Data Processing Addendum

This Data Processing Addendum (“DPA”) is entered into as of the date of the License and Service Agreement and is made by and between Customer (“Data Controller” and “Data Exporter”) and QOMPLX, Inc. (“QOMPLX”) (a “Data Processor” and “Data Importer”). The Data Controller and the Data Processor are collectively referred to as the “Parties”.

WHEREAS this DPA is entered into to provide adequate safeguards with respect to the protection of Personal Data (as defined below) passed from the Data Controller to the Data Processor on the authority of the Data Controller for processing of such Personal Data by the Data Processor in connection with the provision of Services (as defined below),

NOW THEREFORE, the parties agree as follows:

1. General
   a. The above and foregoing recitals are true and correct and are incorporated herein by references.
   b. Any capitalized terms used in this DPA and not otherwise defined in this DPA shall have the same meanings such terms are given in the License and Services Agreement between the parties (“Agreement”).
   c. This DPA shall be subject to the terms and conditions of the Services Agreement. To the extent this DPA, only as it relates to the processing of Personal Data, is inconsistent with the terms of the Services Agreement, this DPA shall govern. All terms of the Services Agreement remain in full force and effect.

2. Subject Matter of this DPA
   a. This DPA applies exclusively to the following: (i) processing of Personal Data by Data Processor on behalf of Data Controller that is subject to Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data repealing Directive 95/46/EC, the General Data Protection Regulation (“GDPR”), and any laws passed by the member states of the European Union to implement GDPR (“EU Data Protection Law”) in connection with the Services under the Agreement; and (ii) the collection, use, retention, or disclosure of Personal Data by Data Processor on behalf of Data Controller that is subject to the California Consumer Privacy Act of 2018, as amended, Cal. Civ. Code §§ 1798.100-199 (the “CCPA”), in connection with the Services under the Agreement.
   b. The terms “Personal Data” (subject to the further clarification by the Data Processor on its processing of IP addresses set out in the Data Processor's documentation relating to its data collection, storage and use), “personal
data breach”, “processing”, “process”, “Data Controller” and “Data Processor” shall have the meanings ascribed to them in the EU Data Protection Law.

c. Insofar as the Data Processor will be processing Personal Data subject to EU Data Protection Law or the CCPA on behalf of the Data Controller in the course of performing the Services under the Agreement, the terms of this DPA shall apply.

d. Processing of Personal Data by the Data Processor under this DPA shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in Schedule 2 of this DPA.

3. **The Data Controller and the Data Processor**

   a. The Data Controller will determine the scope, purposes, and manner by which the Personal Data may be accessed or processed by the Data Processor. The Data Processor will process the Personal Data in accordance with the terms and conditions of the Agreement, this DPA, and any other written instructions from the Data Controller to which the Data Processor has agreed. The Data Processor will limit Personal Data collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the contracted business purposes.

   b. The Data Processor will only process the Personal Data on documented instructions of the Data Controller in such manner as, and to the extent that, is necessary for the provision of Services, except as may be otherwise required for compliance with applicable laws, including, but not limited to, EU Data Protection Law and the CCPA, save that the Data Processor may process Personal Data in aggregated or anonymised form to evaluate the effectiveness of or means of improving its products and services. The Data Processor shall immediately inform the Data Controller if, in its opinion, an instruction from the Data Controller violates EU Data Protection Law or the CCPA.

   c. The Data Processor will not collect, use, retain, disclose or otherwise make Personal Data available for its own commercial purposes or in a way that does not comply with the CCPA. The Data Processor will not sell the Personal Data.

   d. The Data Processor will promptly comply with any Data Controller request or instruction requiring Data Processor to provide, amend, transfer, or delete the Personal Data, or to stop, mitigate, or remedy any unauthorized processing.

   e. The Data Controller represents and warrants that it has all necessary rights to provide the Personal Data to Data Processor for the processing to be performed in relation to the Services. To the extent required, Data Controller is responsible for ensuring that any necessary data subject consents to the
processing of Personal Data by Data Processor are obtained and for ensuring that a record of such consents is maintained by the Data Controller.

f. If the contracted business purposes of the Agreement require the collection of Personal Data from individuals on Data Controller's behalf, Data Processor will, with regard to any Personal Data collected from residents of California, provide a CCPA-compliant, Data Controller-approved notice addressing use and collection methods.

g. The Data Processor shall provide that all persons authorized to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

h. Both Parties will comply with all applicable requirements of the CCPA when collecting, using, retaining, or disclosing personal information collected from residents of California.

