Platform Agreement

Attachment 2 I Version 2.2 I Terms of Access

THIS PLATFORM AGREEMENT (this "**Agreement**") governs access to and use of the Intelligence Community Data Consortium ("ICDC") Platform.

ACCEPTANCE BY USE. By accessing or using the Platform, each user ("User") acknowledges and agrees to comply with the terms of this Agreement. No signature is required; access constitutes acknowledgment as of the date of first use (the "Effective Date"). This acknowledgment constitutes a User-level acceptance of obligations established under the applicable governing agreements and does not create independent contractual obligations on behalf of the User's organization or the United States Government. Users who do not agree must not access the Platform. Users accepting on behalf of an organization represent they will comply with the terms applicable to their role. 10xNatSec logs all acceptance events for audit purposes.

This Agreement is subordinate to the MDVA. Where a conflict exists between this Agreement and the MDVA, the MDVA shall govern, unless this Agreement expressly identifies the specific Section of the MDVA that it supersedes

WHEREAS, 10xNatSec serves as the sole consortium manager of ICDC, providing a marketplace platform (the "Platform") through which Government Customers license Vendor Data and Vendors manage their listings of Vendor Data offerings.

1. Integration. 10xNatSec will provision Government Customers with accounts, which are only fully accessible upon the Government Customer's acceptance of this Agreement. Upon acceptance and execution of the relevant Order Form with Data Vendor, 10xNatSec will (a) provide the Government Customer access to the 10xNatSec Portal and related documentation, for the sole purpose of enabling the Government Customer's access to relevant licensed Vendor Data in accordance with this Agreement and the MDVA, and (b) use commercially reasonable efforts to integrate the 10xNatSec API into the Government Customer's systems.

2. Vendor Data and Data Rights.

2.1 Ownership. All Vendor Data is and remains the sole and exclusive property of the applicable Vendor (MDVA Section 6). 10xNatSec is not responsible for the accuracy or completeness of Vendor Data. Vendor Data is provided on an "as-is" basis as to data quality (MDVA Section 8.4). The as-is warranty does not extend to IT performance, availability, or uptime of the Platform, which are governed by the Service Level Agreement (MDVA Schedule C).

2.2 Government Purpose Rights. The Government Customer is granted Government Purpose Rights in Vendor Data licensed through the Platform, as defined in MDVA Section 5.8. Government Purpose Rights means the right to use, modify, reproduce, release, perform, display, and disclose Vendor Data specifically as detailed in the Vendor-EULA (Schedule E to MDVA). Government purposes do not include the right to use, modify, reproduce, release, perform, display, or disclose Vendor Data for commercial purposes or to authorize others to do so. Government Purpose Rights include, but are not limited to: (a) incorporating Vendor Data into government reports, briefings, assessments, analyses, and publications; (b) combining Vendor Data with other data sources to create derivative analyses for government use; (c) sharing derivative works across government agencies for government purposes; and (d) citing and referencing Vendor Data provided such citation or reference does not compromise operational security. Government Purpose Rights do not transfer ownership of Vendor Data.

2.3 Restrictions. The Government Customer shall comply with: (i) all restrictions pursuant to applicable law; (ii) Vendor Data usage rights as detailed in the relevant Order Form under the MDVA and Vendor-EULA; (iii) the Government Purpose Rights framework (MDVA Section 5.8); and (iv) this Agreement. Government Purpose Rights do not grant the right to disclose Vendor Data to the public or to commercial entities for non-governmental purposes or to those other than permitted Authorized Users.

3. Downstream Users. A Government Customer may authorize Downstream Users (MDVA Section 1.7) to benefit from Vendor Data, provided that: (a) the Government Customer has satisfied its payment obligations under an active purchase order; (b) Downstream Users and their scope of access are enumerated in the applicable Order Form and agreed to by Vendor; (c) the Government Customer remains responsible for its Downstream Users' acts and omissions; and (d) each Downstream User accepts the Vendor-EULA (Schedule E to MDVA) prior to first access. No Downstream User may access Vendor Data unless the conditions in MDVA Section 2A.4 (No Free Riding) have been satisfied.

