the California Consumer Protection Act ("CCPA") and/or the California Privacy Rights Act ("CPRA") (collectively referred to as the "California Privacy Acts"), Member acknowledges that PSTA is a "Service Provider" within the meaning of the California Privacy Acts. PSTA must process Member Data and Personal Data on behalf of Member and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the California Privacy Acts including under any "sale" exemption. In no event will PSTA or Member sell any such data. If a California Privacy Act applies, Personal Data must also include any data identified with the California Privacy Acts or Act's definition of personal data. PSTA shall provide Member with notice should it determine that it can no longer meet its obligations under the California Privacy Acts, and the parties agree that, if appropriate and reasonable, Member may take steps necessary to stop and remediate unauthorized use of the impacted Personal Data.

5.13. CPA. If PSTA is Processing Personal Data within the scope of the Colorado Privacy Rights Act ("CPA"), PSTA will comply with its obligations under the CPA, and shall make available to Member all information in its possession necessary to demonstrate compliance with obligations in accordance with § 6-1-1305(5)(d)(II)(A) of the CPA.

5.14. PSTA Contact. If Member believes that PSTA is not adhering to its privacy or security obligations hereunder, Member must contact the PSTA Data Protection Officer at PSTA Solutions, Inc., 500 W. Monroe, Chicago, IL USA 90661-3618 or at privacy1@PSTAsolutions.com.

6. <u>Term and Termination</u>

This Agreement will be for a twelve (12) month period and will automatically renew for an additional twelve (12) month period unless either Party notifies the other Party of its intent not to renew at least thirty (30) days before the conclusion of the then-current term. PSTA may terminate this Agreement or suspend collection or delivery of the Content Material immediately if (a) Member breaches the Agreement relating to its responsibilities, license obligations, or restrictions relating to the Content Material, or (b) PSTA determines that Member's use of the Content Material poses, or may pose, a security or other risk or adverse impact to the Public Safety Threat Alliance, PSTA, PSTA's systems,

or any third party (including other Public Safety Threat Alliance Members or PSTA customers). Member acknowledges that PSTA made a considerable investment of resources in the development, formation, and operations of the Public Safety Threat Alliance and that Member's breach of the Agreement will result in irreparable harm to the Public Safety Threat Alliance and PSTA for which monetary damages would be inadequate. If Member breaches this Agreement, in addition to termination, the Public Safety Threat Alliance and PSTA will be entitled to all available remedies at law or in equity (including immediate injunctive relief). In addition to any other termination rights PSTA may terminate the Agreement, in whole or in part, in the event it plans to cease offering the Public Safety Threat Alliance to Members.

7 LIMITATION OF LIABILITY

7.1. DISCLAIMER OF CONSEQUENTIAL DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, PSTA, ITS AFFILIATES, AND ITS AND THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, SUBCONTRACTORS, SUBPROCESSORS, AGENTS, SUCCESSORS, AND ASSIGNS (COLLECTIVELY, THE "PSTA PARTIES") WILL NOT BE LIABLE IN CONNECTION WITH THIS AGREEMENT (WHETHER UNDER PSTA OR MOTOROLA'S INDEMNITY OBLIGATIONS, A CAUSE OF ACTION FOR BREACH OF CONTRACT, UNDER TORT THEORY, OR OTHERWISE) FOR ANY INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES OR DAMAGES FOR LOST PROFITS OR REVENUES, EVEN IF PSTA OR MOTOROLA HAS BEEN ADVISED BY CUSTOMER OR ANY THIRD PARTY OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES AND WHETHER OR NOT SUCH DAMAGES OR LOSSES ARE FORESEEABLE.

