AIRBOSS DEFENSE TERMS AND CONDITIONS OF PURCHASE

1. Scope and Acceptance.

(a) These Terms and Conditions of Purchase (the "Terms") apply to all purchase orders and amendments there to (collectively referred to as an "Order") issued by AirBoss Defense Group ("Buyer"). All goods and services (whether or not ancillary to a sale of goods) to be provided under an Order are included in the term "Goods".

(b) Seller will be deemed to have accepted an Order as issued (i) if Seller acknowledges, whether r orally, in writing or electronically, its acceptance of the Order, (ii) if Seller begins performance of the Order, (iii) if Seller ships any goods or materials, or (iv) through any other conduct that recognizes the existence of a contract with respect to the subject matter of the Order.

(c) Upon acceptance, the Order, together with these Terms, the AirBoss Defense Supplier Requirements Manual as in effect at such time (as posted on Buyer's website at https://airboss.com/, and any other document expressly incorporated in such Order or issued by or separately agreed to in writing by Buyer, (collectively the "Contract Documents"), will become a binding contract between Buyer and Seller (collectively, the "Contract").

(d) The Order does not constitute an acceptance of any offer or proposal made by Seller. Any reference in the Order to any offer or proposal made by Seller is solely to incorporate the description or specifications of Goods, but only to the extent that the description or specifications do not conflict with the description and specifications in the Order. The Order is limited to and conditional upon Seller's acceptance of these Terms exclusively, and any terms stated or supplied by Seller by any means, whether in Seller's quotation, acknowledgement, invoice or otherwise, that are additional to or different from those contained in these Terms or in an Order are unacceptable to Buyer, are hereby expressly rejected by Buyer and will not become a part of the Order unless specifically accepted in writing by Buyer. To the extent there is any inconsistency or conflict between any Contract Documents, the order of priority shall be as follows: any document separately agreed to in writing by an officer or director of Buyer after the issuance of the Order, followed by the terms on the face of the Order, followed by any document expressly incorporated into such Order, followed by these Terms, followed by the Supplier Quality Manual, followed by any other document issued by Buyer.

2. Prices

All purchase prices for Goods shall be set forth in each Order and shall be DDP (place of delivery) unless otherwise stated on the face of the Order. The prices contained in an Order shall be complete, and no additional charges of any type shall be added without Buyer's express prior written consent, including but not limited to, shipping, packaging, labeling, custom duties, taxes, storage, insurance, boxing and crating. Unless otherwise stated on the face of the Order or separately agreed in writing by the parties, the purchase price is a firm fixed price for the duration of the Contract and not subject to increase for any reason, including increased raw material costs, increased labor or other manufacturing costs, increased development costs, or changes in volumes or program length from those estimated or expected. Seller warrants that he prices for Goods set forth in this Order are no less favorable than Seller currently offers to any other customer for the same or similar

goods. If Seller reduces its prices to any other customer for the same or similar goods, Seller will immediately reduce the prices for the Goods correspondingly. Seller warrants and guarantees that it will, at all times, remain competitive in price, quality, performance and fulfillment of its obligations. If Seller is determined by Buyer not to be competitive in any of the foregoing areas, Buyer shall be entitled to terminate all or part of an Order pursuant to Section 20 hereof and re-source any or all Goods to a more competitive source.

3. Quantities; Releases

Unless otherwise expressly stated in the Order, if no other quantity is state on the face of the Order or if the quantity is blank or states the quantity as zero, "blanket", "as released", "each", "EA", "blanket", "as scheduled" or similar terms, then the Order is a requirements contract, and Seller shall supply, and Buyer shall purchase from Seller, Buyer's requirements for Goods in such quantities as identified by Buyer as firm orders or as otherwise authorized for fabrication by Seller specified in material releases, scheduling orders, or similar written instruction ("Releases"). Seller shall not fabricate or assemble any Goods, procure any materials or components, or ship Goods except to the extent authorized by such Releases. Releases are part of the Order, are governed by these Terms and are not independent contracts. Seller accepts the risk associated with lead times of various raw materials and/or components if such lead times are beyond those provided for in Releases. Any estimates of forecasts of future requirements of Goods or of production volumes or program durations, whether from Buyer or any Customer (as defined Section 27 below), are subject to change from time to time, with or without notice to Seller, and shall not be binding upon Buyer. Unless otherwise expressly stated in the Order, Buyer makes no representation, warranty, guaranty or commitment of any kind or nature, whether expressor implied, to Seller in respect of Buyer's quantitative requirements for the Goods or the term of the supply of the Goods.

4. Term

The Order is for a definite term. Subject to Buyer's termination rights, for Goods used by Buyer in or for the production of automotive parts or systems the agreement formed by the Order is binding on the parties for the length of the applicable vehicle program production life (including model refreshes as determined by the applicable original equipment manufacturer ("OEM")), of which Seller acknowledges and agrees it is aware, and both Buyer and Seller acknowledge the risk of the vehicle program production life being cancelled or extended by the OEM. To the extent that the Order lists Goods with distinct part numbers that are used in or for different vehicle production programs, the Order is binding on the parties for the length of the applicable vehicle program production life (including model refreshes as determined by the applicable OEM) to which each distinct part number relates. For example, if the Order lists Goods with distinct part numbers A and B, and the vehicle program to which the Goods with part number A ends in 0001and the vehicle program to which the Goods with part number B ends in 0003, then the Order will automatically terminate with respect to part number A in 0001 and, with respect to part number B, in 0003. If the Goods are not utilized by Buyer for the production of automotive parts or systems, the agreement formed by the Order will be binding for one year from the date the Order is transmitted to Seller. In such case, subject to Buyer's termination rights, the Order will automatically renew for successive one-year periods after the initial term unless Seller provides written notice at least 180 days prior to the end of the current term of its desire that the Order not be renewed. Notwithstanding the foregoing, if an expiration date is stated in the Order, the term of the Order will continue until that date. Unless specifically waived in writing by an authorized representative of Buyer, Seller's obligations with respect to service and replacement parts and Transition Support will survive the termination or expiration of the Order asset forth below.

5. Changes

Buyer may, at any time or from time to time, make or direct changes, or cause Seller to make changes, to the Goods under any Order or Order amendment, including, without limitation, changes in required quantities, design, drawings, specifications, applicable testing or quality control, methods of packing and shipment, the date or place of delivery or otherwise change the scope of work covered of an accepted Order. Any such change shall be binding only if made in writing and signed by Buyer. Seller will promptly make any such required change. In order for Seller to request a reasonable adjustment to the price or time for performance as a result of such change, Seller must notify Buyer of its request in writing within ten (10) days after receiving notice of the change and supply with its request all relevant information and documents necessary for Buyer to assess such request. Seller will, as requested by Buyer, promptly provide additional information to Buyer relating to any requested change in price or time for performance, including, without limitation, documentation of changes in Seller's cost of production and the time to implement such change. After receiving all requested information and documentation, Buyer may, in its sole discretion, determine an equitable adjustment in price or time for performance resulting from such changes. If Seller does not provide timely notice to Buyer that a requested change may result in a difference in price or time for performance, Buyer's requested change will not affect the price or time for performance. No adjustments to price or time for performance shall take effect for any change without an Order amendment issued by Buyer.

Seller will not make any change relating to Goods, including, without limitation, in the Goods' contents, design, specifications, processing, packing, marking, shipping, price, date or place of delivery, except at Buyer’s written instruction or with Buyer's written approval. Such prohibited changes include, without limitation, changing (i) any third party supplier to Seller of the services, raw materials or goods used by Seller in connection with its performance under the Order, (ii) any facility from which Seller and/or such third-party supplier operates and that relates in any way to the Goods, or to services, raw materials or goods used by Seller in connection with performance under the Order,(iii)the price of any Goods covered by the Order, (iv) the nature, type or quality of any services, raw materials or goods used by Seller in connection with the Order, (v) the fit, form, function, appearance or performance of any Goods covered by the Order, or (vi) the production method, or any process or software, or any production equipment used in the production or provision of, or as a part of, any Goods under the Order. Any changes by Seller to any Order or to the Goods covered by the order without the prior written approval of an authorized representative of Buyer shall constitute a breach.

6. Delivery

(a) Except as otherwise stated in the Order, Goods will be delivered by Seller DDP Buyer’s facility (Incoterms 2010).

(b) Time and quantities are of the essence. Delivery of Goods shall be on the date indicated in the Order or Release, as applicable, or as otherwise as requested by Buyer. Seller agrees to 100% on-time delivery of the quantities and at the times specified by Buyer in an Order or in Releases. If Seller has any reason to believe that it may not be able to meet the specified delivery date in an Order or Release for any reason, it shall immediately notify Buyer and, unless otherwise directed by Buyer, shall at its own expense take all steps required to eliminate or minimize any delay in delivery. Such notice, however, will not excuse Seller’s obligation to meet the required delivery time. Seller will pay any costs incurred by Buyer, including costs charged by any Customer to Buyer, because of Seller's failure to comply with shipping or delivery requirements. Buyer is not

obligated to accept early, late, partial, or excess deliveries. Goods which are delivered in advance of the specified date may, at the option of Buyer, either (a) be returned at Seller's expense for improper delivery, or

(b) be placed in storage for Seller's account, at Seller's cost, until the delivery date specified in the applicable Order or Release with payment withheld by Buyer until the date that the Products are actually scheduled for delivery. Buyer may, from time to time, change delivery schedules or direct temporary suspension of scheduled shipments.

(c) All Goods shall be suitably packed, marked and shipped in accordance the requirements of Buyer (or in the absence of specific requirements from Buyer, in such a manner to ensure that the Goods are not damaged during transit), the involved carriers and the countries of destination. Packing slips identifying the Order number, Release number, Buyer's part number, number of pieces in the shipment, number of containers in the shipment, Seller's name and number and the bill of lading number must accompany each shipment.

7. Over Shipments; Under Shipments.

Buyer will have no liability for payment of Supplier claims arising from Items delivered to Buyer that exceed the quantities specified in the Purchase Order. At the sole option of Buyer, Buyer may keep any over shipments of Items and elect to have the quantities of Items under the Purchase Order increased by the same number of Items as the quantity of over shipments. Alternatively, over shipments of any Items shall, if so, requested by Buyer, be returned to Supplier at Supplier's expense. In case of under shipments of any Items, Supplier shall, if so, requested by Buyer, immediately at its cost, ship the additional Items needed to fully complete the applicable Buyer's requirements to the destination and by the time designated by Buyer.

Alternatively, Buyer may elect to have the quantities of Items under the Purchase Order reduced by the same number of Items as the quantity of any under shipments.

8. Notification of Delay; Supplier Performance.

If at any time Supplier has reason to believe that the delivery of any Items may not be made in strict conformity with applicable delivery schedules, Supplier shall immediately notify Buyer setting forth the cause for the anticipated delay. Any oral communication shall be immediately confirmed in writing. During the period of any delay, Supplier shall use its best efforts to provide the Items called for in the Purchase Order from other sources and reduce its deliveries of Items to Buyer by such quantities of substituted Items, all without cost or liability to Buyer.

9. Payment

Payment terms are set forth in the Order. If the payment date is not specified in the Order, the payment term is Net 60 from delivery in accordance with the applicable Incoterm delivery term.

10. Risk of Loss and Title to Goods

Title will pass to Buyer at the time that risk of loss or damage to the Goods passes to the Buyer in accordance with the applicable Incoterm 2010 delivery term.

11. Samples.

Seller, at its expense, shall fabricate from production tooling and processes and furnish to Buyer the number of samples specified on the face of the Order, or if none is specified, a reasonable number of samples. Seller shall inspect such samples before delivery and shall certify inspection results in the manner requested by Buyer.