3.1 Restrictions on Use of Platform. The Government Customer shall not (and shall not authorize any third party to): (i) allow anyone other than Authorized Users to use the Platform; (ii) reverse engineer, decompile, or disassemble the Platform; (iii) modify, adapt, or translate the Platform; (iv) copy the Platform except as permitted; (v) resell, distribute, or sublicense the Platform; (vi) remove proprietary markings; (vii) use the Platform in violation of Applicable Law or to build a competitive product; (viii) use the Platform for the benefit of a third party via service bureau or similar activity; or (ix) circumvent security measures.

3.2 Restrictions on use of Vendor Data. The restrictions for the use of Vendor Data by Government Customer and Downstream Users shall be as detailed on Section 2 of the Vendor-EULA (Schedule E to MDVA).

4. Data Protection and Government Customer Data Handling Obligations.

4.1 Security Safeguards. The Parties will employ industry-standard safeguards to secure Vendor Data. The Government Customer shall limit access to Authorized Users and Downstream Users permitted under the relevant Order Form, and shall not process Vendor Data in any manner that violates this Agreement, Vendor Data Limits, the Vendor-EULA (Schedule E to the MDVA) or Applicable Law.

4.2 Independent Controller Obligations. For purposes of Applicable Data Protection Laws (DPA, Attachment 3), the Government Customer shall act as an independent Controller for its own processing of Personal Data. The Government Customer shall: (a) comply with all Applicable Data Protection Laws; (b) implement appropriate security measures; (c) restrict onward disclosure; and (d) cooperate with 10xNatSec on Data Subject Rights requests.

4.3 Security Breach Notification. The Government Customer must notify 10xNatSec and any affected Vendor(s) within forty-eight (48) hours of discovering any unauthorized access, disclosure, or use of Vendor Data and shall cooperate with efforts to investigate, mitigate, remediate, and report on the incident. This forty-eight (48) hour standard is the controlling notification deadline under this Agreement; where the incident involves Personal Data, notice given in accordance with this Section shall also satisfy the corresponding notification obligation under the DPA (Attachment 3).

4.4 Scope of Data Protection Agreement. Personal Data may be contained within Vendor Data notwithstanding any general exclusion stated in the DPA (Attachment 3). The protections and obligations set forth in the DPA shall apply whenever a specific Order Form, Vendor-EULA, or Vendor Data product identifies that Personal Data is contained within the applicable Vendor Data, consistent with MDVA Section 5.9.

5. End User License Agreement. Each Authorized User, Downstream User and Vendor shall accept the EULA (Attachment 1) prior to first access. The Government Customer shall ensure all personnel accessing or interacting within the Platform have accepted the EULA.

6. Financial Terms. All payments are due as set forth in the applicable Purchase Order and administered exclusively by 10xNatSec (MDVA Section 10). The Government Customer's financial obligations are limited to the costs identified in the applicable Purchase Order and are subject to the appropriated funds identified through the data access and purchase request processes. Payment Terms applicable between 10XNatSec and Vendor shall be as detailed within the Purchase Order.

7. Confidentiality; Intellectual Property. Each Party will maintain the confidentiality of non-public information and will not use or disclose it except in connection with this Agreement. 10xNatSec retains all IP rights to the Platform. The Government Customer's rights in Vendor Data are limited to Government Purpose Rights (Section 2.2, MDVA Section 5.8) and Vendor retains all IP rights to the Vendor Data.

8. Term. This Agreement is effective as of the date of the Government Customer's first access to the Platform following acceptance and continues for the period specified in the applicable Purchase Order. Each Order Form shall detail licensing of the Vendor Data to a specific Government Customer and shall include all details as set forth in the Order Form (as incorporated into the MDVA). Each subscription period shall have specific funding and ending dates. This Agreement shall not automatically renew, and this no-automatic-renewal rule controls notwithstanding any renewal mechanism described in any Order Form template or MDVA Schedule. Any continuation of access beyond the expiration of a Subscription Term requires a new Order Form with identified funding and a defined term.

9. Termination. Either Party may terminate upon thirty (30) business days' written notice for uncured material breach. Upon termination, 10xNatSec will disable access. Surviving provisions: Sections 2, 4, 5, 7, 8, 11, 12, 13, 14, and 15.

10. Disclaimers. THE PLATFORM, THE 10XNATSEC API, AND ALL VENDOR DATA ARE PROVIDED "AS IS" AND "AS AVAILABLE." THE AS-IS WARRANTY PERTAINS SOLELY TO DATA QUALITY AND DOES NOT EXTEND TO IT PERFORMANCE (GOVERNED BY THE SLA, MDVA SCHEDULE C). EACH PARTY DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER 10XNATSEC NOR ANY VENDOR IS RESPONSIBLE FOR DECISIONS MADE BASED ON PLATFORM OUTPUT.