4. **Security**

a. Taking into account generally accepted industry standards, the costs of implementation, and the nature, scope, context, and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Data Controller and Data Processor shall implement reasonably appropriate technical and organizational measures to ensure a level of security of processing of Personal Data appropriate to the risk. These measures shall include as appropriate:

   i. Measures to ensure that Personal Data can be accessed only by authorized personnel for the purposes of providing the Services;

   ii. In assessing the appropriate level of security, shall account for the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personal Data transmitted, stored, or otherwise processed;

   iii. The pseudonymization and encryption of Personal Data;

   iv. The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

   v. The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

   vi. Measures to identify vulnerabilities with regard to the processing of Personal Data in systems used to provide Services to the Data Controller;

b. At the request of the Data Controller, the Data Processor shall demonstrate the measures it has taken pursuant to this Section 4 and shall allow the Data Controller to audit such measures no more than once annually, with
reasonable notice to the Data Processor and at the Data Controller’s own cost. The Data Processor shall provide reasonable assistance to the Data Controller with respect to such audits.

5. **Data Transfers**

a. The Parties agree that the Processing of Personal Data by the Data Processor (or its sub-processors) may take place in any country outside of the European Economic Area (“EEA”). The Parties agree that where Processing takes place in connection with the provision of Services under the Agreement the standard contractual clauses approved by the EU authorities under EU Data Protection Laws at Schedule 3 of this DPA apply in respect of that Processing.

b. The Data Processor agrees to enter into the standard contractual clauses referenced at 5a. with any sub-processor which it appoints to Process Personal Data in connection with the provision of Services by the Data Processor (and that in such circumstances it will be the data controller and the sub-processor will be the data processor).

6. **Information Obligations and Incident Management**

a. The Data Processor shall notify the Data Controller promptly of becoming aware of a personal data breach involving Data Controller Personal Data and provide the Data Controller with information relevant to reasonably assist the Data Controller with its own notification obligations as applicable to Data Controller under EU Data Protection Law which may include the following: (i) a description of the nature of the personal data breach; (ii) the categories and approximate number of data subjects impacted; (iii) a description of the measures taken or proposed to be taken by the Data Processor to address the personal data breach.

7. **Sub-processors**

a. The Data Controller authorizes the Data Processor to utilize sub-processors to process Personal Data, provided that such sub-processors enter into written terms consistent with the terms of this DPA. As of the Effective Date of this DPA, Data Processor’s current sub-processors are those listed in Schedule 1 to this DPA attached hereto and incorporated herein. The Data Processor shall inform the Data Controller of any intended changes concerning the addition or replacement of sub-processors, thereby giving the Data Controller the opportunity to object to such changes.

8. **Return or Destruction of Personal Data**

a. Upon termination of the Agreement, and provided there is no applicable retention requirement in place to the contrary, the Data Processor shall, at the election of the Data Controller, either delete, destroy, or return all Personal Data of the Data Controller.
9. **Assistance to Data Controller**

   a. The Data Processor shall, taking into account the nature of the processing, assist the Data Controller by reasonably appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Data Controller's obligation to respond to request for exercising the data subject’s rights, if any, under GDPR and the CCPA.

   b. The Data Processor must notify the Data Controller immediately if the Data Processor receives any complaint, notice, or communication that directly or indirectly relates to either Party’s compliance with the CCPA. Specifically, the Data Processor must notify the Data Controller within five (5) working days if the Data Processor receives a verifiable consumer request under the CCPA.
Schedule 1
Sub-processors

AWS
Schedule 2
Data Processing Details

Processing of the Personal Data by the Data Processor under this DPA shall be for the subject-matter, duration, nature, and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Schedule 2. The Data Controller is responsible for providing to the Data Processor the following information.

1. **Subject-matter of processing:**

   Provision of CMMC Pre-assessment services

2. **Duration of the processing:**

   QOMPLX retains processed information for three years, unless Customer specifies a different retention period in its Master Service and License Agreement or in Statements of Work.