12. Electronic Data Interchange

Seller shall, at Buyer's request, connect to Buyer's electronic data interchange ("EDI") system and/or its web portal. Buyer shall have no liability whatsoever for any damages or loss alleged to have been suffered by Seller as a result of connection to or use of the EDI system, including without limitation in respect of loss of data or computer virus.

13. Quality and Inspection

(a) All Goods are subject to right of inspection and rejection by Buyer and Customers. Buyer may, however, rely on Seller's obligations and is not obligated to inspect goods prior to assembly or use. Neither Buyer's payment for nor Buyer's inspection of Goods, whether during manufacture, prior to delivery, or within a reasonable time after delivery, constitutes acceptance of any work-in-processor finished goods. Buyer's acceptance, inspection, or failure to inspect does not relieve Seller of any of its responsibilities or warranties. Nothing in the Order releases Seller from the obligation of testing, inspection and quality control. In addition to all of its other rights and remedies under the Contract or at law or in equity, Buyer may, in its sole discretion and at Seller's risk and expense, return non-conforming Goods to Seller at or hold them for a reasonable period of time and await Seller's disposal instructions. Goods returned by Buyer to Seller as defective or non-conforming shall not be returned to Buyer, whether reworked or otherwise modified, without Buyer’s approval. Neither assembly nor further use of Goods shall release Seller from its responsibility for non-conforming or defective Goods.

(b) Seller shall provide adequate and safe facilities for inspections requested by Buyer and Customer at Seller's facilities. Seller shall provide and maintain an inspection and process control system covering the Goods that is acceptable to Buyer and Customer(s). Records of all inspection work by Seller shall be kept complete and available to Buyer and Customer(s) during the performance of an Order and for at least five years after the end of serial production of the Goods.

(c) Seller will comply with Buyer's production part approval process ("PPAP") and will obtain all PPAP approvals at its own cost prior to any delivery of or payment for Goods.

14. Non-Conforming Goods

Any Good determined by Buyer to be non-conforming or defective may be rejected by Buyer. If defective Goods are shipped to and rejected by Buyer, the quantities under the Order will be reduced unless Buyer otherwise notifies Seller. Seller will not replace reduced quantities without a new Order or Release from Buyer.

In addition to other remedies available to Buyer:(i) Seller agrees to accept return of non-conforming or defective Goods, at Seller's risk and expense at full invoice price, plus transportation charges, and to replace such defective Goods as Buyer deems necessary; (ii) Buyer may have corrected at any time prior to shipment from Buyer's plant Goods that fail to meet the requirements of the Order; and/or (iii) Seller will reimburse Buyer for all costs and damages that result from any rejection or correction of defective Goods, including,

without limitation, those costs specified in Section 20(b) hereof. In addition, upon request of Buyer, Seller will provide a written description of corrective action taken to assure future compliance.

15. Remedial Work; Replacement Items

If any item or shipment of items is rejected as nonconforming to the Purchase Order by Buyer before the end of the Inspection Period ("Rejected Items"), Buyer shall have the following options:

Buyer may elect to have the quantity of Items under the Purchase Order reduced by the same amount as the quantity of Rejected Items; and Buyer will have no obligation to pay Supplier for such Rejected Items. Supplier will not replace Rejected Items without a new Purchase Order from Buyer. Rejected Items will be held by Buyer in accordance with Supplier's instructions and at Supplier's risk. Supplier's failure to provide instructions to Buyer within ten days (or such shorter period of time as may be commercially reasonable under the circumstances) after notice to Supplier by Buyer, shall entitle Buyer to charge Supplier for storage and handling and to dispose of the applicable Rejected Items without liability to Buyer.

16. Marking

Markings shall be in English, bar code, and such other form as requested by Buyer. Seller shall mark each package as described in the Supplier Requirements Manual.

17. Buyer and Seller's Information

(a) Seller shall keep confidential any technical, process, financial, commercial or other information of Buyer and its subsidiaries, affiliates, subcontractors, and Customers provided to Seller by or on behalf of Buyer, including, without limitation, pricing and other terms of the Contract, specifications, data, formulas, compositions, designs, sketches, photographs, samples, prototypes, test vehicles, manufacturing, packaging or shipping methods and processes and computer software and programs (including object code and source code, and any materials or information that contain or are based on any such information ("Buyer's Information"), and shall not disclose, directly or indirectly, Buyer's Information to any third party or any employee of Seller who does not have a need to know such information in order for Seller to supply the Goods here under except as specifically authorized in writing by Buyer. Seller shall not, directly or indirectly, use or permit Buyer's Information to be used for any purpose other than for supplying the Goods to Buyer here under without obtaining Buyer's prior written consent. Upon completion or termination of an Order, Seller shall promptly return to Buyer all materials incorporating any such Buyer's Information and any copies thereof. Seller shall not in any manner advertise or publish the fact that Seller has contracted to furnish Goods to Buyer or Customers.

(b) Seller will create, maintain, update, and provide to Buyer, in compliance with the drafting and math data standards of Buyer, all technical information about the Goods and their manufacture which is reasonably necessary or requested by Buyer or Customers in connection with the installation, assembly and use of the Goods, including, without limitation, the engineering validation and qualification of the Goods for automotive production and other applications and compliance with any legal or regulatory requirements. Any information

which the Seller has disclosed or may disclose to Buyer that relates to the Goods is acquired by Buyer free from any restrictions or claims (other than for patent infringement).

18. Intellectual Property Rights

(a) Definitions

"Intellectual Property Rights" means any patent, patented articles, patent applications, designs, industrial designs copy rights, software, source code, database rights, moral rights, inventions whether or not capable of protection by patent or registration, techniques, technical data, trade secrets, know- how, and any other proprietary right, whether registered or unregistered, including applications and registrations thereof, all related and continuing rights, and all similar or equivalent forms of protection anywhere in the world. Intellectual Property Rights excludes all brands, trademarks, tradenames, slogans and logos of Seller and Buyer unless specifically identified as a deliverable or work product of Seller pursuant to this Contract “Background Intellectual Property Rights" means any Intellectual Property Rights of either Buyer or Seller relating to the Goods contracted (i) existing prior to the effective date of this Contract or prior to the date Buyer and Seller began any technical cooperation relating to the Goods contracted, whichever is earlier, or (ii) that each party acquires or develops after these dates but in a strictly independent manner and entirely outside of any work conducted under this Contract.

"Foreground Intellectual Property Rights" means any Intellectual Property Rights, except Background Intellectual Property Rights, (i) that are developed in whole or in part by Buyer alone, by Buyer and Seller jointly or by Seller alone, in connection with this Contract or (ii) relating to the Goods contracted.

(b) Foreground Intellectual Property Rights

Buyer and Seller will each retain ownership of any Foreground Intellectual Property Rights that are solely created or made by the irrespective employees, agents or subcontractors ("Personnel"). Buyer and Seller will jointly own any Fore ground Intellectual Property Rights that are jointly created or made by Personnel of both Buyer and Seller with the ability to grant licenses without consultation and no duty of accounting to each other for any use or purpose. For clarity, unless an express written period of exclusivity has been promised to Buyer, Foreground Intellectual Property Rights owned or controlled by Seller may be immediately exploited by Seller in connection with its business with its other customers and will not be exclusive to Seller's performance of this Contract. Seller hereby grants to Buyer and causes its affiliates and Personnel to grant to Buyer, an irrevocable, worldwide, nonexclusive, perpetual to the maximum extent permitted by law, royalty free, fully paid-up license, with right to sublicense, to all Foreground Intellectual Property Rights to make, have made, use, reproduce, modify, improve, prepare derivative works of, distribute, display, perform, offer to sell, sell and import, without limitation.

(c) Background Intellectual Property Rights

Buyer and Seller will each retain ownership of their respective Background Intellectual Property Rights. Seller hereby grants to Buyer and causes its affiliates and Personnel to grant to Buyer, and Buyer hereby accepts, an irrevocable, worldwide, nonexclusive, royalty free, fully paid-up license, with right to sublicense to Buyer's affiliates, Customer(s) and subcontractors, to all Background Intellectual Property Rights to make, have made, use, reproduce, modify, improve, prepare derivative works of, distribute, display, perform, offer to sell, sell and import the Goods that are the subject of this Contract (the "Limited License"), provided that Buyer or its affiliates will only use this Limited License in the event that (i) Seller breaches or repudiates its obligations by being unable or unwilling to deliver Goods under this Contract, or (ii) in the event Seller is unable to supply Goods under this Contract as a result of a force majeure event, but in such event only for the duration of

Seller's inability to supply. In no event will the term of the Limited License extend beyond the expiration date of this Contract.

(d) Copyrights

To the extent that this Contract is issued for the creation of copyright able works, the works will be considered "works made for hire" for Buyer except to the extent that the works do not qualify as "works made for hire" for Buyer in which case Seller here by assigns to Buyer all right, title and interest in all copyrights and if lawfully permitted waives all moral rights therein.

(e) Right to Repair

For the avoidance of doubt, Buyer, its affiliates, subcontractors and Customer(s) have the right to repair, reconstruct, remanufacture, or rebuild the specific Goods delivered under this Contract without payment of any royalty to Seller.

(f) Miscellaneous

Goods manufactured based, in whole or in part, on Buyer's drawings, designs, and/or specifications or other Buyer-provided information as well as any software code or models provided by Buyer may not be used for Seller's own use or sold to third parties without Buyer's express written authorization.

Nothing in this Contract is an admission by Buyer of the validity of any Intellectual Property Rights claimed by Seller, including an admission that any license is required by Buyer to manufacture the goods or continue the services contracted. Seller will claim and acquire all rights and waivers of Seller's personnel required to enable Seller to grant Buyer the rights and licenses in this Contract. Seller assumes full and sole responsibility for compensating Seller's personnel for such rights and waivers, including the remuneration of employees.

Seller, on behalf of itself and Buyer, Customer(s) and its dealers will comply with all obligations with respect to software that forms any part of the Goods contracted, including obligations under any licenses.

Seller grants to Buyer, its subsidiaries and affiliates and customers an irrevocable, assignable, paid-up worldwide license under each right of Seller that is applicable to any intellectual property whatsoever furnished to Buyer in connection with the Goods. Title to any developments made by Seller while in performance of an Order which enhance or improve the Goods or Seller's products shall belong to Buyer unless agreed upon in

writing by both parties. The foregoing license is intended to be subject to11USC Section 365 (n) as an executory agreement under which Buyer has license rights in Seller's intellectual property.

19. Service and Replacement Parts

Seller will sell to Buyer the Goods necessary to fulfill Buyer's replacement parts requirements to Customer(s) at the then current production price(s) under the Order. If the Goods are systems or modules, Seller will sell the components or parts that comprise the system or module at price(s) that will not, in the aggregate, exceed the price of the system or module less assembly costs. Seller will also sell Goods to Buyer to fulfill Buyer's service and replacement parts requirements for Customer(s) during the fifteen (15) year period following the end of the production phase (the "Post-Production Period"), and the Order will remain in effect during the entire Post-Production Period. During the first five (5) years of the Post-Production Period, the price(s) for service Goods will be the production price(s) which were in effect at the commencement of the Post-Production Period. The price(s) for service Goods for the remainder of the Post-Production Period shall be as agreed by the parties. If requested by Buyer, Seller will also make service literature and other materials available at no additional charge to support Buyer's service activities. Seller agrees to maintain in good condition all tools and equipment necessary to produce Goods and all corresponding drawings, designs and manufacturing processes until the end of the Post-Production Period.

