DOMINUS GRAY, LLC

Securing Access to Opportunity

Mutual Non-Disclosure & Confidentiality Agreement

For Cybersecurity Consulting & DoD Contractor Engagements

February 2026

Document ID: DG-NDA-2026-001

CONFIDENTIAL — DO NOT DISTRIBUTE

SDVOSB | MBE | NaBOVA | VetHUB | SAM.gov Registered

Service-Disabled Veteran-Owned Small Business

IMPORTANT LEGAL NOTICE

This template is provided for informational purposes only and does not constitute legal advice. This document should be reviewed, customized, and approved by qualified legal counsel before execution. Dominus Gray, LLC makes no representations or warranties regarding the legal sufficiency of this template for any specific use case or

1. Parties to This Agreement

This Mutual Non-Disclosure and Confidentiality Agreement (this "Agreement") is entered into as of the date of last signature below (the "Effective Date"), by and between:

PARTY A (Disclosing/Receiving Party)

[PARTY A FULL LEGAL NAME]
Address: [PARTY A ADDRESS]
Point of Contact: [PARTY A CONTACT NAME]
Title: [PARTY A CONTACT TITLE]
Email: [PARTY A EMAIL]

PARTY B (Disclosing/Receiving Party)

Dominus Gray, LLC
Address: [PARTY B ADDRESS]
Point of Contact: Odie Gray
Title: Chief Executive Officer
Email: odie.gray@dominusgray.com

Each party may be referred to individually as a "Party" and collectively as the "Parties." This Agreement is mutual in nature; each Party may disclose and receive Confidential Information. The Party disclosing information is the "Disclosing Party" and the Party receiving information is the "Receiving Party."

2. Definition of Confidential Information

"Confidential Information" means any and all non-public, proprietary, or sensitive information disclosed by either Party to the other Party, whether orally, in writing, electronically, or by any other means, including but not limited to:

- Controlled Unclassified Information (CUI) as defined by 32 CFR Part 2002 and the CUI Registry, including all categories and subcategories applicable to defense contracting engagements
- Controlled Technical Information (CTI) as defined in DFARS 252.204-7012, including technical data with military or space application subject to export controls
- Business information, including financial data, pricing structures, strategic plans, customer lists, vendor relationships, contract terms, and bid/proposal information
- Trade secrets, inventions, discoveries, know-how, methodologies, processes, techniques, algorithms, software source code, architectures, and system designs
- Security assessments, vulnerability reports, penetration testing results, risk assessments, security architectures, incident response plans, and cybersecurity documentation
- Network diagrams, system configurations, access credentials, encryption keys, and any technical infrastructure information
- Personnel information, including employee data, organizational structures, staffing plans, and security clearance information
- Any information marked or designated as "Confidential," "Proprietary," "CUI," "FOUO," or with similar restrictive markings
- Any information that a reasonable person would understand to be confidential given the nature of the information and circumstances of disclosure

Confidential Information includes all notes, analyses, compilations, studies, summaries, and other materials prepared by the Receiving Party that contain, reflect, or are derived from Confidential Information.

3. Obligations of Receiving Party

The Receiving Party agrees to the following obligations with respect to all Confidential Information received from the Disclosing Party:

- Hold and maintain all Confidential Information in strict confidence using at least the same degree of care used to protect its own confidential information, but in no event less than reasonable care
- Limit access to Confidential Information to those employees, contractors, and agents ("Representatives") who have a legitimate need to know and who are bound by confidentiality obligations at least as restrictive as those contained herein
- Not disclose, publish, or otherwise disseminate Confidential Information to any third party without the prior written consent of the Disclosing Party
- Not use Confidential Information for any purpose other than the evaluation, negotiation, and performance of the business relationship between the Parties (the "Purpose")
- Not reverse engineer, decompile, or disassemble any Confidential Information, including software, prototypes, or technical materials
- Promptly notify the Disclosing Party in writing upon discovery of any unauthorized use or disclosure of Confidential Information
- Ensure that all copies, reproductions, and summaries of Confidential Information are properly marked with applicable confidentiality and CUI markings
- Implement and maintain administrative, technical, and physical safeguards adequate to protect the confidentiality of the Confidential Information in accordance with NIST SP 800-171 requirements where CUI is involved

Government Disclosure

If the Receiving Party is required by law, regulation, or valid legal process (including subpoena, civil investigative demand, or court order) to disclose any Confidential Information, the Receiving Party shall: (a) provide prompt written notice to the Disclosing Party prior to such disclosure to the extent legally permitted; (b) cooperate with the Disclosing Party in seeking a protective order or other appropriate remedy; and (c) disclose only that portion of Confidential Information that is legally required.