3. **Nature and purpose of the processing:**

   The CMMC Pre-assessment service assists customers in documenting their conformance with the United States Department of Defense’s Cybersecurity Maturity Model Certification (“CMMC”). It combines customer-supplied survey answers with information connected by QOMPLX’s Scan product. Scan analyzes publicly information to identify an organization’s weaknesses and exposures, using either an internet domain or D-U-N-S® number to identify the target organization. The results of the customer-supplied survey responses are combined with Scan data to generate a final score.

4. **Type of Personal Data:**

   Identifiers: email address of the individual registering the account; email Addresses related to the domain; names of High-Value Personnel and Management Team members (when collected on a discretionary basis)

5. **Categories of Data Subjects:**

   Customers

6. **Specific processing instructions:**

   Information to be used only for CMMC Pre-assessment services
Schedule 3
Data Transfer Agreement
for Transfers of Personal Data from the EU to Countries Outside of the EU

DATED as of the date indicated on page 3 of the Data Processing addendum above

DATA EXPORTERS

AND

DATA IMPORTERS

DATA TRANSFER AGREEMENT
TABLE OF CONTENTS

1. DEFINITIONS AND INTERPRETATION ................................................................. 11
2. OBLIGATIONS OF THE DATA EXPORTER ...................................................... 12
3. OBLIGATIONS OF THE DATA IMPORTER ..................................................... 12
4. LIABILITY AND THIRD-PARTY RIGHTS ....................................................... 14
5. LAW APPLICABLE TO THE CLAUSES .......................................................... 14
6. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE AUTHORITY ..... 14
7. TERMINATION .................................................................................................. 15
8. VARIATION OF THE CLAUSES .................................................................... 16
9. DESCRIPTION OF THE TRANSFER ............................................................... 16
10. DURATION OF THIS AGREEMENT ............................................................... 16
11. VARIATION OF THIS AGREEMENT ............................................................. 17
12. GOVERNING LAW .......................................................................................... 17

DATA EXPORTERS .............................................................................................. 17

APPENDIX 2 ....................................................................................................... 18

DATA IMPORTERS .............................................................................................. 18

APPENDIX 3 ....................................................................................................... 19

DATA PROCESSING PRINCIPLES ..................................................................... 19

DESCRIPTION OF THE TRANSFER .................................................................. 21
THIS AGREEMENT is made on the date indicated on page 3 of the Data Processing addendum above.

BETWEEN:

(1) The Data Exporter indicated on page 3 of the Data Processing addendum above DATA EXPORTERS, whose names and particulars are set out in Appendix 3 (each such company a “Data Exporter”);

QOMPLX, Inc. and its affiliates and subsidiaries DATA IMPORTERS, whose names and particulars are set out in Appendix 2 (each such company a “Data Importer”),

Each a “Party”; together “Parties”.

IT IS AGREED as follows:

(A) The Parties transfer personal data of its customers, clients, officers and employees to each other from time to time to facilitate their business activities.

(B) Chapter V, Articles 44-50 of General Data Protection Regulation (EU 2016/479) of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (“GDPR”) regulate the transfer of personal data to countries outside the European Economic Area (“EEA”). GDPR applies to transfers of personal data from each European Union member state and, in addition, from each EEA member state.

(C) GDPR permits the transfer of personal data to countries outside the EEA where there are adequate safeguards in place to protect the personal data.

(D) The Parties wish to enter into this Agreement to safeguard personal data that may be transferred by any Data Exporter to any Data Importer using the standard contractual clauses for the transfer of personal data to countries outside the EEA under GDPR.
1. DEFINITIONS AND INTERPRETATION

1.1. In this Agreement:

**Clauses** means the standard contractual clauses for the transfer of personal data to third countries outside the EEA adopted by the European Commission pursuant to Commission Decision 2004/915/EC amending Decision 2001/497/EC on 27 December 2004 and set out in clauses 1.3 to 9 of this Agreement;

**Commencement Date** means the date of this Agreement;

**Control** (and **Controlled**) shall be construed accordingly) means owning, directly or indirectly, more than fifty percent (50%) the assets or the outstanding shares having voting rights, or otherwise having the right, either by contract or otherwise, to direct the operation, management or policy of such entity

**EEA** is defined in Recital B;

**GDPR** is defined in Recital B;

**Group Companies** means any holding company and each and any subsidiaries from time to time (and **Group** and **Group Company** shall be construed accordingly); and

**Relevant Transfer** means a transfer of personal data outside the EEA.

1.2. Specific references in the Clauses to a “**Data Exporter**”, a “**Data Importer**” or to “**Parties**” shall, where used in the Clauses, be interpreted as references to the relevant Group Company that is either the Data Exporter or the Data Importer (as the case may be) in respect of which a Relevant Transfer is made and together such two Group Companies shall be the construed as the “**Parties**” for the purposes of the Clauses.