20. Warranties

(a) Seller warrants to Buyer and Customers, for the duration set forth in Section 17(c), that all Goods and any services provided under the Contract shall be: (i)merchantable; (ii) free from all defects in design, workmanship and materials; (iii)selected, designed (to the extent designed by Seller or any of its agent or representatives, even if the design has been approved by Buyer), manufactured and assembled by Seller based upon Buyer's stated use and fit and sufficient for the particular purposes intended by Buyer and Customers; (iv) conform strictly with specifications, samples, drawings, designs descriptions or other requirements (including performance specifications) furnished to or by Buyer; (v) free from all liens, claims and encumbrances whatsoever and (v) provided with due care. Any attempt by Seller to limit, disclaim, or restrict any such warranties or any remedies of Buyer, by acknowledgement or otherwise, in accepting or performing an Order, shall be ineffective. Buyer's approval of any design, drawing, material, process, or specifications will not relieve Seller of these warranties. The foregoing warranties are in addition to those available to Buyer at law. For all services, Seller further warrants that its work will be performed in a professional and workman like manner, consistent with all standards and specifications agreed on with Buyer and otherwise consistent with industry standards.

(b) Seller will conform to the quality control and other standards and inspection systems of Buyer and, as applicable, any Customer(s), including, without limitation, quality control policies, ISO-9001 and TS16949 quality certifications. Seller will also participate in supplier quality and development programs of Buyer and, as applicable, any Customer. Seller agrees to meet the full requirements of industry Production Part Approval Processes (PPAP) as specified by Buyer and Customer(s), as applicable, and agrees to present the required information to Buyer upon request at the PPAP level requested by Buyer.

(c) In the case of Goods supplied for use as, or incorporation into, parts, components or systems for automotive vehicles or other finished products, the warranty period will commence upon receipt of the Goods (or services) by Buyer and, except as provided in section 16(e) , end forty-eight (48) months following the date the vehicle or other finished product on which such parts, components or systems are installed is first sold and

delivered or otherwise utilized for consumer or commercial purposes, provided, however, that if Buyer offers and provides a longer warranty to any Customer(s) with respect to any such parts, components or systems, then such longer warranty period will apply to the Goods and services. In the case of Goods supplied for other uses, unless otherwise expressly agreed in writing by an authorized employee of Buyer, the warranty period will be the longer of (i) that provided by applicable law, or (ii) the length of the warranty that Seller offers to any of its other customers for the same of similar goods.

(d) If any Goods are determined by Buyer to be non-conforming or defective, Seller shall reimburse Buyer for all losses, costs and damages (including reasonable attorney and professional fees) caused by such non-conforming Goods, including, without limitation, those costs specified in Section 20(b) hereof.

(e) Notwithstanding the expiration of the warranty period set forth in these Terms, if Buyer or the manufacturer of the vehicles (or other finished product) on which the Goods, or any parts, components or systems incorporating the Goods, are installed, voluntarily or pursuant to a government mandate, makes an offer to owners of such vehicles to provide remedial action to address a defect that relates to motor vehicle safety or the failure of the vehicle to comply with any applicable laws, safety standard or guideline or otherwise implements a field service action or customer service campaign (collectively referred to hereafter as a "Recall"), the warranty shall automatically apply for such period of time as may be dictated by Customer(s) or the federal, state, local or foreign government where the Goods are used or provided.

21. Insurance and Indemnity

(a) Seller shall maintain and carry adequate insurance, on a commercially reasonable basis, on Seller plant(s) and equipment and tooling located at Seller's plant(s), for the full insurable value thereof, as well as comprehensive general liability insurance, including public liability, property damage liability, product liability, recall and contractual liability coverage, and workers' compensation and employees' liability insurance covering all employees engaged in the performance of any Order, all in amounts and with companies satisfactory to Buyer, acting reasonably. Liability coverage shall include completed products and operations coverage. Upon request from Buyer, Seller shall have Buyer named as an additional insured and loss payee on its insurance policies.

Seller shall, on Buyer's request, furnish certificates or other acceptable forms of proof of insurance confirming the foregoing coverages. The receipt or review of such certificates or other forms of proof of coverage by Buyer shall not relieve Seller from its insurance obligations hereunder or reduce or modify such insurance obligations. Seller's failure to comply with these provisions shall not reduce or relieve Seller from its obligations or liabilities hereunder. The certificate must certify that the required insurance is not canceled or materially changed until 30 days after written notice to the Buyer.

(b) If Seller's work under an Order involves operations by Seller on the premises of Buyer or any Customer, Seller shall take all necessary precautions to prevent the occurrence of any injury to persons or damage to property during the progress of such work.

(c) To the fullest extent permitted by law:(i) Seller assumes sole responsibility for any injury to any person (including, without limitation, death) or damage to any property of any kind or nature caused by, resulting from or in connection with furnished of the Goods by Seller, its subcontractors, officers, agents, representatives of employees;(ii) Buyer shall not be responsible for any injury to any person (including, without limitation, death) or damage to any property resulting from Seller's possession, use, misuse or failure of any Furnished Property (as defined in Section 22) or other property furnished to Seller by Buyer, and the use of any such property by Seller shall constitute acceptance by Seller of all responsibility for any claims for such injury or damage, and

(iii) Seller will defend, indemnify and hold harmless Buyer, Customers, and dealers and users of the products sold by Buyer (or the vehicles or other end-use application in which they are incorporated), and all of their respective agents, customers, invitees, subsidiaries, affiliates, successors and assigns, officers, directors and employees (collectively, the "Indemnified Parties") from and against all liability, claims, demands, losses, judgments, damages, expenses or costs (including, without limitation, reasonable attorneys' and other professional fees, settlements and judgments) (collectively, "Costs") arising out of, resulting from, or related to: (i) any actual or alleged non- conformance or defect in Goods supplied by Seller; (ii) any actual or alleged breach or failure by Seller to comply with (A) any of its representations, warranties or obligations under this Contract or (B) applicable laws; and (iii) any alleged or actual negligent or wrongful act or omission of any of the Indemnified Parties. Seller also will defend, indemnify and hold harmless Indemnified Parties from all Costs occasioned by, resulting from or arising out of: (i) any claim relating to the acts or omissions by Seller or its employees, agents or sub-contractors on Buyer's or any Customer's premises except to the extent liability for such Costs arises out of the sole negligence or willful misconduct of Buyer or Customer; and (ii) any claim of direct or contributory infringement or inducement to infringe of any proprietary right (including any patent, trademark, copyright, moral, industrial design or other proprietary rights, or misuse or misappropriation of trade secret) relating to the Goods covered by an Order (including, without limitation, their manufacture, purchase, use and/or sale) under any legal theory related to the Goods, including such claims where Seller has provided only part of the Goods, and Seller waives any claim against Buyer that any such infringement arose out of compliance with Buyer's or Customer's specifications. Seller's obligation to defend indemnify and hold harmless under this Section will apply regardless of whether the claim arises in tort, negligence, contract, warranty, strict liability or otherwise, except for claims that arise as a result of the sole negligence of Buyer. Buyer has the right to be represented by and actively participate through its own counsel in the defense and resolution of any indemnification matters, at Seller's expense. The indemnification obligations of Seller are independent of and in addition to any warranty and insurance obligations of Seller.

22. Termination for Convenience

Buyer may, at any time upon10 days prior written notice to Seller, terminate all or any part of an Order or Release for Buyer's convenience, at any time and for any reason, by giving such written notice to Seller. Upon receipt of notice of termination, and unless otherwise directed by Buyer, Seller will: (a) promptly terminate all work under the Order on the effective date of termination;(b) transfer title and deliver to Buyer the finished Goods, the work in process, and the parts and materials that Seller reasonably produced or acquired according to quantities ordered by Buyer and that Seller cannot use in producing goods for itself or for others; (c) verify and settle any claims by subcontractors for actual costs incurred directly as a result of the termination and ensure the recovery of materials in subcontractors' possession; (d) take actions reasonably necessary to protect property in Seller's possession in which Buyer has an interest until disposal instruction from Buyer has been received; and (e) upon Buyer's request, cooperate with Buyer in transferring the production of Goods to a different supplier, including as described in Section 21 below. Upon such termination, Buyer shall pay to Seller, in full satisfaction of any claim, only the following amounts, without duplication:(i) the Order price for all finished Goods in the quantities ordered by Buyer that conform to and are delivered in accordance with the applicable Order or Release, to the extent not previously paid; (ii) Seller's reasonable actual direct costs of merchantable and useable work in process and raw materials transferred to Buyer under subsection (b) above; (iii) Seller's reasonable actual costs of settling claims regarding its obligations to subcontractors required under the Order, to the extent directly caused by the termination, but limited to the amount of firm quantities of Goods and raw materials/components authorized in outstanding Releases issued by Buyer; (iv) Seller's reasonable actual cost of carrying out its obligation under subsection (d) hereof, and (v)if applicable, amounts due in

connection with Transition Support underSection21. Buyer shall not pay for finished Goods, work in process or raw materials fabricated or processed in excess of those in the terminated Order or Release (as applicable), for undelivered Goods which are Seller's standard stock, or which are readily marketable, or which are not promptly delivered to Buyer after request. Notwithstanding any other provision, Buyer will have no obligation for and will not be required to pay Seller, directly or on account of claims by Seller's subcontractors, for loss of anticipated profits, unabsorbed overhead, interest, development and engineering costs, tooling, facilities and equipment, rearrangement cost or rental, unamortized capital or depreciation, general administrative burden, finished goods, work-in-process or raw materials that Seller fabricates or procures in amounts exceeding those authorized in the Releases, or any other consequential costs or losses. Buyer's obligation upon termination under this Section will not exceed the obligation Buyer would have had to Seller in the absence of termination. Within 60 days after termination (or such shorter period as maybe required by Buyer or Customer), Seller shall provide Buyer with Seller's termination claim and all relevant information and documents necessary for Buyer to assess such request. Seller shall promptly furnish such supplemental and supporting information as Buyer shall request. Seller's failure to timely submit such a termination claim will result in such claim being waived. Buyer or its agent shall have the right to audit and examine all books, records, facilities, work, material, inventories, and other items before or after payment to verify amounts requested in Seller's termination claim. In the event of a termination of the Order by Buyer as a result of Buyer ceasing to be a supplier to the Customer for the vehicle program in respect of which Buyer issued the Order, Buyer shall only be obligated to compensate Seller for any costs under this Section if, when and to the extent that the Customer reimburses Buyer for such costs.

23. Termination for Cause, Default and Remedies

(a) Buyer may terminate all or any part of an Order or Release under the Contract without any liability to Seller or obligation to purchase raw materials, work-in-process or finished goods in any of the following events:(i) Seller repudiates, breaches, or threatens to breach any of the terms of the Contract, including Seller's warranties.

(ii) Seller is declared insolvent or bankrupt or makes a voluntary assignment or other arrangement for the benefit of creditors, is the subject of a filing for involuntary petition into bankruptcy or a receiver or trustee is appointed for Seller;(iii) Buyer reasonably determines, based on results of its rights to audit and review Seller and its operations and records here under, that Seller is or maybe likely to become insolvent or experience financial difficulties that could impact its performance under a Contract; (iv) if Buyer receives notice from Customer that Seller is no longer an acceptable supplier or subcontractor for the Goods; or (v) there occurs a Change of Control in the Seller. "Change of Control" means any sale or exchange of a sufficient number of securities, including as a result of a merger, amalgamation, consolidation, take-over bid or otherwise, of Seller or of any affiliate that controls Seller, to elect a majority of the board of directors or similar governing body of Seller or effect a change in management of Seller. Seller shall notify Buyer in writing within ten (10) days of any Change of Control of Seller.

