Industry Partnership Agreement (I-PA)

between

the NATO Communications and Information Agency (NCI Agency)

and

XXXXX

On

Cyber Security Information Sharing

Revision No: Original

This Industry Sharing Agreement is entered into on the date of last signature by the Parties (hereinafter, the "**Effective Date**")

between

The NATO Communications and Information Agency ("**NCI Agency**") with headquarters at Boulevard Leopold III, B-1110 Brussels, Belgium;

and

XXXXX ("**XXXXX**"), with its registered office at **[insert address]**;

relating to Cyber Security Information Sharing at the Technical Level.

1. Purpose and scope

1.1. The purpose of this Industry Sharing Agreement (the "**Agreement**") is solely for the Parties to share Information within the voluntary bilateral cyber information sharing programme which allows NATO Industry Partners and NATO to share cyber security Information in order to mutually enhance situational awareness and the protection of their respective networks and systems (the "**Purpose**").

1.2. The scope of this Agreement is to specify the procedures, the information sharing principles, the confidentiality measures to protect the exchanged Information and the points of contact authorised to share Information.

2. Definitions

2.1. Cyber: relating to, or involving computers or computer networks, including automated telecommunications networks, software and data.

2.2. Cyber security: body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access.

2.3. Information: any communications or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms relating to actual or potential cyber security threats or incidents.

2.4. Information system: a discrete set of Information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of Information.

2.5. Originator: the Party releasing Information.

2.6. Parties: the signatories to this Agreement.

2.7. Recipient: the Party receiving Information.

2.8. Threat: any circumstance or event which may potentially have an adverse impact on organisational operations, organisation assets, individuals, other organisations, or larger entities through unauthorised access, destruction, disclosure, modification of Information and/or denial of service as a result of a cyber security incident.

2.9. Traffic Light Protocol or TLP: the Information designation assigned by the Originator which defines the basic use and disclosure obligations for such information.

2.10. Indicator of compromise (IOC) — an artefact observed on a network or in an operating system that with high confidence indicates a computer intrusion. Typical IOCs are: malware signatures, MD5 hashes of malicious files, or IP addresses, URLs or domain names of botnet command and control servers.

3. Information Sharing

The following provisions apply to the sharing of Information under this Agreement.

(1) Voluntary participation

Participation in the Programme is voluntary and does not obligate the Parties to share Information, to utilize Information provided, or to implement any changes to their Information systems. It is up to each Party to decide if and when it discloses Information to the other. Neither Party will incur any legal liability under this Agreement for failure to share, use or implement any Information.

(2) Confidentiality – general rule and marking of Information

(a) The Originator of the Information will determine the level of confidentiality of such Information and the appropriate method of disclosure using the Traffic Light Protocol at Annex A ("Red", "Amber", "Green" and "White"). All information will be marked with the traffic light designation determined by the Originator using the following statement, "***This information is disclosed by _____ and is subject to the terms and conditions, including those related to use and disclosure of information, of the Information Sharing Agreement between NCIA and XXXXX dated [insert date]. It is designated [insert color] pursuant to such Agreement"***. The terms of this Agreement may not be amended or superseded by any legends or statements associated with the Information. Each party will promptly notify the other party in writing of any corrections, changes or revisions of markings or legends to Information. However, no such correction, change or revision will expand the Recipient's rights under this Agreement. In the absence of a marking, the information will be considered as subject to "White" designation per the TLP.

(3) Use only for the "Purpose" and Non-Disclosure Obligations

(a) The Recipient agrees that it will use the Information disclosed to it only for the Purpose as defined above and in accordance with the TLP and other obligations of this Agreement.

(b) Prior to disclosing Information within its organization to employees or contractors, the Recipient shall (i) enter or maintain, with each such employee or contractor, a written agreement sufficient to enable the Recipient to comply with the terms of this Agreement or ensure that they are bound by a duty of confidentialty, and (ii) instruct its employees and contractors to abide by the terms of this Agreement. XXXXX acknowledges that the NCI Agency uses contractors as part of NCIRC Tier 2.