1.3. For the purposes of the Clauses:

1.3.1. **personal data**, **special categories of data/sensitive data**, **process/processing**, **controller**, **processor**, **data subject** and **supervisory authority/authority** shall have the same meaning as in GDPR (whereby “**the Authority**” shall mean the competent data protection authority in the territory in which the Data Exporter is established);

1.3.2. the **Data Exporter** shall mean the controller who transfers the personal data; and

1.3.3. the **Data Importer** shall mean the controller who agrees to receive from the Data Exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection.
1.4. The details of the transfer (as well as the personal data covered) are specified in Appendix 3, which forms an integral part of the Clauses.

2. OBLIGATIONS OF THE DATA EXPORTER

The Data Exporter warrants and undertakes that:

(a) the personal data have been collected, processed and transferred in accordance with the laws applicable to the Data Exporter;

(b) it has used reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these Clauses;

(c) it will provide the Data Importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the Data Exporter is established;

(d) it will respond to enquiries from data subjects and the Authority concerning processing of the personal data by the Data Importer, unless the Parties have agreed that the Data Importer will so respond, in which case the Data Exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the Data Importer is unwilling or unable to respond. Responses will be made within a reasonable time; and

(e) it will make available, upon request, a copy of the Clauses to data subjects who are third party beneficiaries under Clause 4, unless the Clauses contain confidential information, in which case it may remove such information. Where information is removed, the Data Exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the Authority. However, the Data Exporter shall abide by a decision of the Authority regarding access to the full text of the Clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The Data Exporter shall also provide a copy of the Clauses to the Authority where required.

3. OBLIGATIONS OF THE DATA IMPORTER

The Data Importer warrants and undertakes that:

(a) it will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected;

(b) it will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the Data Importer, including a data processor, shall be obligated to process the personal data only on instructions from the Data Importer. This
provision does not apply to persons authorised or required by law or regulation to have access to the personal data;

(c) it has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these Clauses, and it will inform the Data Exporter (which will pass such notification on to the Authority where required) if it becomes aware of any such laws;

(d) it will process the personal data for purposes described in Appendix 3, and has the legal authority to give the warranties and fulfil the undertakings set out in these Clauses.

(e) it will identify to the Data Exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the Data Exporter, the data subject and the Authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the Data Exporter, or if the Parties have so agreed, the Data Importer will assume responsibility for compliance with the provisions of Clause 2(e);

(f) at the request of the Data Exporter, it will provide the Data Exporter with evidence of financial resources sufficient to fulfil its responsibilities under Clause 4 (which may include insurance coverage);

(g) upon reasonable request of the Data Exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the Data Exporter (or any independent or impartial inspection agents or auditors, selected by the Data Exporter and not reasonably objected to by the Data Importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the Data Importer, which consent or approval the Data Importer will attempt to obtain in a timely fashion.

(h) it will process the personal data in accordance with the data processing principles set forth; and

(i) it will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the Data Exporter about the transfer and:

(i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection; or

(ii) the third party data controller becomes a signatory to these Clauses or another data transfer agreement approved by a competent authority in the EU; or

(iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and
the fact that the countries to which data is exported may have different data protection standards, or

(iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

4. LIABILITY AND THIRD-PARTY RIGHTS

4.1. Each Party shall be liable to the other Party for damages it causes by any breach of these Clauses. Liability as between the Parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each Party shall be liable to data subjects for damages it causes by any breach of third-party rights under these Clauses. This does not affect the liability of the Data Exporter under its data protection law.