7.2. DIRECT DAMAGES. EXCEPT FOR PERSONAL INJURY OR DEATH, THE TOTAL AGGREGATE LIABILITY OF THE PSTA OR MOTOROLA PARTIES, WHETHER BASED ON A CLAIM IN CONTRACT OR IN TORT, LAW OR EQUITY, RELATING TO OR ARISING OUT OF THIS AGREEMENT, WILL NOT EXCEED TEN THOUSAND DOLLARS ($10,000). FOR AVOIDANCE OF DOUBT, THE LIMITATION IN THIS SECTION 7.2 APPLY IN THE AGGREGATE TO INDEMNIFICATION OBLIGATIONS ARISING OUT OF THIS AGREEMENT OR ANY RELATED ADDENDUM HERETO.

7.3. ADDITIONAL EXCLUSIONS. NOTWITHSTANDING ANY OTHER PROVISION OF THIS AGREEMENT OR ANY RELATED ADDENDUM, PSTA AND MOTOROLA WILL HAVE NO LIABILITY FOR DAMAGES ARISING OUT OF (A) MEMBER DATA OR CONTENT MATERIAL INCLUDING ITS TRANSMISSION TO OR RECEIPT FROM PSTA OR MOTOROLA, THROUGH THE PUBLIC SAFETY THREAT ALLIANCE; (B) CUSTOMER-PROVIDED EQUIPMENT, CONTENT MATERIAL, THIRD-PARTY EQUIPMENT, HARDWARE, SOFTWARE, SERVICES, DATA, OR OTHER THIRD-PARTY MATERIALS, OR THE COMBINATION OF PRODUCTS AND SERVICES WITH ANY OF THE FOREGOING; (C) LOSS OF DATA, HACKING, RANSOMWARE, OR OTHER THIRD-PARTY ATTACKS OR DEMANDS; (D) MODIFICATION OF CONTENT MATERIAL BY ANY PERSON OTHER THAN PSTA OR MOTOROLA; (E) RECOMMENDATIONS PROVIDED IN CONNECTION WITH THE CONTENT MATERIALS; (F) DATA RECOVERY SERVICES OR DATABASE MODIFICATIONS; OR (G) MEMBER'S OR ANY AUTHORIZED USER'S BREACH OF THIS AGREEMENT OR ANY RELATED AGREEMENT OR MISUSE OF THE PUBLIC SAFETY THREAT ALLIANCE; (H) INTERRUPTION OR FAILURE OF CONNECTIVITY, VULNERABILITIES, OR SECURITY EVENTS; (I) DISRUPTION OF OR DAMAGE TO MEMBER'S OR THIRD PARTIES' SYSTEMS, EQUIPMENT, OR DATA, INCLUDING DENIAL OF ACCESS TO USERS, OR SHUTDOWN OF SYSTEMS CAUSED BY INTRUSION DETECTION SOFTWARE OR HARDWARE; (J) AVAILABILITY OR ACCURACY OF ANY DATA AVAILABLE THROUGH THE CONTENT MATERIAL OR OTHERWISE, OR INTERPRETATION, USE, OR MISUSE THEREOF; (K) TRACKING AND LOCATION-BASED SERVICES; OR (L) BETA SERVICES. THE CONTENT MATERIAL IS PROVIDED AS IS AND IS DISTRIBUTED FOR INFORMATION PURPOSES ONLY AND IS NOT WARRANTED FOR COMPLETENESS, TIMELINESS, ACCURACY,

MERCHANTABILITY, FITNESS FOR ANY PARTICULAR PURPOSE, AVAILABILITY OR OTHERWISE.

8. Member Indemnity.

Unless otherwise prohibited by law, Member will defend, indemnify, and hold PSTA and Motorola harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to (a) Member provided Content Material, including any claim, demand, action, or proceeding alleging that any such Content Materials (or the integration or use thereof with the products and Services) infringes or misappropriation a third-party intellectual property or other right, violates applicable law, or breaches the Agreement; or (b) Member's or its Authorized User's use of, access to and/or reliance on any Content Material from PSTA or Motorola through the Public Safety Threat Alliance (b) Member's or its Authorized User's breach of this Agreement; or (c) Member's (or its service providers, agents, employees, or Authorized User's) negligence or willful misconduct.
The Public Safety Threat Alliance will give Member prompt, written notice of any claim subject to the foregoing indemnity. The Public Safety Threat Alliance will, at its own expense, cooperate with Member in its defense or settlement of the claim.