(c) Recipient shall immediately notify Originator in writing of any loss or unauthorized disclosure, reproduction, or access of Information and shall immediately provide a detailed description of the circumstances of the loss, or unauthorized disclosure, reproduction, or access, and the parties involved, to the extent then known.

(4) Non-classified Information

The Information exchange will not include classified Information, i.e. information regulated by law or regulations restricting use and disclosure for security reasons. If, under exceptional circumstances, there is the need to exchange classified Information, it will not be communicated under this Agreement. Arrangements with NATO member Nations for the exchange of classified Information are in place and may be used if XXXXX has the appropriate security clearance to disclose and receive such Information. Points of contact can be made available by the NCI Agency NCIRC TC as and when required.

(5) Ownership, No License Grant

The Originator retains ownership of the Information it provides to the Recipient. Except as otherwise set forth in this Agreement or in a separate written agreement between them, the Parties understand and acknowledge that neither Party grants the other a license under any patents, copyrights, trademarks, inventions, or any other intellectual property in this Agreement or by the disclosure of any Information by the Originator to the Recipient as contemplated hereunder, either expressly, by implication, inducement, estoppel, or otherwise, and that any license under such intellectual property rights must be express and in writing.

(6) Initial incident reporting

Each Party may choose to report cyber incidents to the other if it determines that the incident may be relevant to cyber security activities of the other. The Originator will ensure that such reporting is in line with any applicable law or NATO regulation, as appropriate.

(7) Generic Information

Without disclosing specific Information, each Party may also provide the other with generic non-sensitive Information it has developed concerning the nature, scope, prevention and mitigation of cyber-attacks.

(8) Non attribution

Pursuant to the TLP, the Recipient shall not use or further disclose the Information from the Originator in a manner which attributes it to the Originator, unless expressly permitted by the Originator.

4. Information Sharing Gateways

Only the following Points of Contact are authorised to exchange Information relevant to the Programme:

a. For the NCI Agency:

Mr. Emmanuel Bouillon
NATO Computer Incident Response Capability Technical Centre
NCI Agency
+32 65 44 3668
Emmanuel.Bouillon@ncia.nato.int

Mr. Alex Vandurme
NATO Computer Incident Response Capability Technical Centre
NCI Agency
+32 65 44 2683
Alex.Vandurme@ncia.nato.int

Duty Incident Handling Officer
NATO Computer Incident Response Capability Technical Centre
NCI Agency
dutyiho@ncirc.nato.int

b. For XXXXX:

[insert details]

Generic email address for the analyst on watch:

5. Traffic Light Protocol

(1) The Recipient will handle the Information in line with the Traffic Light Protocol described at Annex A.

(2) Annex A may be modified by the Parties from time to time by an amendment to this Agreement. Any such amendment will require signature by the Parties.

6. General provisions

(1) Participation will not create any competitive advantage or preferential treatment in NATO source selection activities. Participation does not in any way constitute an endorsement by the NCI Agency of XXXXX, its Information systems or products and services.

(2) Information may be retained and used for digital forensics purposes in accordance with applicable law and/or NATO regulations.

(3) Nothing in this Agreement is intended to abrogate the Parties' rights or obligations regarding the handling, safeguarding, sharing, or reporting of Information (whether classified or not), or regarding any physical, personnel, or other security requirements, as required by law, regulation, policy, or a valid legal contractual obligation. It is the Originator's duty to ensure that it has the right to release the Information to the Recipient.

(4) **No Warranty.** All Information is provided by the Originator on an "as is" basis, and the Originator hereby disclaims all representations and warranties on the Information.

(5) **Non-Assignability.** Neither party may assign this Agreement without the prior written consent of the other.