4.2. The Parties agree that a data subject shall have the right to enforce as a third party beneficiary this Clause and Clause 2(b), Clause 2(d), Clause 2(e), Clause 3(a), Clause 3(c), Clause 3(d), Clause 3(e), Clause 3(g), Clause 3(i), Clause 4.1, Clause 6, Clause 7.4 and Clause 8 against the Data Importer or the Data Exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the Data Exporter's country of establishment. In cases involving allegations of breach by the Data Importer, the data subject must first request the Data Exporter to take appropriate action to enforce his rights against the Data Importer; if the Data Exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the Data Importer directly. A data subject is entitled to proceed directly against a Data Exporter that has failed to use reasonable efforts to determine that the Data Importer is able to satisfy its legal obligations under these clauses (the Data Exporter shall have the burden to prove that it took reasonable efforts).

5. LAW APPLICABLE TO THE CLAUSES

These Clauses shall be governed by the law of the country in which the Data Exporter is established.

6. RESOLUTION OF DISPUTES WITH DATA SUBJECTS OR THE AUTHORITY

6.1. In the event of a dispute or claim brought by a data subject or the Authority concerning the processing of the personal data against either or both of the Parties, the Parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

6.2. The Parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Authority. If they do participate in the proceedings, the Parties may elect to do so remotely (such as by telephone or other electronic means). The Parties also agree to consider participating in any other
arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

6.3. Each Party shall abide by a decision of a competent court of the Data Exporter’s country of establishment or of the Authority which is final and against which no further appeal is possible.

7. **TERMINATION**

7.1. In the event that the Data Importer is in breach of its obligations under these Clauses, then the Data Exporter may temporarily suspend the transfer of personal data to the Data Importer until the breach is repaired or the contract is terminated.

7.2. In the event that:

(i) the transfer of personal data to the Data Importer has been temporarily suspended by the Data Exporter for longer than one month pursuant to Clause 7.1;

(ii) compliance by the Data Importer with these Clauses would put it in breach of its legal or regulatory obligations in the country of import;

(iii) the Data Importer is in substantial or persistent breach of any warranties or undertakings given by it under these Clauses;

(iv) a final decision against which no further appeal is possible of a competent court of the Data Exporter’s country of establishment or of the authority rules that there has been a breach of the Clauses by the Data Importer or the Data Exporter; or

(v) a petition is presented for the administration or winding up of the Data Importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the Data Importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the Data Exporter, without prejudice to any other rights which it may have against the Data Importer, shall be entitled to terminate these Clauses, in which case the Authority shall be informed where required. In cases covered by Clause 7.2(i), Clause 7.2(ii), or Clause 7.2(iv) above the Data Importer may also terminate these Clauses.

7.3. Either Party may terminate these Clauses if:

(a) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the Data Importer, or
(b) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

7.4. The Parties agree that the termination of these Clauses at any time, in any circumstances and for whatever reason (except for termination under Clause 7.3) does not exempt them from the obligations and/or conditions under the Clauses as regards the processing of the personal data transferred.

8. VARIATION OF THE CLAUSES

The Parties may not modify these Clauses except to update any information in Appendix 3, in which case they will inform the Authority where required. This does not preclude the Parties from adding additional commercial clauses where required.

9. DESCRIPTION OF THE TRANSFER

The details of the transfer and of the personal data are specified in Appendix 3. The Parties agree that Appendix 3 may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under Clause 2(e). The Parties may execute additional annexes to cover additional transfers, which will be submitted to the Authority where required. Appendix 3 may, in the alternative, be drafted to cover multiple transfers.

10. DURATION OF THIS AGREEMENT

10.1. This Agreement shall take effect on and from the Commencement Date and shall continue in full force and effect until terminated in accordance with this Clause 10.

10.2. This Agreement shall terminate:

(a) with respect to the relevant Data Exporter or Data Importer (as the case may be), upon written notice from the relevant Data Exporter or Data Importer (as the case may be) to the relevant Data Exporter or Data Importer (as the case may be) in the circumstances set out in Clauses 7.2 and 7.3; and

(b) with respect to any Party, without any requirement to give notice, upon such Party ceasing to be a Group Company.