(b) The rights and remedies reserved to Buyer under the Contract are cumulative with and in addition to all other or legal or equitable remedies. Upon the occurrence of an event identified in Section 20; Buyer may by written notice to Seller (without limiting any of the remedies available to Buyer) (i) terminate the whole or any part of an Order; and (ii) procure alternative goods or services upon such terms as it shall deem appropriate. Seller shall continue performance of an Order to the extent not terminated. Seller will reimburse Buyer for any and all incidental, consequential or other damages (including lost profits) caused or required by any of the events identified in Section 20(a), or by non-conforming or defective Goods, including without limitation costs, expenses and losses incurred directly or indirectly by Buyer or Customer(s) resulting from or in connection

with: (i) inspecting, sorting, storing, reworking, repairing or replacing the non-conforming Goods; (ii) line stoppage or production interruptions;(iii) a Recall, including, without limitation, the amounts paid to distributors and/or dealers for materials and replacement parts(including reasonable mark up to recover administrative costs or other capital expenses) and the labor costs to perform such work; (iv) off lining of vehicles or component systems, or (v) personal injury (including death) or property damage caused by the non-conforming or defective Goods. Buyer's damages include reasonable attorneys' fees and other professional fees, settlements and judgments incurred by Buyer and other costs associated with Buyer's administrative time, labor, and materials. If requested by Buyer, Seller will enter into a separate agreement for the administration or processing of warranty charge- backs for non-conforming or defective Goods and will participate in and comply with warranty reduction or related programs of Buyer or (to the extent directed by Buyer Customer(s) that relate to the Goods. In any action brought by Buyer to enforce Seller's obligations in connection with the production or delivery of Goods or transition support, or for possession of property, Seller acknowledges and agrees that monetary damages are not a sufficient remedy for any actual, anticipatory or threatened breach of the Contract and that, in addition to all other rights and remedies that Buyer may have, Buyer shall be entitled to specific performance and injunctive equitable relief as a remedy for any such breach, plus Buyer's reasonable attorneys' fees and professional fees. The rights and remedies of the Buyer provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or under an Order.

(c) In addition to any right of set off or recoupment provided by law, Buyer may set-off against or recoup from any amount due or to become due to Seller, in whole or in part, any amount due to Buyer or its subsidiaries or affiliates from Seller or its subsidiaries or affiliates. Buyer will provide Seller with a statement describing any offset or recoupment taken by Buyer.

23. Transition of Supply

Upon the expiration, cancellation, or termination of the Contract, in whole or in part, by either party for any reason, or Buyer's decision to change to an alternate source of Goods (including, without limitation, a Buyer-owned or operated facility) ("Alternative Supplier"), Seller will cooperate in the transition of supply, including, without limitation, the following transition support ("Transition Support"):(i) following termination, Seller will continue production and delivery of all Goods as ordered by Buyer at the prices and other terms of the Contract, without premium or other condition, during the entire period reasonably needed by Buyer to complete the transition to the Alternative Supplier(s), including, without limitation, at Buyer's request, providing a sufficient bank of Goods, such that Seller's action or inaction causes no interruption in Buyer's ability to obtain the Goods covered by the Order, such that Seller's action or inaction cause no interruption in Buyer's ability obtain Goods as needed; (ii) at no cost to Buyer, Seller (A) will promptly provide all requested information and documentation regarding and access to Seller's manufacturing process, including, without limitation, on-site inspections, bill-of-material data, tooling and process detail, and samples of Goods and component parts, (B) will provide all notices necessary or desirable for Buyer to resource production of the Goods to an Alternative Supplier, (C) when requested by Buyer, will return to Buyer all Furnished Property in as good condition as when received by Seller (reasonable wear and tear excepted); and (iii) subject to Seller's reasonable capacity constraints, Seller will provide special overtime production, storage, and/or management of extra inventory of Goods, extraordinary packaging and transportation and other special services as expressly requested by Buyer in writing.

If the transition occurs for reasons other than termination of Seller pursuant to Section 20, Buyer will, at the end of the transition period, pay the reasonable, actual cost of Transition Support as requested and incurred, provided that Seller has advised Buyer prior of its estimate of such costs prior to incurring such amounts and

has received Buyer approval for such costs. If the parties disagree on the cost of Transition Support, Buyer will pay the agreed portion to Seller and pay the dispute portion into escrow for disbursement by a court or arbitration tribunal.

25. Property Furnished by Buyer and Its Customers

Unless otherwise agreed in writing, all information, documents, tooling (such as fixtures, gauges, jigs, patterns, castings, cavity dies, molds, with all related appurtenances, accessions, and accessories), equipment or materials of every description furnished to Seller by Buyer either directly or indirectly to perform the Order or for which Buyer has agreed to reimburse Seller(s), and any replacement thereof, or any materials affixed or attached thereto ("Furnished Property"), shall be and remain the personal property of Buyer or Customer and shall be held by Seller or by a third party, to the extent that Seller has transferred possession of Buyer's Property to a third party with Buyer's permission, on a bailment basis as a bailee-at-will. To the extent that Buyer has agreed to reimburse Seller for Furnished Property, Seller must provide all required information as specified in the Supplier Requirements Manual. Seller is solely responsible for inspecting, testing and approving all Furnished Property prior to any use, and Seller assumes all risk of injury to persons or property arising from Furnished Property. Furnished Property will, at all times, be housed, maintained, repaired and replaced by Seller at Seller's expense in good working condition capable of producing Goods meeting all applicable specifications. Furnished Property shall be plainly marked or otherwise adequately identified by Seller as the property of Buyer or Customer and shall be safely stored separate and apart from Seller's property. Buyer may enter Seller's premises and inspect Furnished Property and all related records during normal business hours. Seller shall not substitute any of its own property for Furnished Property and shall not use Furnished Property except in filling an Order. Such property while in Seller's custody or control shall be held at Seller’s risk, shall be kept insured by Seller at Seller's expense in an amount equal to the replacement cost with loss payable to Buyer or Customer. Buyer and its affiliates have the right to take immediate possession of Furnished Property at any time without payment of any kind. Seller agrees to cooperate with Buyer if Buyer elects to take possession of Furnished Property. Effective immediately upon written notice to Seller, without further notice or legal action, Buyer has the right to enter the premises of Seller and take possession of all Furnished Property. Seller expressly waives any right to additional notice or process and agrees to provide Buyer or its nominee(s) with immediate access to Furnished Property. Seller grants to Buyer a limited and irrevocable power of attorney, coupled with an interest, to execute and record on Seller's behalf any notice financing statements with respect to Furnished Property that Buyer determines are reasonably necessary to reflect Buyer's interest in Furnished Property. At Buyer's request, Furnished Property will be immediately released to Buyer or delivered by Seller to Buyer or Customer in the same condition as originally received by Seller, reasonable wear and tear excepted, all at Seller's expense. Seller waives, to the extent permitted by law, any lien or other rights that Seller might otherwise have on any Furnished Property, including but not limited to molder's and builder's liens, or any liens or other rights that Seller might otherwise have on Furnished Property for work performed on such property, for the purchase price of Goods, or otherwise.

TO THE EXTENT PERMITTED BY LAW, BUYER SHALL HAVE NO LIABILITY TO SELLER OR ANYONE CLAIMING BY OR THROUGH SELLER FOR ANY INCIDENTAL OR CONSEQUENTIAL OR OTHER DAMAGES OF ANY KIND WHATSOEVER RELATING FURNISHED PROPERTY SUPPLIED BY BUYER. BUYER DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO SUCH FURNISHED PROPERTY, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS

FORA PARTICULARPURPOSE, AND SELLER WAIVES, FOR ITSELF AND ITS SUCCESSORS AND ASSIGNS, ALL CLAIMS OF NEGLIGENCE AND STRICT LIABILITY.

26. Seller's Tooling

Seller, at its own expense, shall furnish, keep in good condition, and replace when necessary all tooling, jigs, dies, gages, fixtures, molds, and patterns that are not Furnished Property ("Seller's Tooling") throughout the term of the Order and for a period of 15 years after production. The cost of changes to Seller's Tooling necessary to make design changes and specification changes authorized by Buyer in writing shall be paid for by Buyer. Buyer may inspect Seller's Tooling and production facilities during normal working hours upon reasonable notice to Seller. Seller shall insure Seller's Tooling with full fire and extended coverage insurance for the replacement thereof. Seller grants Buyer an irrevocable option to take possession of and title to Seller's Tooling that is special for the production of Goods upon payment to Seller of the book value thereof less any amounts the Buyer has previously paid to Seller for the cost of Seller's Tooling; provided, however, that this option shall not apply if Seller's Tooling is used to produce products that are standard stock of Seller. Seller grants Buyer a security interest in Seller's Tooling to secure Buyer's rights in Seller's Tooling.

27. Audit Rights

During the term of the Order and for an additional six (6) years after the final payment under the Order, Buyer, at its expense, shall have the right to audit and review all relevant information, including books, records, income statements, balance sheets, cash flow statements, payroll data, receipts and other related supporting data, including Seller's administrative and accounting policies, guidelines, practices and procedures, as well as correspondence, test results, other documents in order to (i) substantiate any charges and other matters under the Contract (ii) assess Seller's ongoing ability to perform its obligations under an Order, and (iii) assess Seller's compliance with the terms of the Order. Seller will maintain and preserve all such information and documents for a period of six (6) years following final payment under the Contract. In addition, all Goods, work, materials, inventories and other items provided for under or related to the Order must at all times be accessible to Buyer and to Buyer's authorized agents and representatives, including parts, tools, fixtures, gauges and models. Seller will provide Buyer with reasonable access to its facilities and otherwise cooperate and facilitate any such audits by Buyer.

28. Compliance with Laws

(a) Seller's performance of its obligations under an Order shall be incompliance with all applicable federal, provincial, state, municipal and local laws, ordinances, rules, codes, standards and regulations in the country of receipt, the country of shipment and the customer-identified country of destination, including but not limited to the United States Foreign Corrupt Practices Act, the Arms Export Control Act, the International Traffic in Arms Regulations, the Export Administration Act and the Export Administration Regulations (collectively, "Laws").

Seller shall furnish Buyer with certificates of compliance, where required under such applicable Laws or when requested by Buyer. Each invoice rendered to Buyer under an Order shall constitute written assurance by Seller that Seller has fully complied with all applicable Laws.

(b) Seller shall package, label and transport the Goods and their containers, in particular those which constitute a health, poison, fire, explosion, environmental, transportation or other hazard, in compliance with all applicable laws in effect in the place to which the Goods are shipped or as otherwise specified by Buyer. Upon request, Seller shall furnish Buyer with information regarding the ingredients of the Goods. Seller warrants that each chemical substance constituting or contained in the Goods sold is on the list of chemical substances compiled and published by the Administrator of the Environmental Protection Administration pursuant to the Toxic Substances Control Act(15U.S.C.Sec.2601et.seq.) as amended, and that the Goods are not hazardous under any applicable Laws except as clearly stated on the shipping and storage containers. Seller shall provide Safety Data Sheets upon delivery of Goods.

(c) Seller represents that: (i) neither it nor any of its subcontractors or suppliers will either engage in or permit substandard working conditions in the supply of the Goods under an Order, (ii) child labor or underage labor, as defined by applicable law, will not be utilized, (iii) it will not allow any form of forced or compulsory labor, (iv) workers, without fear of reprisal, intimidation or harassment, shall have the right to associate freely and join labor unions and workers' councils or to otherwise refrain from joining such organizations as they so choose, in accordance with applicable laws, (v) workers shall be protected against any form of harassment and discrimination in any form, including but not limited to gender, age, religion, disability and political beliefs, (vi) workers shall have a safe and healthy workplace that meets or exceeds all applicable standards for occupational health and safety.

(d) Upon request, Seller shall furnish Buyer with such written verification as Buyer deems necessary to certify the origin of any ingredients or materials in the Goods. Seller shall also promptly furnish to Buyer all documents and other information requested by Buyer so that Buyer may comply in a timely manner with all applicable Laws governing consumer protection, conflict minerals or similar materials or ingredients.

(e) Upon request, Seller shall furnish promptly certificates of local value added in accordance with applicable government regulations. Each January, Seller shall provide NAFTA certifications for Goods shipped the prior year, including Certificates of Origin.

