TO OUR VALUED SUPPLIERS & VENDORS,

Action required- Please read this letter in its entirety and respond with the attached document signed and dated by an authorized person at your company as soon as possible. Failure to do so may impede our ability to enter into future contracts or services with your company.

We at Bourdon Forge Company, Inc. are steadfast in our commitment to working with our suppliers to keep sensitive information safe, secure, and out of the hands of those who would use it to endanger global security. As a supplier to Bourdon Forge Company, Inc., you may be required to comply with the Flowdown of government compliancy that has been mandated for all government contractors, subcontractors, and suppliers of said contractors.

U.S. Government Subcontractor Regulatory Alert

- Beginning November 30, 2020, Contracting Officers must include the new DFARS 252.2047019 provision and DFARS clause 252.204-7020 clause in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of commercial-off-the-shelf (COTS) items. These will require the DoD supply chain to quantify their current cybersecurity compliance with NIST SP 800-171 requirements using the NIST SP 800-171 DoD Assessment Methodology.
- Pursuant to 252.204-7020, contractors such as Bourdon Forge Company, Inc. may not award a subcontract or other contractual instrument that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS 252.204-7012, unless the supplier has:
    1. Completed at least a Basic Assessment in accordance with NIST SP 800-171 DoD Assessment Methodology (or in the alternative the Government performed Medium or High Assessment) within the last three years for all covered contractor information systems relevant to its offer that are not part of an information technology system operated on behalf of the Government; *and*
    2. "To the extent the supplier completed a Basic Assessment, it submitted its summary level scores, and other information required by paragraph (d) of DFARS 252.204-7020, either directly into the Supplier Performance Risk System (SPRS) or via encrypted email to webptsmh@navy.mil for posting to the SPRS."

Cybersecurity Maturity Model Certification (CMMC)

Independent 3rd Party Certification Requirements:

- CMMC Level certification requirements for parts and services Beginning in 2020, CMMC requirements will be required in select contracts. Full implementation will begin in 2021 with expectations to be required in all contracts by 2026. When required in contracts issued by DoD, Sellers of each part/service throughout the supply chain must be CMMC certified at or above the required CMMC level.

Contractual Requirements

- "Notional Example of Possible Contractual Requirements that Bourdon Forge Company, Inc. may utilize flow CMMC requirements to suppliers. These are subject to change pending release of

CMMC requirements into contracts and Bourdon Forge Company, Inc.'s review of those requirements."

- In 2020, the Department of Defense (DoD) mandated cyber certification (known as CMMC) for all suppliers who support DoD contracts. This certification will potentially eliminate self-attestation and require an independent 3rd party certification based on three levels. The CMMC levels will be used as a "go" or "no go" criteria to bid on or receive contracts.
- All Defense Industrial Base (DIB) companies must comply with CMMC, not just companies handling Controlled Unclassified Information (CUI). We, along with our industry peers, are working closely with the government throughout the development of the CMMC program.
- Suppliers can start to prepare for CMMC by ensuring their compliance to DFARS 252.204-7012 and NIST SP 800-171 and by ensuring that your suppliers are aware of the CMMC effort and encourage them to become educated on it.

Learn More About CMMC and Your Company

- In an effort stay current with the updates on this program, suppliers are encouraged to frequently check the Office of the Under Secretary of Defense for Acquisition and Sustainment CMMC website.
- To assist suppliers in preparing for the upcoming CMMC requirements the Defense Industrial Base (DIB) Sector Coordinating Council (SCC) launched a new CyberAssist Website to provide trusted resources for short-term and long-term cyber resiliency within the supply chain. Resources include guides, standards, sample policies and procedures, videos, example tools, lessons learned, and other helpful information. Users can simply click on a security control family and be directed to a list of resources to help with successful implementation and assessment. This website will also serve as a platform to share awareness, threats, best practices, tools and other resources from industry peers, government groups and initiatives.

Frequently Asked Questions for CMMC have been provided by the OUSD A&S and the CMMC Accreditation Board (now known as CyberAB).