11. Liability. THIS SECTION 11 GOVERNS LIABILITY AS BETWEEN 10XNATSEC AND THE GOVERNMENT CUSTOMER AND SUPERSEDES MDVA SECTION 9 SOLELY AS TO CLAIMS BETWEEN 10XNATSEC AND THE GOVERNMENT CUSTOMER.EXCEPT FOR FRAUD, WILLFUL MISCONDUCT, OR A KNOWING AND MATERIAL BREACH OF THE SECURITY SAFEGUARDS OBLIGATIONS IN SECTION 4.1, THE CONFIDENTIALITY OBLIGATIONS IN SECTION 7, OR THE GOVERNMENT PURPOSE RIGHTS RESTRICTIONS IN SECTION 2.2: (I) NEITHER PARTY WILL BE LIABLE FOR INCIDENTAL, SPECIAL, PUNITIVE, EXEMPLARY, INDIRECT, OR CONSEQUENTIAL DAMAGES; AND (II) 10XNATSEC'S AGGREGATE LIABILITY WILL NOT EXCEED FEES PAID DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM.

12. Indemnification; Sovereign Immunity.

12.1 No Indemnification. As between 10xNatSec and the Government Customer, no

Party shall have any obligation to indemnify, defend, or hold harmless any other Party under this Agreement, and each such Party bears sole responsibility for its own acts, omissions, breaches, and legal obligations arising out of its performance under this Agreement. This Section 12.1 applies solely as between 10xNatSec and the Government Customer and does not limit, discharge, or otherwise affect 10xNatSec's separate indemnifications obligations to Vendor under MDVA Section 10.3. Notwithstanding the foregoing, where 10xNatSec makes a payment to a Vendor under MDVA Section 10.3 that is directly attributable to a specific Government Customer's, or its Downstream User's, unauthorized use or misuse of Vendor Data or other unauthorized conduct, 10xNatSec shall have a right of reimbursement or contribution from that Government Customer for such payment, to the extent consistent with the Anti-Deficiency Act and subject to the availability of appropriated funds. This narrow reimbursement right is limited to conduct attributable to the responsible Government Customer and does not create any general indemnification obligation inconsistent with the first sentence of this Section 12.1

12.2 Sovereign Immunity. Nothing in this Agreement constitutes a waiver of the sovereign immunity of the United States or any agency thereof. Consistent with MDVA Section 10.4, no term of this Agreement shall be interpreted to subject the U.S. Federal Government or any Government Customer to liability beyond that which is expressly authorized by applicable federal law.

13. Feedback and Usage Reporting. In relation to Vendor Data licensed to Government Customers under an Order Form, at the Government's discretion, qualitative feedback of data and product usage may be provided to Vendors, subject to applicable public release procedures (MDVA Section 5.10). The Government Customer shall cooperate with reasonable usage information requests. For the avoidance of doubt, no feedback or usage information provided under this Section shall be used by any Vendor to imply, suggest, or state endorsement by the U.S. Federal Government or any Government Customer (MDVA Section 5.10(e)).

14. Vendor Notice of Licensing Changes. Vendors must provide 10xNatSec with at least fifteen (15) business days' written notice before making any substantive changes to licensing terms, pricing, or service levels applicable to Vendor Data or Vendor products made available through the Platform (MDVA Section 5.6).

15. Dispute Resolution.

15.1 10xNatSec and Vendor/User Disputes. This Agreement is governed by the laws of the State of Delaware. All actions shall be brought exclusively in Delaware state or federal courts. Each Party consents to jurisdiction and venue and waives objections thereto. 10xNatSec is the initial point of contact for all disputes (MDVA Section 13.3.1). This Section 15.1 does not apply to the United States Government or any Government

Customer, whose disputes are governed exclusively by Sections 15.2–15.4.

15.2 Claims Against the USG. Any action against the United States Government brought by a Vendor shall be filed under the Federal Tort Claims Act, consistent with MDVA Section 13.3.2. To the extent permitted by US federal law, the prevailing party in such action may seek recovery of costs and reasonable attorneys' fees.