29. Assignment and Non-Assignment

Seller shall not assign or subcontract any right or obligation under an Order without the prior written consent of Buyer. Buyer may assign its rights and obligations under the Order without Seller's prior written consent.

30. Customer Requirements.

(a)Seller agrees to comply with the applicable terms and conditions of any agreements (" Customer Terms") received by Buyer from a third party ("Customer"), or directly or indirectly applicable to Buyer, pursuant to which Buyer agrees to supply to its customer, or to incorporate into goods supplied to its customer, Goods purchased by Buyer from Seller. The terms "Customer" and "Customer Terms" also include, where applicable, the final equipment manufacturer of the goods or services into which the Goods are or will be incorporated, as well as any intermediate entities in the supply chain between Buyer's direct Customer and such final equipment manufacturer, and related terms and conditions of such Customers. Buyer may, in its discretion, supply Seller with information regarding Customer Terms. Seller will be responsible for ascertaining how such disclosed Customer Terms affect Seller's obligations under the Contract, and Seller will meet all such disclosed Customer Terms. In the event of a conflict between the Order or these Terms and the Customer Terms, Buyer will determine, in its sole and absolute discretion, which terms will supersede and apply to Seller. Seller will take all steps necessary to enable Buyer to comply with the Customer Terms, including, without limitation, cost and

productivity terms and price reductions. By written notice to Seller, notwithstanding Section 1(d) above, Buyer may elect to have the provisions of this Section prevail over any conflicting term of any Contract Document. (b) In the event that a Customer files or has filed against it a petition in bankruptcy or insolvency and, in the course of such proceeding and in connection with actual or threatened termination by the Customer of its contract(s) with Buyer (by rejection or otherwise), Buyer permits a reduction in the price(s) paid to Buyer for products incorporating the Goods, the price paid to Seller for the Goods from and after the date of such reduction will be automatically adjusted proportionally by the same percentage as the price paid to Buyer, and the Order will otherwise remain in effect without modification.

(c) If a Customer directed, required, recommended, requested, suggested or otherwise identified Seller as the source from which Buyer is to obtain the Goods ("Direct Supply Relationship"), then notwithstanding anything to the contrary in the Contract Documents, including the particular payment term:(1) in no event will Seller have a right to receive payment from Buyer for the Goods except following, and in proportion to Buyer's actual receipt of payment for those goods in which the Goods supplied by Seller are incorporated, and (2) any lengthening of applicable payment terms to Buyer will automatically lengthen the payment terms as between Buyer and Seller by an identical amount of time, and Buyer may, at its option and on notice to Seller, otherwise revise its payment terms for the Goods to take into account any other change in the payment terms of Buyer's Customer(s) for the Goods under the Contract; (3) within three business days of any change in price, specifications or other terms negotiated or proposed between Seller and Customer, Seller will notify Buyer in writing and will immediately adjust its invoices to reflect any price reduction, provided that no change will be binding on Buyer without Buyer's specific written consent;(4) (without limiting any other rights and remedies of Buyer)Seller will indemnify and hold harmless Buyer from any liabilities, claims, demands, losses, damages, costs and expenses (including without limitation attorneys' fees and other professional fees) incurred by Buyer arising from or relating to the Goods supplied by Seller- and including without limitation any charges or set-offs (including without limitation interim field service action cost recovery debits) taken by Customer against Buyer by reason of alleged defects in Goods, even if such set-offs by Customer are before final determination of (and subject to adjustment based upon) whether and to what extent defects in Goods were a cause of the related remedial action undertaken and related costs/damages incurred by Customer; (5) Seller will resolve all commercial issues (including pricing disputes), collection and/or insolvency risks of OEM and/or Seller, warranty charges, product liability claims, recalls, intellectual property matters and production interruptions arising from or relating to the Goods (except in each case to the extent caused by Buyer) directly and exclusively with Customer and Seller will indemnify and hold harmless Buyer for any of the foregoing matters; and (6) any debits claimed by Customer arising from or relating to the Goods will be passed through Buyer to Seller.

(d) If any requirement imposed by the Contract on Seller is found to be unenforceable or a gap otherwise exists or is created in the terms applicable to any Order through operation of law conflict in terms or otherwise, the corresponding requirement(s) of Customer shall be applicable to and binding on Seller for the benefit of Buyer. Seller acknowledges that it is familiar with the automotive industry and the applicable terms of Customer(s) that would apply in such event.

31. Governing Law and Disputes

The Contract shall be construed in accordance with the laws of the State of Michigan. The Convention on the International Sales of Goods shall not apply. In the event of any dispute arising from a Contract, the parties agree that they shall negotiate in good faith to resolve any such dispute. In the event such dispute is not resolved within 30 days upon receipt by one party of notice of a dispute, the parties agree to submit the matter to binding

arbitration in accordance with the Commercial Rules of Arbitration of the American Arbitration Association. The parties agree the arbitration shall occur in Oakland County in the State of Michigan. Notwithstanding the foregoing, the parties agree that Buyer may seek injunctive or other equitable relief from a competent court in any jurisdiction in order to protect its intellectual property rights and Confidential Information without submission to arbitration.

32. Severability

If any provision of a Contract is invalid or unenforceable under any statute, regulation, ordinance, executive order or other rule of law, such provision shall be deemed reformed or deleted, as the case may be, but only to the extent necessary to comply with such statute, regulation, ordinance, order or rule, and the remaining provisions of the Order shall remain in full force and effect.

33. Entire Agreement

Each Contract is a complete and exclusive statement of the terms of the parties' agreement with respect to the manufacture and supply of Goods under an Order. No course of prior dealings between the parties and no usage of the trade may be used by Seller to supplement or explain any term used in an Order. Except as otherwise provided herein, no amendments, subsequent terms, conditions, understandings or agreements purporting to modify the terms of the Contract will be binding unless in writing and signed by the authorized representatives of both parties.

34. Force Majeure

If Seller is unable to produce, sell or deliver any Goods or perform any services covered by the Contract, or Buyer is unable to accept delivery, buy or use any Goods covered by the Contract, as a result of an event or occurrence beyond the reasonable control of the affected party and without such party's fault or negligence, then any delay or failure to perform under the Contract that results from such event or occurrence will be excused for only so long as such event or occurrence continues, provided, however, that the affected party gives written notice of each such delay (including the anticipated duration of the delay) to the other party as soon as possible after the event or occurrence (but in no event more than seventy-two (72) hours thereafter). Such events and occurrences may include, by way of example and not limitation, natural disasters, fires, floods, windstorms, severe weather, explosions, riots, wars, sabotage and power failures. However, Seller's inability to perform as a result of or delays caused by Seller's insolvency or lack of financial resources will not excuse Seller's performance under the Contract. The change in cost or availability of materials or components based on market conditions, Seller or supplier actions, or contract disputes or any labor strike or other labor disruption applicable to Seller or any of its subcontractors or suppliers will not excuse Seller's performance under the Contract (under theories of force majeure, commercial impracticability or otherwise), and Seller assumes these risks. During any delay or failure to perform by Seller, Buyer may (a) purchase substitute goods or services from other available sources, in which case the quantities under the Contract will be reduced by the quantities of such substitute goods or services, without liability to Seller, and Seller will reimburse Buyer for any additional costs to Buyer of obtaining the substitute goods or services compared to the prices set forth in the Contract and/or (b) have Seller provide substitute goods or services from other available sources in quantities and at times Buyer requests and at the prices set forth in the Contract. If Seller fails to provide adequate assurances that any delay will not exceed thirty (30) days within forty-eight (48) hours of Buyer's request for such assurances, or if any delay lasts more than thirty (30) days, Buyer may terminate the

Contract without any liability to Seller whatsoever except for confirming Goods already delivered in accordance with an Order or Release. As soon as Seller anticipates or learns of any impending strike, labor dispute, work stoppage or other disruption at its facilities that might affect the delivery of Goods, Seller will produce (and, subject to the consent of Buyer and, if applicable, Buyer's customer, locate in an area that will not be affected by any such disruption) a finished inventory of Goods in quantities sufficient to ensure the supply of Goods to Seller for at least thirty (30) days after such disruption commences.

35. Relationship of Parties

The relationship between Buyer and Seller is that of independent contractors. Nothing contained in these Terms or any Contract will be construed to create a principal-agent or employer-employee relationship between the parties. Neither party will represent to others that it is the agent of the other nor have the authority to bind the other. Except as may be expressly set out herein in respect of a customer of Buyer, there are no third-party beneficiaries to an Order.

36. Ethical Standards

Seller's performance of its obligations under an Order shall be incompliance with the applicable provisions of the AirBoss Anti-Corruption Policy and Code of Business Conduct and Ethics and all ethical, social and environmental commitments that may be requested by a director in direct customer of Buyer. Seller shall not give or offer to give any direct or indirect gift or benefit to Buyer's employees or enter into any outside business relationship with Buyer's employees.

37. TSO/TATF Requirement

All AFP production part or production service suppliers must be registered to either ISO 9001-2015 or ISO/ IATF16949-2016. AFP's goal is for all of its suppliers to be ISO/ IATF16949 2016 registered. AFP encourages all of its suppliers to be committed to the protection of our environment through pollution prevention and to be ISO 14001 registered.

Dear Supplier/Service Provider:

Some technology, technical and other data, and parts to which your company may have access while working with AirBoss Defense Group, LLC 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 AirBoss Defense Group, LLC to obtain the agreement of its suppliers to comply with the same requirements that AirBoss Defense Group, LLC must observe for protecting CUI. AirBoss Defense Group, LLC 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, 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 (Oct 2016) and NIST 800-171.

1. Controlled Unclassified Information (CUI)

1.1. AirBoss Defense Group, LLC, 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.

1.2. 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 (https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html)as: Controlled Unclassified Information, Distribution Statements B through F, For Official Use Only, EAR/ITAR.

Contact your AirBoss Defense Group, LLC Sponsor for question on if information pertaining to a subcontract or service constitutes CUI.

1.3. 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 Section O Attachment 2.

1.3.1. 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

AirBoss Defense Group, LLC buyers point of contact, the AirBoss Defense Group, LLC service desk at (855) 532-3456, 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 General Dynamics Mission Systems as soon as practical.

1.4. 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 AirBoss Defense Group, LLC that require sharing of CUI.

1.5. 1.5 All DFARS compliance as described in this document are subject to audit and verification by AirBoss Defense Group, LLC.

We request that an authorized official execute this agreement on behalf of supplier/service provider and return it. Thank you.

Sincerely,

Edward Kiell, Vice President of Corporate Supply-Chain

ACKNOWLEDGED AND AGREED TO:

Supplier

By:_____

Printed Name:_____

Title:_____

Date: _____

Supplier Export Control Certification

Some of the technology, technical data, or parts to which your company will have access (or that your company will supply) while working with the AirBoss Defense Group, LLC Corporation family of companies are controlled for export under the International Traffic in Arms Regulations, 22 C.F.R. Parts 120-130 (the "ITAR") or the Export Administration Regulations, 15 C.F.R. Parts 730-774 (the "EAR"). Accordingly, we will share such controlled technology, technical data, or parts with your company subject to the following conditions:

1. Your company certifies that it is a company located in the United States.
2. Your company acknowledges that it may not export any ITAR- or EAR- controlled technology, technical data, services, or parts, except as authorized by the appropriate U.S. government agency.
3. Your company acknowledges that it may not disclose or transfer ITAR- or EAR-controlled technology, technical data, or services to non-U.S. persons, except as authorized by the appropriate U.S. government agency.
4. Your company certifies that it is registered or will register with the Directorate of Defense Trade Controls in accordance with 22 C.F.R. Part 122 if it manufactures or will manufacture ITAR-controlled defense articles.