(6) **Entire Agreement.** This Agreement constitutes the entire agreement between the Parties relating to the information disclosed hereunder. This Agreement supersedes and repeals all previous negotiations, representations or understandings between the Parties relating to the information disclosed hereunder. There are no understandings, agreements, or representations, express or implied, related to the information disclosed hereunder not specified herein. This Agreement may not be modified except by mutual agreement in writing.

(7) **Governing Law.** This Agreement shall be governed by the laws of the Kingdom of Belgium.

7. Term and Termination

(1) This Agreement shall be effective for a term of three (3) years from the Effective Date.

(2) Each Party may discontinue participation under this Agreement at any time upon thirty (30) days written notice to the other party. Shared Information cannot be reclaimed.

(3) Termination shall not relieve each Recipient of obligations to protect against the unauthorised use or disclosure of Information exchanged under this Programme. Such obligations of confidentiality shall cease, however, at the latest one year after disclosure by the Originator of the Information.

8. Arbitration

All disputes arising as a result of this Agreement shall be subjected to the dispute resolution procedure as detailed below:

a.) All disputes arising under, or which are related to this Agreement or with respect to its effectiveness shall be resolved by consultation between the Parties. If no agreement can be found, either party may open arbitration proceedings in accordance with the following arbitration provisions.

b.) The party instituting the arbitration proceedings shall advise the other party by registered letter, with official notice of delivery, of his desire to have recourse to arbitration. Within a period of thirty (30) days from the date of receipt of this letter, the parties shall jointly appoint an arbitrator. In the event of failing to appoint an arbitrator, the dispute or disputes shall be submitted to an Arbitration Tribunal consisting of three arbitrators, one being appointed by the NCI Agency, another by XXXXX and the third, who shall act as President of the Tribunal, by these two arbitrators. Should one of the parties fail to appoint an arbitrator during the fifteen (15) days following the expiration of the said first period, the appointment shall be made, within twenty-one (21) days, at the request of the party instituting the proceedings, by the Secretary General of the Permanent Court of Arbitration at The Hague.

c.) Regardless of the procedure concerning the appointment of this Arbitration Tribunal, the third arbitrator will have to be of a nationality different from the nationality of the other two members of the Tribunal. Any arbitrator must be of the nationality of any one of the member states of the NATO and shall be bound by the rules of security in force within NATO.

d.) Any person appearing before the Arbitration Tribunal in the capacity of an expert witness shall, if he is of the nationality of one of the member states of the NATO, be bound by the rules of security in force within NATO; if he is of another nationality, no NATO classified documents or information shall be communicated to him.

e.) An arbitrator, who, for any reason whatsoever, ceases to act as an arbitrator, shall be replaced under the procedure laid down in paragraph d.) above.

f.) The Arbitration Tribunal will take its decisions by a majority vote. It shall decide where it will meet and, unless it decides otherwise, shall follow the arbitration procedures of the International Chamber of Commerce in force at the date of signature of the present Agreement. The awards of the arbitrator or of the Arbitration Tribunal shall be final and there shall be no right of appeal or recourse of any kind. These awards shall determine the appointment of the arbitration expenses.

9. <u>Signatures</u>

For the NCI Agency	For XXXXX
_____	_____
Mr. Koen Gijsbers General Manager NCI Agency	Mr XXX

Annex A – Traffic Light Protocol

1. Marking of Information

1.1 Under the Agreement, the Originator must assign one of the following Traffic Light Protocol marking on every piece of Information provided to the Recipient.

1.2 The Originator shall use one of the following four markings: “Red”, “Amber”, “Green” or “White” when marking Information.

1.3 The specific marking assigned to a piece of Information will determine the release conditions for the information, in line with the description below.

1.4 Information provided by the Originator to the Recipient without any marking will be handled as TLP White.

2. NCIRC Tiers definition

2.1 NCIRC Tier 1 refers to the NCIRC Co-ordination Centre (NCIRC CC) located at NATO Headquarters, Brussels, Belgium.

2.2 NCIRC Tier 2 refers to the NCIRC Technical Centre (NCIRC TC) located in NCIA Agency Mons, Belgium.

2.3 NCIRC Tier 3 refers to the system and network centres / administrators across NATO.

3. Information provided to the NCI Agency

3.1 TLP Red

3.1.1 Release conditions

- TLP Red Information will only be shared within the NCIRC Tier 2 to a limited number of individuals involved in the Cyber Security Operations functions.