4. Exclusions from Confidential Information

The obligations set forth in this Agreement shall not apply to information that the Receiving Party can demonstrate by competent evidence:

- Was already known to the Receiving Party at the time of disclosure without obligation of confidentiality, as evidenced by written records predating the disclosure
- Is or becomes publicly available through no fault, act, or omission of the Receiving Party
- Is rightfully received from a third party without restriction on disclosure and without breach of any obligation of confidentiality
- Is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information, as evidenced by contemporaneous written records
- Is approved for release by prior written authorization of the Disclosing Party

CUI Exception

Notwithstanding the foregoing exclusions, information designated as Controlled Unclassified Information (CUI) shall remain subject to all applicable federal regulations governing CUI handling regardless of whether such information falls within any of the above exclusions. CUI safeguarding requirements are mandated by federal law and cannot be waived by private agreement.

5. Term and Duration

a) Term. This Agreement shall become effective as of the Effective Date and shall remain in full force and effect for a period of two (2) years from the Effective Date, unless earlier terminated by either Party upon thirty (30) days' prior written notice to the other Party.

b) Survival. The confidentiality obligations set forth in this Agreement shall survive the expiration or termination of this Agreement for a period of five (5) years from the date of disclosure of the applicable Confidential Information, except that:

- Obligations with respect to trade secrets shall survive for so long as such information remains a trade secret under applicable law
- Obligations with respect to CUI shall survive for the duration required by applicable federal regulations, which may exceed the five-year survival period

- Obligations with respect to personally identifiable information (PII) shall survive indefinitely or as required by applicable privacy laws

c) Renewal. This Agreement may be renewed for successive one (1) year periods upon mutual written agreement of the Parties prior to expiration.

6. Return and Destruction of Materials

Upon the earlier of (a) the expiration or termination of this Agreement, or (b) written request by the Disclosing Party, the Receiving Party shall, at the Disclosing Party's election:

- Promptly return to the Disclosing Party all tangible materials containing or embodying Confidential Information, including all copies, reproductions, and summaries thereof; or
- Destroy all such materials and certify such destruction in writing to the Disclosing Party within thirty (30) days, using methods consistent with NIST SP 800-88 Guidelines for Media Sanitization where applicable

Notwithstanding the foregoing, the Receiving Party may retain: (a) one (1) archival copy of Confidential Information solely for legal compliance and dispute resolution purposes, subject to the ongoing confidentiality obligations of this Agreement; and (b) any copies required to be retained by applicable law, regulation, or professional standards, provided that such retained copies remain subject to the terms of this Agreement.

CUI Destruction Requirements

Destruction of media containing CUI must comply with NIST SP 800-88 Rev 1 and applicable CUI Registry destruction requirements. Electronic media must be sanitized using approved methods (e.g., cryptographic erase, degauss, or physical destruction). Paper documents containing CUI must be destroyed using cross-cut shredders meeting NSA/CSS EPL specifications.

7. Remedies

a) Injunctive Relief. The Parties acknowledge that a breach of this Agreement may cause irreparable harm to the Disclosing Party for which monetary damages would be an inadequate remedy. Accordingly, the Disclosing Party shall be entitled to seek equitable relief, including injunction and specific performance, in addition to all other remedies available at law or in equity, without the necessity of proving actual damages or posting a bond or other security.

b) Indemnification. The Receiving Party shall indemnify, defend, and hold harmless the Disclosing Party and its officers, directors, employees, agents, and affiliates from and against any and all losses, damages, liabilities, costs, and expenses (including reasonable attorneys' fees) arising out of or related to any breach of this Agreement by the Receiving Party or its Representatives.

c) No Limitation. The rights and remedies provided in this Agreement are cumulative and are in addition to, not in lieu of, any other rights or remedies available at law or in equity. No failure or delay in exercising any right or remedy shall operate as a waiver thereof.

8. CUI-Specific Provisions

DFARS 252.204-7012 COMPLIANCE

Where Confidential Information includes Covered Defense Information (CDI) or CUI, the Parties shall comply with all requirements of DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," including the implementation of NIST SP 800-171 security requirements.

8.1 Safeguarding Requirements

Each Party that receives CUI from the other Party shall:

- Implement and maintain security controls in accordance with NIST SP 800-171 Rev 2 (or its successor) on all information systems that process, store, or transmit CUI

- Maintain a current System Security Plan (SSP) and Plan of Action and Milestones (POA&M) for systems handling CUI
- Limit CUI processing to information systems that meet the security requirements and are within the defined CUI boundary
- Ensure that cloud services used to process or store CUI meet FedRAMP Moderate baseline requirements or equivalent

8.2 Marking Requirements

All CUI shall be marked in accordance with 32 CFR Part 2002 and the CUI Marking Handbook. At a minimum:

- CUI designation indicators shall be applied to all documents containing CUI
- Banner markings shall be applied to the top and bottom of each page containing CUI
- Portion markings are encouraged and may be required for certain CUI categories
- Electronic media containing CUI shall be marked with appropriate CUI labels
- Email containing CUI shall include "CUI" or "CONTROLLED" in the subject line