We request that an authorized representative execute below and return a copy of this signed certification to the AirBoss Defense Group, LLC Corporation representative that sent it to you.

Questions about this form may be directed to Josh Rozier, Vice President of Contracts and Trade Compliance 912-346-7757 or Josh.Rozier@adg.com.

Thank you.

ACKNOWLEDGED AND CERTIFIED:

Supplier

Signature: _____

Printed Name: _____

Title: _____

Date: _____

U.S. Government Subcontractor Regulatory Alert

Supply Chain Cybersecurity Compliance - DFARS Interim Rule Released 09-30-20

252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

Please note, the following is for informational purposes only and not for purposes of providing legal advice. You should contact your attorney to obtain legal advice as needed.

This communication is to inform you of an interim rule (DFARS Case 2019-D041) – *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements*, the Department of Defense (DoD) published on September 30. The interim rule takes effect November 30, 2020 and will require immediate action by the DoD supply chain to be eligible to receive awards after the interim rule goes into effect.

Currently, pursuant to DFARS 252.204-7012, government suppliers must provide adequate security for covered contractor information systems. A "covered contractor information system" is defined as an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. More specifically, government suppliers must protect such information systems by implementing the security controls of National Institute of Standard and Technology (NIST) Special Publication (SP) 800-171.[1]

Beginning November 30, 2020, among other things, Contracting Officers must include the new DFARS 252.204- 7019 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 ADG 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 levelscores, 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.**

In addition, the contractor must insert the substance of DFARS 252.204-7020, including paragraph (g), in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of COTS.

---

[1] In accordance with NIST SP 800-171, suppliers should already be aware of the security requirements they have not yet implemented and have documented plans of actions for those requirements.

Accordingly, suppliers subject to this requirement should take the necessary steps for compliance and be prepared to provide ADG with a representation and certification of compliance upon request.

Overview of Interim Rule

The interim rule creates three new provisions and clauses:

- 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
- 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
- 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

Together, they implement two cybersecurity initiatives, the: (1) Cybersecurity Maturity Model Certification (CMMC) framework and (2) NIST SP 800-171 DoD Assessment Requirements.

The DoD is implementing a systematic, phased rollout of the CMMC requirements over five years, after which, it will apply to all DoD procurements, except for certain acquisitions such as those that are solely for COTS items. In FY2021, the DoD is expected to identify only 10 to 15 programs that will require CMMC. To the extent CMMC applies, the solicitation will include the required CMMC level and DFARS 252.204-7021 will be incorporated in the applicable contract and subcontract(s). It requires contractors subject to the CMMC requirement to have and maintain a current third-party CMMC certificate issued at the CMMC level required by the contract, and prior to making an award to a subcontractor, to ensure that the subcontractor has a current CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

Beginning November 30, 2020, the DoD will implement its other initiative, the NIST SP 800-171 DoD Assessment Requirements through the new provisions DFARS 252.204-7019 and DFARS 252.204- 7020. These provisions, and in particular, the impact of DFARS 252.204-7020 on supply chain, are discussed above in more detail.

Key Takeaways

To summarize and reinforce some important potential compliance impacts from the interim rule:

- Your company must immediately take steps to complete at least a Basic Assessment (or in the alternative, the Government has conducted a Medium or High Assessment) for all covered contractor systems relevant to your offer that are not part of an information system or service operated on behalf of the Government, and submit your company's summary level scores and other required information to SPRS if your company is subject to implementation of the NIST SP 800-171 security requirements in accordance with DFARS 252.204-7012.
- Contractors must insert the substance of DFARS 252.204-7020, including paragraph (g) titled "subcontracts," in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of COTS.
- It is important your company continue its CMMC readiness activities, be prepared to respond to inquiries regarding your CMMC readiness plan, and ensure that your suppliers are

aware of the CMMC effort and encourage them to become educated on it.

Additional Information

- The USG's Supplier Performance Risk System (SPRS) can be accessed here
- Additional information on CMMC and a copy of the CMMC model can be found here
- The interim rule can be found here

Thank you for your support. If you have any questions regarding cybersecurity and the DFARS 252.204-7020 provision related to ADG or its business units, please e-mail:

Jack.bergman@airbossofamerica.com

Table of Contents

Accordingly, suppliers subject to this requirement should take the necessary steps for compliance and be prepared to provide ADG with a representation and certification of compliance upon request.

Overview of Interim Rule

The interim rule creates three new provisions and clauses:

- 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements
- 252.204-7020, NIST SP 800-171 DoD Assessment Requirements
- 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement

Together, they implement two cybersecurity initiatives, the: (1) Cybersecurity Maturity Model Certification (CMMC) framework and (2) NIST SP 800-171 DoD Assessment Requirements.

The DoD is implementing a systematic, phased rollout of the CMMC requirements over five years, after which, it will apply to all DoD procurements, except for certain acquisitions such as those that are solely for COTS items. In FY2021, the DoD is expected to identify only 10 to 15 programs that will require CMMC. To the extent CMMC applies, the solicitation will include the required CMMC level and DFARS 252.204-7021 will be incorporated in the applicable contract and subcontract(s). It requires contractors subject to the CMMC requirement to have and maintain a current third-party CMMC certificate issued at the CMMC level required by the contract, and prior to making an award to a subcontractor, to ensure that the subcontractor has a current CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.

Beginning November 30, 2020, the DoD will implement its other initiative, the NIST SP 800-171 DoD Assessment Requirements through the new provisions DFARS 252.204-7019 and DFARS 252.204-7020. These provisions, and in particular, the impact of DFARS 252.204-7020 on supply chain, are discussed above in more detail.

Key Takeaways

To summarize and reinforce some important potential compliance impacts from the interim rule:

- Your company must immediately take steps to complete at least a Basic Assessment (or in the alternative, the Government has conducted a Medium or High Assessment) for all covered contractor systems relevant to your offer that are not part of an information system or service operated on behalf of the Government, and submit your company's summary level scores and other required information to SPRS if your company is subject to implementation of the NIST SP 800-171 security requirements in accordance with DFARS 252.204-7012.
- Contractors must insert the substance of DFARS 252.204-7020, including paragraph (g) titled "subcontracts," in all solicitations and contracts, with certain exceptions including solicitations or contracts solely for the acquisition of COTS.
- It is important your company continue its CMMC readiness activities, be prepared to respond to inquiries regarding your CMMC readiness plan and ensure that your suppliers are aware of the CMMC effort and encourage them to become educated on it.

Additional Information

- The USG's Supplier Performance Risk System (SPRS) can be accessed here
- Additional information on CMMC and a copy of the CMMC model can be found here

- The interim rule can be found here

Thank you for your support. If you have any questions regarding cybersecurity and the DFARS 252.204-7020 provision related to ADG or its business units, please e-mail jack.bergman@airbossofamerica.com

1) Background

a) Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, requires contractors and subcontractors to provide 'adequate security' to safeguard covered defense information, hereto referred to, for the purposes of this methodology, as Department of Defense (DoD) controlled unclassified information (CUI)[1], when residing on or transiting through a contractor's/subcontractor's internal information system or network, and to report cyber incidents that affect that system or network to DoD. DFARS clause 252.204-7012 further states that to provide adequate security, the Contractor shall implement, at a minimum, the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations. Contractors are also required to flow down DFARS Clause 252.204- 7012 to all subcontracts for operationally critical support, or for which subcontract performance will involve DoD CUI. Contractors must mark or otherwise identify, in accordance with direction contained within the specific contract, DoD CUI that is collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of performance of the contract.

b) DFARS provision 252.204-7008, Compliance with Safeguarding Covered Defense Information Controls, requires, among other things, offerors to represent they will implement the security requirements in NIST SP 800-171 in effect at the time the solicitation is issued or as authorized by the contracting officer. To document implementation of NIST SP 800-171, the contractor must develop, document, and periodically update a system security plan that describes system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. If implementation of the security requirements is not complete, companies must develop and implement plans of action to describe when and how any unimplemented security requirements will be met.

c) Under Secretary of Defense (Acquisition and Sustainment) (USD(A&S)) memorandum, "Strategically Implementing Cybersecurity Contract Clauses," dated February 5, 2019, directed the Defense Contract Management Agency (DCMA) to pursue, with companies for which they administer contracts, the application of a standard methodology and approach to assess a contractor's implementation of NIST SP 800- 171 at a strategic (corporate-wide) level as an alternative to the requirement for

[1] DoD is transitioning from the use of the term 'covered defense information' in the DFARS to "DOD Controlled Unclassified Information (CUI), consistent with DoDI 5200.48, Controlled

Unclassified Information (CUI)"

contractors to document implementation of NIST SP 800-171 on a contract-by- contract basis.

2) Purpose

   a) The *NIST SP 800-171 DoD Assessment Methodology, Version 1.2* documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171, a requirement for compliance with DFARS clause 252.204-7012.

   b) This methodology is used for assessment purposes only and does not, and is not intended to, add any substantive requirements to either NIST SP 800-171 or DFARS clause 252.204-7012.

   c) DoD will use this methodology to assess the implementation of NIST SP 800-171 by its prime contractors. Prime contractors may use this methodology to assess the implementation status of NIST SP 800-171 by subcontractors.

   d) This methodology informed the conduct of pilot *NIST SP 800-171 DoD Assessments* performed by DCMA, in partnership with the Defense Counterintelligence and Security Agency (DCSA) and the DoD Components, during 2019. DoD will update and codify this methodology in policy/regulation.

3) Strategically Assessing a Contractor's Implementation of NIST SP 800-171

   a) The *NIST SP 800-171 DoD Assessment Methodology* enables DoD to strategically assess a contractor's implementation of NIST SP 800-171 on existing contracts which include DFARS clause 252.204-7012, and to provide DoD Components with visibility to the summary level scores of strategic assessments completed by DoD, thus providing an alternative to the contract-by-contract approach.

   b) The *NIST SP 800-171 DoD Assessment* consists of three levels of assessments (see Section 4 of this document). These three types of assessments reflect the depth of the assessment, and the associated level of confidence in the assessment results.

   c) Assessment of contractors with contracts containing DFARS clause 252.204-7012 is anticipated to be once every three years unless other factors, such as program criticality/risk or a security-relevant change, drive the need for a different assessment frequency.