- TLP Red Information shall not include actionable information.

- TLP Red Information can be used for the Recipient’s own intelligence and knowledge.

- TLP Red Information cannot be shared with NATO technology providers.

- No TLP Red information will be stored in MISP, even if it contains IoCs.

- TLP Red Information cannot be used directly or indirectly and in any form in reports or notification bulletin without the prior explicit approval of the Originator.

3.1.2 Protection mechanisms

TLP Red Information will be stored in password protected encrypted format, benefiting from the strong security protection profile of internal NATO networks.

3.2 TLP Amber

3.2.1 Release conditions

- Unless associated with a special release marking as defined below, TLP Amber Information will only be shared with NCIRC at Tier 1, Tier 2 and to a small number of selected Tier 3 elements, depending on the context. It will not be shared outside of NATO.

- IOC derived from TLP Amber Information will be stored in MISP as Private Intel (PRIVINT) events marked as “My org only” and hence not shared with any other member of the community like the Nations.

- Additional release conditions – release marking limitations or extensions: in exceptional cases, the Originator may want to further restrict or extend the distribution of TLP Amber Information by adding a release marking that will depict the additional release conditions – this should only be used on an exceptional basis as it requires a non-standard handling of the Information.

- IOCs derived from TLP Amber Information can be used to create security detection and protection rules for NATO’s corporate IT infrastructure without any mention of the origin and context of the Information. The detection and protection rules will be developed by NCIRC Tier 2. The IOCs cannot be passed to technology providers used within NATO infrastructure.

- Isolated elements of TLP Amber Information can be used in reports or notification bulletin without any mention of the origin and context of the Information, with prior consent of the Originator.

3.2.2 Protection mechanisms

TLP Amber information will be stored in its original format, benefiting from the strong security protection profile of internal networks.

3.3 TLP Green

3.3.1 Release conditions

- TLP Green Information will be shared within NATO and NATO nations appropriate liaison officers/agencies.

- IOC derived from TLP Green Information will be stored in MISP marked “our community” and can be shared with other NATO entities and NATO nations.

- IOCs derived from TLP Green Information can be used to create security detection and protection rules for NATO’s corporate IT infrastructure. Their origin and context can be disclosed. The IOCs can be passed to other technology providers used within NATO infrastructure, e.g. subcontractors and service providers.

- TLP Green Information that has been anonymized can be used directly or indirectly and reports or notification bulletin without the prior explicit approval of the Originator.

3.3.2 Protection mechanisms

TLP Green Information will be stored in its original format, benefiting from the security protection profile of internal NATO networks.

3.4 TLP White

3.4.1 Release conditions

- TLP White Information will be shared within NATO and NATO nations appropriate liaison officers/agencies as well as other stakeholders.

- IOC derived from TLP White Information will be stored in MISP marked “All community” and can be shared with other NATO entities and NATO nations as well as other stakeholder.

- IOCs derived from TLP White Information can be used to create security detection and protection rules for NATO’s corporate IT infrastructure. Their origin and context can be disclosed. The IOCs can be passed to other technology providers used within NATO infrastructure.

- TLP White Information can be used directly or indirectly and reports or notification bulletin without the prior explicit approval of the Originator.

3.4.2 Protection mechanisms

No specific protection mechanisms will be applied to TLP White Information.

4. Information provided by the NCI Agency

4.1 TLP Red

4.1.1 Release conditions

- TLP Red Information will only be shared within the Recipient’s organization to a limited number of individuals involved in the Cyber Security Operations, Malware Detection and Analysis, Intelligence, Incident Response and Internal Security functions.