9. General Provisions

9.1 Third-Party Beneficiaries. The Agreement is entered into solely between, and may be enforced only by, the Parties. Each Party intends that the Agreement will not benefit, or create any right or cause of action in or on behalf of, any entity other than the Parties.

9.2 Entire Agreement; General Information. This Agreement constitutes the entire agreement between Member and the PSTA with respect to the subject matter hereof and governs the use of Content Material and other related services. If any provision of this Agreement is held to be invalid by any law, rule, order or regulation of any government or by the final determination of any state or federal court, such invalidity shall not affect the enforceability of any other provision of this Agreement. The failure of PSTA or Motorola to exercise or enforce any right or provision of the Agreement shall not constitute a waiver of such right or provision. The Parties agree that the statutes and laws of the United States and the State of Member's jurisdiction without regard to conflicts of laws principles, will apply to all matters relating to this Agreement, and that any litigation shall be subject to the exclusive jurisdiction of the state or federal courts in the State of Member's jurisdiction. The Parties further agree that regardless of any statute or law to the contrary, any claim or cause of action arising out of or related to this Agreement must be filed within one (1) year after such claim or cause of action arose or be forever barred.

9.3 Authority. Each party represents that it has obtained all necessary approvals, consents and authorizations to enter into this Agreement and to perform its duties under this Agreement; the person executing this Agreement on its behalf has the authority to do so; upon execution and delivery of this Agreement by the parties, it is a valid and binding contract, enforceable in accordance with its terms; and the execution, delivery, and performance of this Agreement does not violate any bylaw, charter, regulation, law or any other governing authority of the party. The terms of this Agreement may be amended or modified only by a written instrument signed by authorized representatives of both Parties. The preprinted terms and conditions found on any Member purchase order, acknowledgment or other form will not be considered an amendment or modification of this Agreement, even if a representative of each Party signs that document.

9.4. Assignment and Subcontracting. Neither Party may assign or otherwise transfer this

Agreement without the prior written approval of the other Party. PSTA or Motorola may assign or otherwise transfer this Agreement or any of its rights or obligations under this Agreement without consent (a) for financing purposes, (b) in connection with a merger, acquisition or sale of all or substantially all of its assets, (c) as part of a corporate reorganization, (d) to a non-profit entity approved as an ISAO or (e) to a subsidiary corporation. Subject to the foregoing, this Agreement will be binding upon the Parties and their respective successors and assigns.

9.5. Independent Contractors. Each Party will perform its duties under this Agreement as an independent contractor. The Parties and their personnel will not be considered to be employees or agents of the other Party. Nothing in this Agreement will be interpreted as granting either Party the right or authority to make commitments of any kind for the other. This Agreement will not constitute, create, or be interpreted as a joint venture, partnership, or formal business organization of any kind.

9.6. Interpretation. The section headings in this Agreement are included only for convenience The words “including” and “include” will be deemed to be followed by the phrase “without limitation”. This Agreement will be fairly interpreted in accordance with its terms and conditions and not for or against either Party.

9.7. Notices. Notices required under this Agreement to be given by one Party to the other must be in writing and either personally delivered or sent to the address provided by the other Party by certified mail, return receipt requested and postage prepaid (or by a recognized courier service, such as FedEx, UPS, or DHL), and will be effective upon receipt.

9.8. Cumulative Remedies. Except as specifically stated in this Agreement, all remedies provided for in this Agreement will be cumulative and in addition to, and not in lieu of, any other remedies available to either Party at law, in equity, by contract, or otherwise. Except as specifically stated in this Agreement, the election by a Party of any remedy provided for in this Agreement or otherwise available to such Party will not preclude such Party from pursuing any other remedies available to such Party at law, in equity, by contract, or otherwise.