4) Levels of Assessment

   a) Basic (Contractor Self-Assessment) *NIST SP 800-171 DoD Assessment*

      i) The Basic Assessment is the Contractor's self- assessment of NIST SP 800-171 implementation status, based on a review of the system security plan(s) associated with covered contractor information system(s), and conducted in accordance with

NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and Section 5 and Annex A of this document.

ii) The Basic Assessment results in a confidence level of 'Low' in the resulting score because it is a self-generated score.

iii) The summary level scores resulting from Basic *NIST SP 800-171 DoD Assessments* should be documented as indicated in Section 6 and Annex B of this document.

b) Medium *NIST SP 800-171 DoD Assessment*

i) The Medium Assessment is conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment. It is anticipated that Medium Assessments will be conducted primarily by Program Management Office cybersecurity personnel, as part of a separately scheduled visit (e.g., for a Critical Design Review).

ii) The assessment will consist of a review of the system security plan description of how each requirement is met to identify any descriptions which may not properly address the security requirements.

iii) The Medium Assessment results in a confidence level of 'Medium' in the resulting score.

iv) The DoD assessor will document summary level scores resulting from Medium *NIST SP 800-171 DoD Assessments* as indicated in Section 6 of this document.

c) High (On-Site or Virtual) *NIST SP 800-171 DoD Assessment*

i) The High Assessment, conducted by DoD personnel who have been trained in accordance with DoD policy and procedures to conduct the assessment, requires a thorough on-site or virtual[2] verification/examination/demonstration of the Contractor's system security plan and implementation of the NIST SP 800-171 security requirements.

ii) The High Assessment is conducted using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information." The assessment will determine if the implementation meets the requirements by reviewing appropriate evidence and/or demonstration (e.g., recent scanning results, system inventories, configuration baselines, demonstration of multifactor authentication).

iii) An on-site High *NIST SP 800-171 DoD Assessment* is the preferred methodology for a full evaluation of the risk to DoD CUI because of the ability to verify and validate the effectiveness of the safeguards that implement security

[2] A virtual High Assessment was developed in response to the COVID-19 epidemic to allow protections

of assessors and DIB personal to limit travel and exposure of staffs whilst still being able to assess contractor risk. The government may utilize this methodology in the future as required in response to similar or other scenarios.

requirements defined in NIST Special Publication 800-171. While a High Assessment may be be conducted virtually in lieu of onsite, a virtual assessment will not fully cover all the NIST SP 800-171 requirements, resulting in a less than full understanding of overall risk.

iv) A virtual High Assessment utilizes the same methodology as the on-site with added data protections processes enacted to protect the DIB data that is shared with assessment teams. All data is transmitted through DoD Secure Access File Exchange (SAFE), is only reviewed locally on each assessor's computer (screen sharing is conducted utilizing DoD collaboration mediums that are approved for processing CUI) and contractor data is destroyed post assessment using NSA guidance for data destruction. With concurrence from the DIB companies being assessed, the assessment verifies and examines all documents utilizing the NIST SP 800-171A methodology minus the demonstration or testing of some requirements. In some cases, a follow-up on-site assessment of the items not assessed may be required or requested.

v) The first step in a High Assessment is for the contractor to conduct a Basic Assessment and submit results to the Department using the procedures in Annex B of this document. The High Assessment consists of a review of the Basic Assessment, a thorough document review and discussion with the contractor regarding the results to obtain additional information or clarification as needed, combined with government validation that the security requirements have been implemented as described in the system security plan. Network access by the assessor(s) is not required.

vi) The High Assessment results in a confidence level of 'High' in the resulting score.

vii) The DoD assessor will document summary level scores resulting from High *NIST SP 800-171 DoD Assessments* as indicated in Section 6 of this document.

5) *NIST SP 800-171 DoD Assessment* Scoring Methodology

a) This scoring methodology is designed to provide an objective assessment of a contractor's NIST SP 800-171 implementation status. With the exception of requirements for which the scoring of partial implementation is built-in (e.g., multi- factor authentication, security requirement 3.5.3) the methodology is not designed to credit partial implementation.

b) Conduct of the *NIST SP 800-171 DoD Assessment* will result in a score reflecting the net effect of security requirements not yet implemented. If all security requirements are implemented, a contractor is awarded a score of 110, consistent with the total number of NIST SP 800-171 security requirements. For each security requirement not met, the associated value is subtracted from 110. The score of 110 is reduced by each requirement not implemented, which may result in a negative score.

c) While NIST SP 800-171 does not prioritize security requirements, certain requirements have more impact on the security of the network and its data than others. This scoring methodology incorporates this concept by weighting each security requirement based on the impact to the information system and the DoD CUI created on or transiting through that system, when that requirement is not implemented.

d) Weighted requirements include all of the fundamental NIST SP 800-171 'Basic Security Requirements' - high-level requirements which, if not implemented, render ineffective the more numerous 'Derived Security Requirements'; and a subset of the 'Derived Security Requirements'- requirements that supplement the Basic Security Requirements - which, if not implemented, would allow for exploitation of the network and its information.

   i) For security requirements that, if not implemented, could lead to significant exploitation of the network, or exfiltration of DoD CUI, 5 points are subtracted from the score of 110. For example, failure to limit system access to authorized users (Basic Security Requirement 3.1.1) renders all the other Access Control requirements ineffective, allowing easy exploitation of the network; failure to control the use of removable media on system components (Derived Security Requirement 3.8.7) could result in massive exfiltration of CUI and introduction of malware.

      (1) Basic Security Requirements with a value of 5 points include 3.1.1, 3.1.2, 3.2.1, 3.2.2, 3.3.1, 3.4.1, 3.4.2, 3.5.1, 3.5.2, 3.6.1, 3.6.2, 3.7.2, 3.8.3, 3.9.2, 3.10.1, 3.10.2, 3.12.1, 3.12.3, 3.13.1, 3.13.2, 3.14.1, 3.14.2, and 3.14.3.

      (2) Derived Security Requirements with a value of 5 points include 3.1.12, 3.1.13, 3.1.16, 3.1.17, 3.1.18, 3.3.5, 3.4.5, 3.4.6, 3.4.7, 3.4.8, 3.5.10, 3.7.5, 3.8.7, 3.11.2, 3.13.5, 3.13.6, 3.13.15, 3.14.4, and 3.14.6.

   ii) For Basic and Derived Security Requirements that, if not implemented, have a specific and confined effect on the security of the network and its data, 3 points are subtracted from the score of 110. For example, failure to limit access to CUI on system media to authorized users (Security Requirement 3.8.2) or failure to encrypt CUI stored on a mobile device (Security Requirement 3.1.19), put the CUI stored on the system media or mobile device at risk, but not the CUI stored on the network itself.

      (1) Basic Security Requirements with a value of 3 points include 3.3.2, 3.7.1, 3.8.1, 3.8.2, 3.9.1, 3.11.1, and 3.12.2.

      (2) Derived Security Requirements with a value of 3 points include 3.1.5, 3.1.19, 3.7.4, 3.8.8, 3.13.8, 3.14.5, and 3.14.7.

   iii) All remaining Derived Security Requirements, if not implemented, have a limited or indirect effect on the security of the network and its data. For these, 1 point

is subtracted from the score of 110. For example, failing to prevent reuse of identifiers for a defined period (Security Requirement 3.5.5) could allow a user access to CUI to which they were not approved.

e) Two Derived Security Requirements can be partially effective even if not completely or properly implemented, and the points deducted should be adjusted depending on how the security requirement is implemented.

   i) Multi-factor authentication (MFA) (Security Requirement 3.5.3) is typically implemented first for remote and privileged users (since these users are both limited in number and more critical) and then for the general user, so 3 points are subtracted from the score of 110 if MFA is implemented only for remote and privileged users; 5 points are subtracted from the score of 110 if MFA is not implemented for any users.

   ii) FIPS validated encryption (Security Requirement 3.13.11) is required to protect the confidentiality of CUI. If encryption is employed, but is not FIPS validated, 3 points are subtracted from the score of 110; if encryption is not employed, 5 points are subtracted from the score of 110.

f) Although not common, future revisions of NIST SP 800-171 may add, delete or substantively revise security requirements. When this occurs, a value will be assigned to any new or modified requirements in accordance with this scoring methodology.

g) The contractor must have a system security plan (Basic Security Requirement 3.12.4) in place to describe each covered contractor information system, and a plan of action (Basic Security Requirement 3.12.2) in place for each unimplemented security requirement to describe how and when the security requirement will be met.

   i) Since the NIST SP 800-171 DoD Assessment scoring methodology is based on the review of a system security plan describing how the security requirements are met, it is not possible to conduct the assessment if the information is not available. The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'

   ii) Plans of action addressing unimplemented security requirements are not a substitute for a completed requirement. Security requirements not implemented, whether a plan of action is in place or not, will be assessed as 'not implemented.' For example, if the initial roll-out of 3.5.3, multifactor authentication, is only 75% complete, and there is a plan of action still being implemented, 3.5.3 will be considered 'not implemented', as the requirement has not been fully implemented.

   iii) A lack of plan of action for unimplemented security requirements will result in Security Requirement 3.12.2 being assessed as 'not implemented.'

h) Temporary deficiencies and/or isolated enduring exceptions which occur during initial implementation, or arise after implementation, are to be expected in most complex environments.

   i) Temporary deficiencies that are appropriately addressed in plans of action (i.e., include deficiency reviews, milestones, and show progress towards the implementation of corrections to reduce or eliminate identified vulnerabilities) should be assessed as 'implemented.' For example, when a plan of action addresses a 'temporary deficiency' that arises after implementation (e.g., 3.13.11, employ FIPS validated cryptography, had been implemented, but subsequently a patch invalidated the FIPS validation of a particular cryptographic module), the requirement will be scored 'as implemented.' A 'temporary deficiency' may also arise during initial implementation of a NIST SP 800-171 requirement if, during roll-out, specific issues with certain equipment is discovered that has to be separately addressed (e.g., certain specific hardware or software unexpectedly needs to be changed for the requirement to be successfully applied). If the implementation roll-out has otherwise been completed, this 'temporary deficiency' plan of action would be considered, and the requirement scored 'as implemented.' There is no standard duration for which a 'temporary deficiency' may be active. It is what is reasonable, which would take into consideration the availability of the solution, the cost and time to implement, the overall risk and whether any mitigations are applied in the interim. Generally, deficiencies should be resolved as soon as is reasonably possible.

   ii) Isolated enduring exceptions encountered during implementation, such as unique equipment or environments (e.g., specialized manufacturing equipment or a unique laboratory environment) may prevent the implementation of certain security requirements. Isolated enduring exceptions are typically not suitable to address in plans of action, but when described, along with any mitigations, in the system security plan such exceptions should be assessed as 'implemented.'

i) For certain requirements, questions often arise on whether or not they are actually implemented. These situations are addressed below:

   i) Security Requirements 3.1.12, 3.1.16, 3.1.18: Companies commonly do not allow remote access, wireless access or connection of mobile devices and may indicate these requirements as 'Not Applicable' or 'Not Implemented' in the system security plan. The evaluator should not deduct points in such cases. However, if the company disallows use of remote, wireless, or mobile access, they should also have a policy and procedure in place to insure these capabilities are not enabled inadvertently. This should be discussed as part of the Medium-

Level assessment, and if such policy and procedures are not in place a point should be assessed.

ii) Security Requirement 3.13.8: When implementing this requirement, encryption, though preferred, is not required if using common-carrier provided Multiprotocol Label Switching (MPLS), as the MPLS separation provides sufficient protection without encryption.

iii) Security Requirement 3.13.11: Cryptography used to protect the confidentiality of CUI must be FIPS-validated, which means the cryptographic module has to have been tested and validated to meet FIPS 140-1 or -2 requirements. Simply using an approved algorithm (e.g., FIPS 197 for AES) is not sufficient - the module (software and/or hardware) used to implement the algorithm must be separately validated under FIPS 140. Note however, that this is required when encryption is required for protection, which is typically external to the contractor's covered information system (assuming the system meets NIST SP 800-171). Cryptography used for other purposes within the protected information system need not be FIPS validated. When required, if encryption is not employed (FIPS validated or otherwise), 5 points are subtracted from the score of 110. If encryption is employed, but is not FIPS validated, 3 points are subtracted from the score of 110. Isolated use of non-FIPS validated cryptography, with an associated Plan of Action, should be treated as a temporary deficiency and assessed as 'implemented.'

j) If a contractor received a favorable adjudication from the DoD CIO indicating that a requirement is not applicable or that an alternative security measure is equally effective in accordance with DFARS 252.204-7008 or 7012, the DoD CIO assessment should be included in the Contractor's system security plan. Implemented security measures adjudicated by the DoD CIO as equally effective, and security requirements approved by the DoD CIO as 'not applicable,' will be assessed as 'implemented.' Once DOD CIO assessments approving "not applicable" requirements or "alternative security measures" are included in the Contractor's system security plan, the contractor does not need to submit that documentation for every current contract with the DFARS 252.204-7012 clause unless specifically requested to do so by the contracting officer. When completing the Basic (Contractor Self-Assessment) NIST SP 800-171 DoD Assessment Results Format, the contractor shall score any security requirements for which an assessment of "not applicable" or "alternative security measures" was previously approved by DoD CIO as 'implemented'.

k) A template illustrating the application of this scoring methodology is provided at Annex A of this document.