- TLP Red Information shall not include actionable information.

- TLP Red Information can be used for the Recipient’s own intelligence and knowledge.

- IOCs derived from TLP Red Information cannot be passed to any third party such as technology providers or Recipient’s customers.

- TLP Red Information cannot be used directly or indirectly in any form in reports or notification bulletin without the prior explicit approval of the Originator.

4.1.2 Protection mechanisms

TLP Red Information will be stored in password protected encrypted format, benefiting from the strong security protection profile of the Recipient's networks.

4.2 TLP Amber

4.2.1 Release conditions

- Unless associated with a special release marking, TLP Amber Information will only be shared within a limited number of individuals in the Recipient Organization, depending on the context.

- Additional release conditions – release marking limitations or extensions: in exceptional cases, the Originator may want to further restrict or extend the distribution of TLP Amber Information by adding a release marking that will depict the additional release conditions – this should only be used on an exceptional basis as it requires a non-standard handling of the Information.

- IOCs derived from TLP Amber Information can be used for the Recipient's own intelligence and knowledge to create security detection and protection rules for the Recipient's own corporate IT infrastructure without any mention of the origin and context of the Information. IOCs derived from TLP Amber Information cannot be passed to any third party such as technology providers or the Recipient's customers.

- IOCs derived from TLP Amber Information may be used to deploy to endpoints detection mechanisms that identify but do not name or block the threat. Any identification received from the endpoint detection mechanism will remain with the Recipient. The Recipient may share some of the results of its research with NCIRC Tier 2.

- Isolated elements of TLP Amber Information can be used in reports or notification bulletin without any mention of the origin and context of the information, with prior consent of the Originator.

4.2.2 Protection mechanisms

TLP Amber information will be stored in its original format, benefiting from the strong security protection profile of the Recipient's networks.

4.3 TLP Green

4.3.1 Release conditions

- TLP Green Information can be shared within the Recipient's different Communities. For the purpose of this provision, Communities are the following groups or organizations located in NATO countries: (i) information sharing groups between local industry and government; (ii) government CERTs; and (iii) paying XXXXX customers for managed services, e-mail security, security intelligence and incident response.

- IOCs derived from TLP Green Information can be used to create security detection and protection rules for the Recipient's corporate IT infrastructure. Their context can be disclosed but not their origin. The IOCs can be passed to other technology providers used within the Recipient's infrastructure, e.g. subcontractors and service providers.

- IOCs derived from TLP Green Information can be used to publicly release detection and blocking mechanisms and to name the threat.

- TLP Green Information that has been anonymized can be used directly or indirectly in reports or notification bulletin without the prior explicit approval of the Originator.

4.3.2 Protection mechanisms

TLP Green Information will be stored in its original format, benefiting from the security protection profile of the Recipient's networks.

4.4 TLP White

4.4.1 Release conditions

- TLP White Information will be freely sharable within the Recipient Organization.

- IOCs derived from TLP White Information can be used to create security detection and protection rules for the Recipient's corporate IT infrastructure. Their context can be disclosed but not their origin. The IOCs can be passed to other technology providers.

- IOCs derived from TLP White Information can be used to publicly release detection and blocking mechanisms and to name the threat.

- TLP White Information can be used directly or indirectly on reports or notification bulletin without the prior explicit approval of the Originator.

4.4.2 Protection mechanisms

No specific protection mechanisms will be applied to TLP White Information.

5. Exceptions to confidentiality markings

The above restrictive markings (Red, Amber and Green) do not apply to information that the Recipient can prove that:

(a) the Information is now, or hereafter, through no act or failure to act on the part of the Recipient, becomes generally known or available to the public without breach of this Agreement;

(b) the Information is known to the Recipient at the time of disclosure of such information or is developed by the Recipient independently of such disclosure; or

(c) the Information is hereafter received by the Recipient by a third party without that third party being in breach directly or indirectly of an obligation to the Originator to keep the information confidential.

*

***