Supplier Annual Certification CR-003

- Our annual supplier certification (CR-003) includes a question about your company's ability to handle Covered Defense Information (CDI) in compliance with the cyber DFARS clause 252.204-7012. For an accurate response, we recommend checking with your IT Security professionals and legal counsel. It is our policy to only share CDI with suppliers who have assured us that they are capable of handling it.
- Going forward, we will also be asking your company to confirm that you have System Security Plans (SSPs).

Cyber Security

- Together with our suppliers, we play a shared role in securing our global supply chain. On October 21, 2016, the DOD published the Final Rule for DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. It represents DoD's efforts to prevent improper access to important unclassified information in the supply base. The DFARs clause contains the following main requirements:
    - Adequate Security
        - Contractors must provide adequate security for "covered contractor information systems," to include implementing the security controls of National

Institute of Standards and Technology (NIST) SP 800-171 as required. A "covered contractor information system" is an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

- Cyber Incident Reporting
  - Contractors must report cyber incidents to the DoD at https://dibnet.dod.mil within 72 hours of discovery, and subcontractors must provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable.
  - Contractors must also conduct a review for evidence of compromise, isolate and submit malicious software in accordance with instructions provided by the contracting Officer, preserve and protect images of all known affected information systems and relevant monitoring/packet capture data for at least 90 days for potential DoD review, and provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.
- Subcontractor Flowdown
  - This DFARS clause must be flowed down in any subcontracts or similar contractual instruments in which subcontract performance will involve covered defense information or operationally critical support. The clause must be flowed down without alteration, except to identify the parties. The full DFARS clause can be found in its entirety under Related Links. Together, the threats we face necessitate that we work together to minimize risk, protect our sensitive information, and safeguard our global security. If you have any questions or would like additional information, please contact paulaj@bourdonforge.com

Immediate Attention Required by You- Supplier to BFI

Attached, please find our Mutual Non-Disclosure & Proprietary Information Exchange Agreement. This is considered the first step in the process, and we ask that a company officer or other qualified person at your company please sign and date this document and return it post haste.

In addition, we ask that you supply Bourdon Forge Company, Inc. with your current SPRS score- and update it whenever that score changes as your company moves through the compliance process.

If an SPRS score is not available currently, Bourdon Forge Company, Inc. requests that you please provide information on company letterhead with an explanation of a Plan of Action (POAM) to become compliant with the above-mentioned requirements.

ATTACHED: 5 PAGES – MUTUAL NON-DISCLOSURE & PROPRIETARY INFORMATION EXCHANGE AGREEMENT

MUTUAL NON-DISCLOSURE & PROPRIETARY

INFORMATION EXCHANGE AGREEMENT

BETWEEN:

Bourdon Forge Company, Inc.

AND:

_____
(Company Name)

_____
(Company Rep)

MUTUAL NONDISCLOSURE AGREEMENT

This Mutual Nondisclosure Agreement (the "**Agreement**") dated on _____ of 20____ (the "Effective Date"), by and between **The Bourdon Forge Company, Inc**. ("**BFI**") a Connecticut Corporation, with a principal address at 99 Tuttle Road, Middletown, CT 06457 and _____, a _____ corporation with a principal place of business at _____ ("**Company**"), individually referred to as "Party" and collectively referred to as the "Parties".

In consideration for the Parties' agreement to participate in the activities described below, the parties agree:

1. Purpose. The Parties wish to engage in business (the "Business Purpose") and in connection with the Business Purpose, each Party may disclose to the other certain confidential technical and business information which the disclosing Party (in each case, the "Disclosing Party") desires the receiving Party (in each case, the "Receiving Party") to treat as confidential.

2. Confidential Information. "Confidential Information" means any information disclosed by the Disclosing Party either directly or indirectly in writing, orally or transmitted in any manner related to the Business Purpose, which may include, but is not limited to, trade secrets, discoveries, ideas, concepts, know-how, techniques, designs, specifications, drawings, diagrams, data, computer programs, business activities and operations, customers, reports, studies and other technical and business information. Confidential Information may or may not be patentable, constitute the basis of patentable inventions, or be otherwise protectable.