10.3. If the Agreement terminates with respect to any Party pursuant to Clause 10.2, subject to Clause, a Party’s further rights and obligations cease immediately on such termination except that termination does not affect a Party’s accrued rights and obligations at the date of termination.
10.4. In the event of termination of this Agreement or the Clauses pursuant to Clauses 10.2 or 10.3 with respect to any Party that is a Data Importer, such Data Importer must return all personal data and all copies of the personal data subject to the Clauses to the data exporter forthwith or, at the Data Exporter’s choice, will destroy all copies of the same and certify to the Data Exporter that it has done so, unless the Data Importer is prevented by its national law or local regulator from destroying or returning all or part of such data, in which event the data will be kept confidential and will not be actively processed for any purpose. The Data Importer agrees that, if so requested by the Data Exporter, it will allow the Data Exporter, or an inspection agent selected by the Data Exporter and not reasonably objected to by the Data Importer, access to its establishment to verify that this has been done, with reasonable notice and during business hours.

11. VARIATION OF THIS AGREEMENT

Without prejudice to Clause 8, any provision of this Agreement other than the Clauses may be deleted, varied, supplemented, restated or otherwise changed in any way at any time, in which case such change shall be binding against all Parties hereto.

12. GOVERNING LAW

Without prejudice to Clause 5, this Agreement is otherwise governed by and shall be construed in accordance with English law.

APPENDIX 1

DATA EXPORTERS

<table>
<thead>
<tr>
<th>Name</th>
<th>Place of Incorporation</th>
<th>Federal Employer Identification Number (FEIN) or Company Number</th>
<th>Principal place of business/ Registered Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>Per D&amp;B record</td>
<td>Per D&amp;B record</td>
<td>Per D&amp;B record</td>
<td>Per D&amp;B record</td>
</tr>
</tbody>
</table>
## APPENDIX 2

### DATA IMPORTERS

<table>
<thead>
<tr>
<th>Name</th>
<th>Place of Incorporation</th>
<th>Company Number or Federal Employer Identification Number</th>
<th>Registered Office / Principal place of business</th>
</tr>
</thead>
<tbody>
<tr>
<td>QOMPLX, Inc.</td>
<td>Delaware, USA</td>
<td>47-4091518</td>
<td>1775 Tysons Blvd, Suite 800, Tysons, VA 22102-4284</td>
</tr>
<tr>
<td>QOMPLX Government Solutions, LLC</td>
<td>Delaware, USA</td>
<td>84-3675432</td>
<td>1775 Tysons Blvd, Suite 800, Tysons, VA 22102-4284</td>
</tr>
</tbody>
</table>
APPENDIX 3

DATA PROCESSING PRINCIPLES

1. PURPOSE LIMITATION

Personal data may be processed and subsequently used or further communicated only for purposes described in Appendix 3 or subsequently authorized by the data subject.

2. DATA QUALITY AND PROPORTIONALITY

Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3. TRANSPARENCY

Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the Data Exporter.

4. SECURITY AND CONFIDENTIALITY

Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5. RIGHTS OF ACCESS, RECTIFICATION, DELETION AND OBJECTION

As provided in Article 15 of GDPR, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the Data Exporter. Provided that the Authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the Data Importer or other organisations dealing with the Data Importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the
organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the Data Importer, and the data subject may always challenge a refusal before the Authority.

6. **SENSITIVE DATA**

The Data Importer shall take such additional measures (e.g., relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause 2.

7. **DATA USED FOR MARKETING PURPOSES**

Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.

8. **AUTOMATED DECISIONS**

For purposes hereof “automated decision” shall mean a decision by the Data Exporter or the Data Importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The Data Importer shall not make any automated decisions concerning data subjects, except when:

(a) such decisions are made by the Data Importer in entering into or performing a contract with the data subject; and

(b) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that party.

or

(c) where otherwise provided by the law of the Data Exporter.
APPENDIX 4

DESCRIPTION OF THE TRANSFER

Data subjects

Identifiers: email address of the individual registering the account; email Addresses related to the domain; names of High-Value Personnel and Management Team members (when collected on a discretionary basis)

Purposes of the transfer(s)

Provision of CMMC Pre-assessment services

Categories of data

Employees

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

1. Data Importers;
2. Data processors of the data importer, subject to the terms of this agreement and applicable law;
3. Dun and Bradstreet Corporation

The contact point for all data protection enquiries relating to any group Company is:

Contact Name: Andy Jaquith
Company: QOMPLX, Inc.
Position: CISO
Email: andy.jaquith@qomplx.com
Telephone: 703.995.4199 ext. 712