15.3 No Arbitration Against the USG. No dispute against the USG shall be submitted to binding arbitration. All such disputes shall be resolved through the FTCA or judicial proceedings, consistent with MDVA Section 13.3.3.

15.4 USG Jurisdiction. Claims against the USG shall be governed by US Federal law and brought exclusively in United States federal courts in the District of Columbia, consistent with MDVA Section 13.3.4. Vendor consents to personal jurisdiction and waives venue objections.

16. Acceptable Use; AI Safety, Security, and Platform Integrity

16.1 Intended Use and Compliance with Guardrails. Users shall use the Platform, including any chat agent or other artificial-intelligence-enabled feature, solely for authorized, lawful, and intended purposes and in accordance with this Agreement, the MDVA, the Vendor-EULA, applicable policies, and all applicable laws, regulations and security requirements. Users shall comply with all technical, operational, safety, security, access-control, and content-use restrictions, controls, limitations, instructions, and guardrails implemented by 10xNatSec, or the Platform.

16.2 Prohibited Conduct. A User shall not, and shall not attempt to, assist, encourage, direct, or permit any other person to:

- evade, defeat, bypass, disable, manipulate, override, test, probe, or otherwise circumvent any Platform security control, access restriction, monitoring mechanism, technical limitation, content filter, safety measure, usage restriction, or artificial intelligence guardrail;
- submit, upload, transmit, embed, conceal, or use prompts, instructions, content, code, data, files, links, tools, or other inputs intended to cause a chat agent or other Platform feature to disregard, disclose, alter, override, or act inconsistently with its system instructions, safety controls, access controls, intended functions, or applicable restrictions, including through prompt injection, jailbreak attempts, instruction-hierarchy attacks, indirect prompt injection, adversarial inputs, role-playing intended to defeat controls, encoded or obfuscated instructions, or similar techniques;
- attempt to discover, obtain, extract, reconstruct, infer, reveal, or exfiltrate non-public system prompts, hidden instructions, model configurations, model weights, source code, algorithms, training data, evaluation data, credentials,

authentication tokens, encryption keys, security architecture, proprietary methodologies, non-public Vendor Data, Government Customer data, or other restricted or confidential information;

- introduce, upload, transmit, distribute, execute, attempt to execute, or cause the Platform to generate, deploy, or facilitate Harmful Code, including malware, viruses, worms, trojan horses, ransomware, spyware, malicious scripts, exploit code, command-and-control mechanisms, credential-harvesting tools, phishing content, denial-of-service tools, destructive payloads, or code intended to gain unauthorized access to, disrupt, damage, impair, monitor, or interfere with any system, network, device, account, data, or service;
- use the Platform or any chat agent to plan, facilitate, enable, conceal, automate, or assist unlawful, hazardous, dangerous, fraudulent, malicious, or unauthorized conduct, including cyber intrusion, unauthorized surveillance, credential theft, fraud, evasion of security controls or law-enforcement activity, exploitation of vulnerabilities, unauthorized collection or disclosure of information, or conduct that could reasonably threaten national security, public safety, persons, property, systems, networks, or data;
- use the Platform to obtain, generate, process, disseminate, or disclose classified information, controlled unclassified information, export-controlled information, Personal Data, operationally sensitive information, law-enforcement-sensitive information, or other restricted information except where expressly authorized by the applicable Government Customer, Vendor, Order Form, Platform authorization level, security requirements, and Applicable Law;
- access or attempt to access the Platform, Vendor Data, a chat agent, another user's account, or any data, capability, system, model, or administrative function without authorization; use another person's credentials; impersonate another person or entity; or misrepresent the User's identity, authorization, affiliation, role, or purpose;
- conduct automated scraping, crawling, bulk extraction, enumeration, probing, vulnerability scanning, load testing, penetration testing, model extraction, model inversion, model evasion, benchmarking, or other automated or manual activity directed at the Platform, except where expressly authorized in writing by 10xNatSec;
- use Platform outputs, including chat-agent outputs, as a substitute for required human judgment, independent verification, authorized analytical review, security review, legal review, operational approval, or other required Government, Vendor, or organizational process; or
- otherwise use the Platform in a manner that 10xNatSec reasonably believes threatens or may threaten the confidentiality, integrity, availability, safety, security, lawful operation, or intended use of the Platform, Vendor Data, Government Customer data, any User, or any third party.