3. Limitations on Confidential Information. Confidential Information shall not include the Disclosing Party's information which:

3.1. The Receiving Party knows at the time of disclosure, free of any obligation to keep it confidential, as evidenced by written records;
3.2. Is in the public domain at the time of disclosure or becomes publicly available through authorized disclosure;
3.3. Is independently developed by the Receiving Party without the use of any Confidential Information as evidenced by written records;
3.4. Is rightfully in the possession of the Receiving Party prior to the time of disclosure;
3.5. The Receiving Party rightfully obtains from a third party who has the right to transfer or disclose it.

If any portion of any Confidential Information falls within any of the above exceptions, the remainder of the Confidential Information shall continue to be subject to the requirements of this Agreement.

4. Protection of Confidential Information.

4.1. Receiving Party agrees that it will use reasonable care to keep in confidence all Confidential Information of the Disclosing Party, will exercise reasonable care to protect the Confidential Information of the Disclosing Party and will not directly or indirectly disclose or transmit any Confidential Information of the Disclosing Party in any manner or form or for any purpose to any person, party, firm or entity except as expressly permitted herein. "Reasonable care" shall mean the

degree of care a reasonably prudent person entrusted with confidential information would exercise under the circumstances, and in no event less than the same degree of care to protect the Confidential Information as a Party would employ with respect to its own information of like importance which it does not desire to have published or disseminated. Without limiting the foregoing, the Receiving Party shall have the right to disclose Confidential Information of the Disclosing Party on a need-to-know basis only to its employees, officers, directors, attorneys, accountants and auditors provided that such parties are subject to confidentiality obligations with respect to such Confidential Information at least as restrictive as the obligations set forth in this Agreement.

4.2. Each Party further agrees not to use any Confidential Information of the other Party for any purpose except the Business Purpose. The Disclosing Party shall use reasonable care to mark all written Confidential Information "CONFIDENTIAL". However, failure to mark written Confidential Information "CONFIDENTIAL" does not constitute a designation of non-confidentiality when the confidential nature would be reasonably recognized by the Receiving Party from the subject matter or subject type of the information disclosed and such information shall be deemed confidential.

4.3. Receiving Party shall not make copies of Disclosing Party's Confidential Information unless previously approved in writing by Disclosing Party. Receiving Party shall reproduce Disclosing Party's proprietary rights notices on any such approved copies, in the same manner in which such notices were set forth in or on the original.

5. Compelled Disclosure. Notwithstanding the foregoing, a Receiving Party may disclose Confidential Information to the extent such disclosure is compelled by applicable law, court order or similar governmental process, provided that the Receiving Party being required to make such compelled disclosure notifies the Disclosing Party as soon as possible and, upon the request of the latter, shall cooperate with the Disclosing Party in contesting such a disclosure. Except in connection with failure to discharge the responsibilities set forth in the preceding sentence, neither party shall be liable in damages for any disclosures pursuant to such legal action.

6. Ownership of Confidential Information. All information furnished or disclosed under this Agreement shall at all times remain the property of the Disclosing Party unless otherwise agreed in writing and all documents furnished by the Disclosing Party shall be returned to the Disclosing Party or destroyed promptly at the request of the Disclosing Party together with all copies made of such information by the Receiving Party and all documents, memoranda, notes and other writings whatsoever prepared by the Receiving Party based on Confidential Information. Such destruction shall be certified in writing to the Disclosing Party by an authorized officer of the Receiving Party.

7. No License or Future Obligation. Notwithstanding the foregoing, nothing contained in this Agreement shall be construed as creating an express or implied license or any rights in or to use any of the Confidential Information. Further, the disclosure of Confidential Information shall not result in any obligation on the part of either Party to enter into any future agreement relating to the Confidential Information, Business Purpose or to undertake any other obligation not set forth in a separate written agreement signed by the authorized parties thereto.

8. No Warranty. ALL CONFIDENTIAL INFORMATION IS PROVIDED "AS IS". NEITHER PARTY MAKES ANY WARRANTIES, EXPRESS, IMPLIED OR OTHERWISE, REGARDING THE ACCURACY, COMPLETENESS OR PERFORMANCE OF THE CONFIDENTIAL INFORMATION.