8.3 Cyber Incident Reporting

MANDATORY 72-HOUR REPORTING REQUIREMENT

In the event of a cyber incident that affects CUI or the information system on which CUI resides, the Receiving Party shall:

1. Report the incident to the Disclosing Party within seventy-two (72) hours of discovery
2. Report to the DoD via DCISE Portal (ICF) (https://icf.dcise.cert.org) within 72 hours per DFARS 252.204-7012 (Legacy DIBNet portal decommissioned June 2025)
3. Preserve and protect images of all known affected information systems and relevant monitoring data for at least 90 days
4. Cooperate fully with any investigation conducted by the Disclosing Party or the DoD
5. Provide the DoD Cyber Crime Center (DC3) with access to affected systems and forensic images upon request

8.4 Export-Controlled Information (ITAR/EAR)

ITAR / EAR COMPLIANCE PROVISION

If Confidential Information includes data subject to ITAR (22 CFR 120-130) or EAR (15 CFR 730-774), the Receiving Party shall additionally comply with applicable export control regulations, restrict access to U.S. persons only, and report any unauthorized disclosure to the Directorate of Defense Trade Controls (DDTC) or Bureau of Industry and Security (BIS) as applicable.

8.5 Subcontractor Flow-Down

The Receiving Party shall not provide CUI to any subcontractor or lower-tier entity without: (a) prior written approval from the Disclosing Party; (b) ensuring the subcontractor has implemented NIST SP 800-171 security requirements; and (c) flowing down equivalent CUI protection requirements through a binding agreement.

9. General Provisions

9.1 Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of [STATE], without regard to its conflict of laws principles. Any legal action or proceeding arising under this Agreement shall be brought exclusively in the federal or state courts located in [STATE], and the Parties hereby consent to personal jurisdiction and venue therein.

9.2 Severability

If any provision of this Agreement is held to be invalid, illegal, or unenforceable, the validity, legality, and enforceability of the remaining provisions shall not in any way be affected or impaired thereby. The invalid provision shall be modified to the minimum extent necessary to make it valid and enforceable while preserving the Parties' original intent.

9.3 Entire Agreement

This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements, understandings, negotiations, and discussions, whether oral or written, relating to the subject matter of this Agreement. There are no warranties, representations, or

agreements between the Parties in connection with the subject matter hereof except as set forth herein.

9.4 Amendments

No amendment, modification, or waiver of any provision of this Agreement shall be effective unless in writing and signed by both Parties. No waiver of any provision shall constitute a waiver of any other provision or of the same provision on any other occasion.

9.5 Assignment

Neither Party may assign or transfer this Agreement or any rights or obligations hereunder without the prior written consent of the other Party, except that either Party may assign this Agreement to a successor entity in connection with a merger, acquisition, or sale of all or substantially all of its assets, provided that the assignee agrees in writing to be bound by the terms of this Agreement.

9.6 No License or Implied Rights

Nothing in this Agreement grants the Receiving Party any license, right, title, or interest in or to any Confidential Information, intellectual property, or other proprietary rights of the Disclosing Party. All Confidential Information remains the exclusive property of the Disclosing Party.

9.7 No Obligation

This Agreement does not obligate either Party to enter into any further agreement, transaction, or business relationship. Either Party may terminate discussions at any time for any reason.

9.8 Counterparts

This Agreement may be executed in counterparts, each of which shall be deemed an original and all of which together shall constitute one and the same instrument. Electronic signatures and PDF copies shall be deemed to have the same force and effect as originals.

9.9 Notices

All notices required or permitted under this Agreement shall be in writing and shall be deemed effectively given: (a) upon personal delivery; (b) upon confirmed transmission by email; (c) one (1) business day after deposit with a nationally recognized overnight courier; or (d) three (3) business days after deposit in the United States mail, postage prepaid, certified or registered, return receipt requested, addressed to the Parties at their respective addresses set forth above or to such other address as either Party may

designate by written notice.

10. Execution

IN WITNESS WHEREOF, the Parties have executed this Mutual Non-Disclosure and Confidentiality Agreement as of the Effective Date.

[PARTY A]

Signature

Printed Name

Title

Date

Dominus Gray, LLC

Signature

Printed Name

Title

Date

DOCUMENT CONTROL

Document ID: DG-NDA-2026-001
Version: 1.0
Classification: CONFIDENTIAL
Prepared by: Dominus Gray, LLC
CEO: Odie Gray
Designation: SDVOSB | SAM.gov Registered
Status: Template — Requires legal review before execution

ABOUT DOMINUS GRAY, LLC

Dominus Gray, LLC is a Service-Disabled Veteran-Owned Small Business (SDVOSB) specializing in cybersecurity consulting, CMMC compliance, and IT staffing for Department of Defense contractors and federal agencies. Registered on SAM.gov and certified through multiple veteran and minority business programs.