9.9. Survival. The following provisions will survive the expiration or termination of this Agreement for any reason: Section 3 - Member Obligations; Section 6 - Term and Termination; Section 7 - LIMITATION OF LIABILITY; Section 8 - Member Indemnity; Section 9.7 - Notices and Section 9.8 - Cumulative Remedies.

PSTA, Registered ISAO **Motorola Solutions, Inc.**	**Member: _____**
Signed: Leah Schmid	Signed: _____
Name: Leah Schmid	Name: _____
Title: Director, Business Operations	Title: _____
Date: 03/01/2023	Date: _____

Signed pursuant to a delegation of authority from:

Name: Scott Kaine

Title: Corporate Vice President

Entity: Motorola Solutions, Inc.

ADDENDUM A - Traffic Light Protocol Labeling

Public Safety Threat Alliance furnished Intelligence information shall not include classified information. The Member and PSTA agree that all information submitted, processed, stored, archived, or disposed of on or through Public Safety Threat Alliance is “sensitive” information and will be labeled and handled in accordance with the U.S. Department of Homeland (“DHS”) Security classification guidelines (Traffic Light Protocol (TLP)).

As part of the PSTA, agencies and other Members are encouraged to share their own cybersecurity threat experiences to improve the awareness and readiness of the overall group. Submitting agencies should stipulate the level of disclosure required for their submissions according to the PSTA Traffic Light Protocol (TLP), based upon the CISA Traffic Light Protocol guidance, which helps all Members submit and leverage insights while being respectful of the submitting agency’s preferences.

NOT FOR DISCLOSURE:
Restricted to the immediate PSTA participants only
When should it be used? - Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.
How may it be shared? - Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.

LIMITED DISCLOSURE:
Restricted to participants’ organizations
When should it be used? - Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
How may it be shared? - Recipients may only share TLP:AMBER information with Members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. TLP:AMBER+STRICT Restricts sharing to the organization only.

LIMITED DISCLOSURE
Restricted to the community
When should it be used? - Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.
How may it be shared? - Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

DISCLOSURE IS NOT LIMITED
When should it be used? - Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.
How may it be shared? - Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction.

ANNEX I

A. Categories of Data Subjects whose Personal Data may be transferred

Content Material provided by Member and Content Material from Other Sources which will be aggregated may include the Member's or Other Sources representatives and end-users including employees, contractors, collaborators, and customers of the same. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the Public Safety Threat Alliance provided by PSTA. PSTA acknowledges that, depending on Member's use of the Public Safety Threat Alliance, Member may elect to include personal data from any of the following types of data subjects in the Content Materials:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;
- Data exporter's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with Member (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

D. Categories of Personal Data transferred

Through Member's use of the Public Safety Threat Alliance, Member may elect to include personal data from any of the following categories:

- Basic personal data (for example place of birth, street name, and house number (address), Agreemental code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);

- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);

- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);

- Pseudonymous identifiers;

- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);

- Commercial Information (for example history of purchases, special offers, subscription information, payment history);

- Biometric Information (for example DNA, fingerprints and iris scans);

- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);

- Photos, video, and audio;

- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);

- Device identification (for example IMEI-number, SIM card number, MAC address);

- Profiling (for example based on observed criminal or antisocial behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);

- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);

- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);

- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);

- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;

- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose

of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offenses); or

- Any other personal data identified under applicable law or regulation.

ANNEX II

List of Sub-Processors:

Cyware

PUBLIC SAFETY THREAT ALLIANCE ORDERING DOCUMENT

FEES

Please see the pricing summary included below.

Part Number	Description	Annual Price
N/A	Public Safety / Public Sector Membership	$0
SWV00S03680A	PSTA Strategic Partner Membership	$0

A Strategic Partner is any non-Public Safety / Public Sector entitiy