Dear Supplier/Service Provider:

Some technology, technical and other data, or parts to which your company may have access while working with Banks Technologies (Banks Tech) constitutes Controlled Unclassified Information (CUI) subject to protection under the Information Assurance (IA) provisions in certain Government contracts, Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulations Supplements (DFARS) and federal laws. The Government requires Banks Tech to obtain the agreement of its suppliers to comply with the same requirements that Banks Tech must observe for protecting CUI. Banks Tech will share CUI as necessary for carrying out statements of work with its suppliers and service providers that demonstrate and verify compliance to these requirements.

CYBERSECURITY AND INCIDENT REPORTING-CONTROLLED UNCLASSIFIED INFORMATION

NOTE: This requirement applies when you receive Controlled Unclassified Information, as defined in Section 1.2 below, in execution of your subcontract or service. Suppliers/service providers are required to comply with all applicable DFARS and NIST standards, including without limitation DFARS flow down clause 252.204-7012 and NIST 800-171.

1. Controlled Unclassified Information (CUI)
   1. Banks Tech and its suppliers/service providers, with contracts that requires the storing, transmittal, or processing of controlled unclassified information (CUI) on subcontractor/service provider systems relating shall meet requirements of DFARS 252.204-7012 and NIST 800-171.
   2. CUI is unclassified information about government platforms, systems, and parts subject to access, safeguarding, dissemination or distribution limitations and marked according to Department of Defense manual 5200.01 Volume 4 and the National Archives CUI Registry as: Controlled Unclassified Information, Distribution Statements B through F, For Official Use Only, EAR/ITAR. Contact your Banks Tech buyer for questions regarding information pertaining to any subcontract or services that constitutes CUI.
   3. Supplier/service provider agrees to incorporate and flow down DFARS clause 252.204-7012 to all suppliers/subcontractors storing, processing and/or generating CUI as part of contract performance. See Safeguarding Covered Defense Information and Cyber Incident Reporting (Doc #50307).
      1. In accordance with DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting, subcontractors, including vendors and consultants, are required to rapidly report cyber incidents within 72 hours of discovery to the Banks Tech buyer point of contact and directly to Department of Defense (DoD) at <https://dibnet.dod.mil/portal/intranet/>. This includes providing the incident report number, automatically assigned by DoD to Banks Tech as soon as practical.
   4. Supplier/service provider agrees to incorporate this section, including this clause, into all its subcontracts or purchase orders for goods or services furnished in support of all Government contracts with Banks Tech that require sharing of CUI.
   5. All DFARS compliance as described in this document are subject to audit and verification by Banks Tech.

We request that an authorized official execute this agreement on behalf of supplier/service provider

and return it. Thank you.

ACKNOWLEDGED AND AGREED TO:

Company: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Printed Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Title: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_