9. Independent Development.

9.1. Each party understands that the Receiving Party may currently or in the future be developing information internally or receiving information from other parties that may be similar to the Disclosing Party's information. Accordingly, nothing in this Agreement will be construed as a representation or inference that the Receiving Party will not develop products, or have products developed for it, that, without violation of this Agreement, compete with the products or systems contemplated by the furnishing party's Confidential Information.

9.2. Notwithstanding the foregoing, Receiving Party agrees that it shall not reverse engineer or create or attempt to create or permit any third party to reverse engineer or create new products or variations or improvements based on or derived from Disclosing Party's Confidential Information or any part thereof, whether in tangible or intangible form. Receiving Party is prohibited from dissembling or decompiling Disclosing Party's Confidential Information, creating derivative works from Disclosing Party's Confidential Information, or using Disclosing Party's Confidential Information on a computer-based information system that is publicly accessible.

10. Equitable Relief. Each Party acknowledges that its breach of this Agreement may result in immediate and irreparable harm to the Disclosing Party, for which there will be no adequate remedy at law, and the Disclosing Party shall be entitled to equitable relief to compel the Receiving Party to cease and desist all unauthorized use and disclosure of the Disclosing Party's Confidential Information.

11. Notices. All notices under this Agreement shall be deemed to have been duly given upon the mailing of the notice, postpaid, or upon the facsimile transmission, to the party entitled to such notice at the address set forth below.

12. Export Regulations. Notwithstanding any other provision of this Agreement, neither Party shall export any technical Confidential Information acquired under this Agreement or any commodities using such Confidential Information to any country to which the United States government forbids export or, at the time of export, requires an export license or approval.

13. Termination. A Party may unilaterally terminate this Agreement by providing not less than thirty (30) days prior written notice thereof to the other Party. Upon the expiration or termination of this Agreement, or receipt of a written request from the Disclosing Party, Receiving Party shall return to the Disclosing Party, or certify to the Disclosing Party the destruction of all Confidential Information received under this Agreement within thirty (30) days from such termination, expiration or request. Termination of this Agreement for any reason shall not relieve the Parties of the obligation not to disclose Confidential Information in any manner received hereunder, as provided in this Agreement, and the Parties shall treat all Confidential Information as such for a period of three (3) years from the date of termination.

14. Severability. Should any provisions of this Agreement be found unenforceable, the remainder shall still be in effect.

15. No Waiver. The failure of any Party to require performance by another Party of any provision of this Agreement shall in no way affect the full right to require such performance at any time thereafter.

16. Entire Agreement. This Agreement embodies the entire understanding between the Parties respecting the subject matter of this Agreement and supersedes any and all prior negotiations, correspondence, understandings and agreements between the Parties respecting the subject matter of this Agreement. This Agreement shall not be modified except by a writing duly executed on behalf of the Party against whom such modification is sought to be enforced.

17. Binding Effect. This Agreement shall benefit and be binding upon the Parties to this Agreement and their respective successors and assigns. This Agreement is non-assignable and non-transferable.

18. Construction of Agreement. This Agreement has been negotiated by the Parties and their respective attorneys, and the language of this Agreement shall not be construed for or against either Party.

19. Governing Law. This Agreement shall be governed by and construed in accordance with the laws of the State of Connecticut, without reference to conflicts of law or choice of law principles.

20. Counterparts. Either the original or copies, including facsimile transmissions, of this Agreement, may be executed in counterparts, each of which shall be an original as against any Party whose signature appears on such counterpart and all of which together shall constitute one and the same instrument.

IN WITNESS WHEREOF, the parties have caused their respective duly authorized representatives to execute and deliver this Agreement.

Company: _____	The Bourdon Forge Company, Inc.
By (signature): _____	By (signature): _____
Printed Name: _____	Printed Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Address for Notices:	Address for Notices:
_____	99 Tuttle Road
_____	Middletown, CT 06457
Attn: _____	Attn: Patricia Bourdon, CEO