l) DoD will provide medium and high assessment results to the Contractor and offer the opportunity for rebuttal and adjudication of assessment results. Upon completion of

each assessment, the assessed contractor has 14 business days to provide additional information to the assessment team, to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

6) Documenting *NIST SP 800-171 DoD Assessment* Results

a) A summary level score for basic assessments completed by the Contractor, and for medium and high assessments conducted by DoD, will be posted in the Supplier Performance Risk System (SPRS) to provide DoD Components with visibility to the results of strategic assessments.

i) SPRS is defined by DoD Instruction (DoDI) 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information, October 15, 2019 available at https:\\www.esd.whs.mil/DD/.

ii) SPRS is the authoritative source to retrieve supplier and product performance information for the DoD acquisition community to assess and monitor unclassified performance, and to assess corporate business practices related to DoD contracts and the supplier's management of risk.

b) Assessment results posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI), available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500079p.PDF?v er=2019-10-15-115609-957. Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own results in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

c) A contractor may post the results of their Basic Assessments conducted in accordance with Section 5 and Annex B of this document in SPRS (via the Procurement Integrated Enterprise Environment (PIEE)).

d) DoD will post the following Medium and/or High *NIST SP 800-171 DoD Assessment* results to SPRS for each system security plan assessed:

i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC) or Commercial and Government Entity (CAGE) Code).

iii) Each system security plan assessed, mapped to the specific industry CAGE code(s) associated with the information system(s) addressed by the system security plan. All corporate CAGE codes must be mapped to all appropriate

system security plan(s) if the contractor has more than one system security plan and CAGE code. Additionally, a brief description of the system security plan architecture may be required if more than one plan exists.

iv) Date and level of the assessment, i.e., basic, medium, or high.

v) Summary level score (e.g., 105 out of 110), but not the individual value assigned for each requirement.

vi) Date a score of 110 is expected to be achieved (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

e) Department policy/procedures/guidance will be updated to direct acquisition/procurement officials and contractors to access SPRS to determine if a strategic assessment has been conducted.

f) DoD Components should rely on assessment results posted in SPRS in lieu of including requirements to assess implementation of NIST SP 800-171 on a contract- by-contract basis.

g) A High *NIST SP 800-171 DoD Assessment* may result in documentation in addition to that listed in 6) d) of this document. DoD will retain and protect any such documentation as For Official Use Only (FOUO) and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

7) Glossary of Terms

a) Enduring exception. Remediation is not feasible; no plan of action required; must be documented within a system security plan.

b) Temporary deficiency. Remediation of deficiency is feasible; known fix is in process; requires a plan of action. For the purposes of a DoD NIST SP 800-171 DoD Assessment, a 'temporary deficiency' is not based on an 'in progress' initial implementation of the requirement. A temporary deficiency arises after implementation. A Temporary deficiency may also apply during the initial implementation of a NIST SP 800-171 requirement if, during roll-out, specific issues with certain equipment is discovered that has to be separately addressed.

Annex A - *NIST SP 800-171 DoD Assessment* **Scoring Template**

- The following template illustrates the scoring methodology described in Section 5. If all requirements are met, a score of 110 is awarded. For each requirement not met, the associated value is subtracted from 110. Consistency results from the fact that the assessments are based on what is not yet implemented, or document that all requirements have been met.
- It is important to note an assessment is about the extent to which the company has implemented the requirements. It is not a value judgement about the specific approach to implementing – in other words, all solutions that meet the requirements are acceptable. This is not an assessment of one solution compared to another.
- Scoring for Basic, Medium, and High *NIST SP 800-171 DoD Assessments* is the same.
- While NIST does not prioritize requirements in terms of impact, certain requirements do have more impact than others. In this scoring methodology security requirements are weighted based on their effect on the information system and DoD CUI created on or transiting that system.

NIST SP 800-171 DoD Assessment **Scoring Template**

Security Requirement		Value	Comment
3.1.1*	Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).	5	
3.1.2*	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	5	
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1	
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1	
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	3	
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1	
3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	1	
3.1.8	Limit unsuccessful logon attempts.	1	

Security Requirement		Value	Comment
3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1	
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	1	
3.1.11	Terminate (automatically) a user session after a defined condition.	1	
3.1.12	Monitor and control remote access sessions.	5	Do not subtract points if remote access not permitted
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	5	Do not subtract points if remote access not permitted
3.1.14	Route remote access via managed access control points.	1	
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1	
3.1.16	Authorize wireless access prior to allowing such connections.	5	Do not subtract points if wireless access not permitted
3.1.17	Protect wireless access using authentication and encryption.	5	Do not subtract points if wireless access not permitted
3.1.18	Control connection of mobile devices.	5	Do not subtract points if connection of mobile devices is not permitted
3.1.19	Encrypt CUI on mobile devices and mobile computing platforms	3	Exposure limited to CUI on mobile platform
3.1.20*	Verify and control/limit connections to and use of external systems.	1	
3.1.21	Limit use of portable storage devices on external systems.	1	
3.1.22*	Control CUI posted or processed on publicly accessible systems.	1	
3.2.1	Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	5	

Security Requirement		Value	Comment
3.2.2	Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	5	
3.2.3	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	1	
3.3.1	Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	5	
3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	3	
3.3.3	Review and update logged events.	1	
3.3.4	Alert in the event of an audit logging process failure.	1	
3.3.5	Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	5	
3.3.6	Provide audit record reduction and report generation to support on-demand analysis and reporting.	1	
3.3.7	Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	1	
3.3.8	Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	1	
3.3.9	Limit management of audit logging functionality to a subset of privileged users.	1	
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	5	

Security Requirement		Value	Comment
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	5	
3.4.3	Track, review, approve or disapprove, and log changes to organizational systems.	1	
3.4.4	Analyze the security impact of changes prior to implementation.	1	
3.4.5	Define, document, approve, and enforce physical and logical access restrictions associated with changes to organizational systems.	5	
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	5	
3.4.7	Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	5	
3.4.8	Apply deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	5	
3.4.9	Control and monitor user-installed software.	1	
3.5.1*	Identify system users, processes acting on behalf of users, and devices.	5	
3.5.2*	Authenticate (or verify) the identities of users, processes, or devices, as a prerequisite to allowing access to organizational systems.	5	
3.5.3	Use multifactor authentication (MFA) for local and network access to privileged accounts and for network access to non-privileged accounts.	3 to 5	Subtract 5 points if MFA not implemented. Subtract 3 points if implemented for remote and privileged users, but not the general user
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1	
3.5.5	Prevent reuse of identifiers for a defined period.	1	
3.5.6	Disable identifiers after a defined period of inactivity.	1	

Security Requirement		Value	Comment
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1	
3.5.8	Prohibit password reuse for a specified number of generations.	1	
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1	
3.5.10	Store and transmit only cryptographically-protected passwords.	5	Encrypted representations of passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords
3.5.11	Obscure feedback of authentication information.	1	
3.6.1	Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	5	
3.6.2	Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	5	
3.6.3	Test the organizational incident response capability.	1	
3.7.1	Perform maintenance on organizational systems.	3	
3.7.2	Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.	5	
3.7.3	Ensure equipment removed for off-site maintenance is sanitized of any CUI.	1	
3.7.4	Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	3	
3.7.5	Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.	5	

Security Requirement		Value	Comment
3.7.6	Supervise the maintenance activities of maintenance personnel without required access authorization.	1	
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	3	Exposure limited to CUI on media
3.8.2	Limit access to CUI on system media to authorized users.	3	Exposure limited to CUI on media
3.8.3*	Sanitize or destroy system media containing CUI before disposal or release for reuse.	5	While exposure limited to CUI on media, failure to sanitize can result in continual exposure of CUI
3.8.4	Mark media with necessary CUI markings and distribution limitations.	1	
3.8.5	Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.	1	
3.8.6	Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.	1	
3.8.7	Control the use of removable media on system components.	5	
3.8.8	Prohibit the use of portable storage devices when such devices have no identifiable owner.	3	
3.8.9	Protect the confidentiality of backup CUI at storage locations.	1	
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	3	
3.9.2	Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	5	
3.10.1*	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5	
3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	5	

Security Requirement		Value	Comment
3.10.3*	Escort visitors and monitor visitor activity.	1	
3.10.4*	Maintain audit logs of physical access.	1	
3.10.5*	Control and manage physical access devices.	1	
3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1	
3.11.1	Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI.	3	
3.11.2	Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.	5	
3.11.3	Remediate vulnerabilities in accordance with risk assessments.	1	
3.12.1	Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.	5	
3.12.2	Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems.	3	
3.12.3	Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.	5	
3.12.4	Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems.	NA	The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'
3.13.1*	Monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems.	5	

Security Requirement		Value	Comment
3.13.2	Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.	5	
3.13.3	Separate user functionality from system management functionality.	1	
3.13.4	Prevent unauthorized and unintended information transfer via shared system resources.	1	
3.13.5*	Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	5	
3.13.6	Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).	5	
3.13.7	Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunneling).	1	
3.13.8	Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.	3	
3.13.9	Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.	1	
3.13.10	Establish and manage cryptographic keys for cryptography employed in organizational systems.	1	
3.13.11	Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.	3 to 5	Subtract 5 points if no cryptography is employed; 3 points if mostly not FIPS validated
3.13.12	Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.	1	

Security Requirement		Value	Comment
3.13.13	Control and monitor the use of mobile code.	1	
3.13.14	Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.	1	
3.13.15	Protect the authenticity of communications sessions.	5	
3.13.16	Protect the confidentiality of CUI at rest.	1	
3.14.1*	Identify, report, and correct system flaws in a timely manner.	5	
3.14.2*	Provide protection from malicious code at designated locations within organizational systems.	5	
3.14.3	Monitor system security alerts and advisories and take action in response.	5	
3.14.4*	Update malicious code protection mechanisms when new releases are available.	5	
3.14.5*	Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.	3	
3.14.6	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	5	
3.14.7	Identify unauthorized use of organizational systems	3	

* Basic safeguarding requirements and procedures to protect covered contractor information systems per Federal Acquisition Regulation (FAR) clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

Annex B - Basic (Contractor Self-Assessment) NIST SP 800-171 DoD Assessment Results Format

- Score your implementation of the security requirements in NIST SP 800-171 based on Section 5 and Annex A of this document.
- Document your Basic (self) NIST SP 800-171 DoD Assessment score in Supplier Performance Risk System (SPRS). A Procurement Integrated Enterprise Environment (PIEE) account with a SPRS "Cyber Vendor" role will be required to enter Basic Assessment information into SPRS. This role may be requested through PIEE.
- Information required for entering results of a Basic NIST SP 800-171 DoD Assessment into SPRS include:
  - Date of the assessment
  - Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement)
  - Scope of the Basic Assessment - Identify each system security plan (security requirement 3.12.4) supporting the performance of this contract. All company CAGE codes must be mapped to the appropriate system security plan(s). Additionally, a brief description of the plan architecture may be required, if more than one plan exists.
    - Select Open CAGE Hierarchy to choose CAGEs covered by the system security plan.
    - Note: if a CAGE does not appear in the hierarchy, update your company's records in the System for Award Management (SAM); ensure immediate/ highest level owner CAGEs are correctly indicated. SPRS will normally be updated within 24 hours.
  - Plan of Action Completion Date – date that a score of 110 is expected to be achieved for each system security plan assessed (i.e., all requirements implemented) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171 (security requirement 3.12.2).
- Informational links include:
  - PIEE Landing Page: https://wawf.eb.mil/piee-landing/
  - Information on requesting access via PIEE may be found here: https://www.sprs.csd.disa.mil/access.htm
  - Information on entering Cyber assessment scores into SPRS may be found here: https://www.sprs.csd.disa.mil/reference.htm
  - SPRS Homepage: https://www.sprs.csd.disa.mil/default.htm