16.3 Monitoring, Investigation, and Preservation of Evidence. To the extent permitted by Applicable Law, 10xNatSec may monitor, log, review, analyze, retain, preserve, and disclose Platform activity, prompts, inputs, outputs, account information, audit records, technical telemetry, and other information reasonably necessary to administer the Platform; enforce this Agreement; investigate suspected misuse; protect the Platform, Users, Vendor Data, Government Customer data, and third parties; meet legal, regulatory, contractual, security, or audit obligations; or respond to a lawful request. Users shall cooperate with reasonable investigations of suspected violations of this Section.

16.4 Administrative Enforcement. If 10xNatSec reasonably believes that a User has violated, attempted to violate, or presents a material risk of violating this Section, any applicable guardrail, or any related Platform security or acceptable-use requirement, 10xNatSec may take any action it reasonably considers necessary to protect the Platform and affected persons or entities. Such action may include:

- issuing a warning or notice of noncompliance;
- requiring remediation, corrective action, additional training, written acknowledgment, or certification of compliance;
- restricting, modifying, or disabling access to particular Platform features, Vendor Data, chat-agent functions, accounts, integrations, APIs, tools, or administrative capabilities;
- suspending or terminating an individual User's access;
- suspending or terminating access for a Government Customer, Vendor, Authorized User group, Downstream User group, or other sponsoring organization, subject to applicable law and contractual requirements;
- removing, quarantining, blocking, or preserving prompts, files, code, content, outputs, accounts, integrations, or other materials associated with suspected misuse;
- notifying the applicable Government Customer, Vendor, sponsoring organization, contracting/agreement officer, program office, security office, information-system security officer, agency point of contact, or other responsible authority; and/or
- pursuing any other remedy available under this Agreement, the MDVA, an Order Form, the Vendor-EULA, or Applicable Law.

The foregoing measures are administrative, protective, and remedial measures intended to safeguard the Platform and its users and are not contractual penalties.

16.5 Notice and Opportunity to Cure. Except where immediate action is reasonably necessary to protect the Platform, Vendor Data, Government Customer data, Users, third parties, national security, public safety, or the integrity, confidentiality, or availability of systems or information, 10xNatSec will provide notice of an alleged violation and a

reasonable opportunity to cure or explain the matter. Notwithstanding the foregoing, 10xNatSec retains sole discretion to take immediate action, including suspension or termination of access, without prior notice or opportunity to cure where 10xNatSec reasonably believes that a violation is ongoing, intentional, malicious, hazardous, unlawful, likely to recur, incapable of cure, or presents a security, safety, operational, legal, or reputational risk.

16.6 Government Users. With respect to Government Customers, Authorized Users, and Downstream Users, enforcement actions under this Section may include suspension, restriction, or revocation of Platform access and notification to the applicable Government Customer and appropriate Government point of contact, including a contracting/agreement officer, program office, security office, information-system security officer, or agency-designated representative. Nothing in this Section creates a monetary penalty, indemnification obligation, or liability of the United States Government or any Government Customer beyond that expressly authorized by Applicable Law and subject to the availability of appropriated funds.

16.7 Reporting of Hazardous or Dangerous Activity. Where 10xNatSec reasonably believes that a User's activity may be unlawful, malicious, hazardous, dangerous, threaten national security or public safety, compromise or threaten to compromise systems or data, involve actual or attempted unauthorized access, or otherwise require escalation, 10xNatSec may preserve relevant information and report the activity to the appropriate United States Government authority, law-enforcement agency, regulatory authority, cybersecurity authority, affected Government Customer, Vendor, or other appropriate third party, to the extent permitted or required by Applicable Law. Nothing in this Section limits 10xNatSec's ability to cooperate with lawful governmental, regulatory, audit, investigative, or judicial requests.

16.8 No Reliance on Platform Availability or Outputs. 10xNatSec may modify, limit, suspend, disable, or discontinue any Platform feature, including chat-agent capabilities, at any time to maintain security, safety, legal compliance, data protection, Platform integrity, or conformance with applicable guardrails. Users remain responsible for reviewing and validating Platform outputs before relying on them for any decision, action, analysis, recommendation, or operational purpose.

— No signature required —

This Agreement is effective upon any User's first access to the Platform following acceptance of the Platform Access Acknowledgment. 10xNatSec shall maintain a log of all acceptance events for audit and compliance purposes.