1 General Applicability and Compliance Requirements

1.1 This Supplement sets out minimum cybersecurity requirements applicable to Seller and must be fulfilled for any Products or Services that are provided by Seller to Buyer. Seller must also comply with requirements set forth in the Addendum relating to Electronic Access to Buyer Systems (Addendum A).

1.2 Seller is responsible for taking any and all necessary measures and steps to comply with the requirements in this Supplement and Addendum A.

1.3 Buyer reserves the right to ask for documentation and evidence, as well as to perform a compliance audit, in order to determine whether the listed requirements are fulfilled or to assess the security of Seller's Product or Services. Seller must provide documentation and evidence within 24 hours following a request from Buyer.

1.4 The requirements set forth in this Supplement and Addendum A apply to data in all forms, whether electronic, printed or written, and for all Products and Services that use or support Buyer-owned data, systems, network or applications, including those in development, test or production.

1.5 To the extent that this Supplement and Addendum A contain the terms "including," "include," "in particular," "such as," or similar expressions, they shall be construed as illustrative and shall not limit the sense of the words preceding those terms.

1.6 This Supplement or Addendum A may be modified or amended from time to time. Any such modifications or amendments will be applicable from the date of the respective modification or amendment as indicated in new releases which shall, however, not be earlier than the actual release date.

1.7 Seller's violations or failure to comply with the requirements in this Supplement or Addendum A will result in a material breach of the Contract.

2 Definitions

These definitions apply in this Supplement and Addendum A:

"Access Control" means the process of granting or denying specific requests to obtain and use Information and related Information processing services, to access Buyer System and to enter specific facilities.

"BEMSID" means Boeing Electronic Messaging System Identifier, a unique identifier assigned to every Buyer Computing Device end user.

"Buyer" means the entity of The Boeing Company, its affiliates, divisions, or wholly owned subsidiaries that is a party to the Contract.

"Buyer System(s)" means Information Systems or Computing Devices owned or operated by Buyer or a third party on behalf of Buyer.

"Computing Device" means any desktop or laptop computer, mobile device (e.g., cellular phone, smartphone, tablet), server and/or storage device, real or virtual, that (a) is involved in the performance of the Contract, (b) may be used to access Buyer's network or an environment, or (c) may access or store Buyer information.

"Contract" means any agreement between Buyer and Seller to which this Supplement and Addendum A applies.

"Cybersecurity Vulnerability(ies)" means any bug, software defect, design flaw, or other issue with software associated with a Product that could adversely impact the confidentiality, integrity or availability of information or processes associated with the Product.

"Electronic Access" means the authority and ability to access and make use of Buyer Systems, including Networks or environments owned or operated by Buyer or a third party on behalf of Buyer.

"Information" means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

"Information System(s)" means any system, including development, test, stage and production systems, or storage/backup systems, that may access, process or store Buyer information.

"Malware" means any malicious hardware, firmware or software that is included or inserted in a system.

"Network" means any Buyer networks to which Seller is provided access in connection with the performance of services under the Contract and/or any Seller networks that are used to access sensitive information or information systems.

"Product(s)" means any goods, services, software and deliverables supplied under the Contract.

"Security Controls" means those security controls in Section 3 of this Supplement.

"Security Incident" means any actual or suspected (a) misappropriation or unauthorized access to or accidental or unlawful destruction, loss, alteration, unauthorized disclosure of Buyer information, including Sensitive Information, (b) unauthorized access to or compromise of Seller Systems, or (c) theft, loss or damage to Seller Systems or assets.

"Seller" means the entity identified in the Contract who contracts with Buyer and includes Seller's representatives, agents, successors, and permitted assigns and includes any subcontractor or supplier engaged by Seller in relation to this Supplement.

"Seller System(s)" means Information Systems or Computing Devices owned or operated by Seller or a third party on behalf of Seller.

"Sensitive Information" means Information that is collected, processed, maintained, used, shared, or disseminated in connection with the Contract that requires protection to ensure its confidentiality, integrity and availability, including any Buyer or Seller proprietary information and third-party proprietary Information (identified as such in the Contract), personal information, Covered Defense Information as defined in DFARS 252.204-7012, and Controlled Unclassified Information (CUI) as defined in the National Archives and Records Administration (NARA) Registry.

"Services" means work or functional services ancillary to the supply of Products to be performed by Seller for Buyer as specified in the Contract.

3 Minimum Security Controls

Seller shall:

3.1 In addition to maintaining cybersecurity management standards[1], apply reasonable and appropriate administrative, technical, physical, organizational, and operational safeguards, including complying with the following minimum International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 (2022) controls set forth below and, to the extent that there

[1] Examples of cybersecurity management standards include ISO/IEC 27001, NIST 800-53, and NIST 800-171.

are conflicts or inconsistencies between the requirements in this Supplement or Addendum A and the ISO/IEC 27001 controls, the more stringent requirement shall prevail;

Minimum Required ISO/IEC 27001 Controls
5.9 Inventory of information and other associated assets
5.11 Return of assets
5.14 Information transfer
5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
5.19 Information security in supplier relationships
5.22 Monitoring, review, and change management of supplier services
5.26 Response to information security incidents
5.35 Independent review of information security
5.36 Compliance with policies, rules, and standards for information security
6.3 Information security awareness, education and training
7.1 Physical security perimeter
7.2 Physical entry
7.3 Securing offices, rooms and facilities
7.5 Protecting against external and environmental threats
7.12 Cabling security
8.1 User end point devices
8.2 Privileged access rights
8.3 Information access restriction
8.5 Secure authentication
8.7 Protection against malware
8.8 Management of technical vulnerabilities
8.15 Logging
8.20 Networks security
8.22 Segregation of networks
8.24 Use of cryptography
8.31 Separation of development, testing and operational environments
8.26 Application security requirements
8.33 Test information

3.2 Deploy multiple layers of defense on Seller Systems to protect Sensitive Information against accidental and unlawful destruction, alteration, and unauthorized or improper disclosure or access, including firewalls, network intrusion detection, and host-based intrusion detection systems. All security monitoring systems including firewalls and intrusion detection systems must be monitored 24 hours per day, 365 days per year;

3.3 Employ the latest, commercially available, anti-Malware, antivirus and malicious code detection and protection products on all Seller Systems, including networks, workstations and servers used to provide services under the Contract;

3.4 Implement Data Loss Prevention (DLP) controls (e.g. DLP software, disabling USB ports, and URL/web filtering) to detect and prevent compromise or unauthorized removal of Buyer data, including Sensitive

Information, from Seller Systems and networks. Ports/services on Seller Systems that are not used should be disabled;

3.5 To the extent that Seller uses Active Directory, follow the latest Microsoft best practices for security;

3.6 Establish and enforce security configuration settings for information technology products employed in Seller Systems based on any one or more of the guidelines listed below:

3.6.1 National Institute of Standards and Technology (NIST) National Checklist Program

3.6.2 Center for Internet Security (CIS) Benchmarks

3.6.3 U.S. Government Configuration Baselines (USGCB)

3.7 Transmit Buyer data, including Sensitive Information, using compatible, encrypted protocols that protect the transfer of information, such as the latest version of TLS encryption;

3.8 Prohibit the processing, transmission, or storage of Buyer data, including Sensitive Information, on Seller personnel's personal accounts or personally owned Information System or Computing Device;

3.9 Maintain a formal, clearly-defined, and written information security policy in accordance with technical standards for protecting the confidentiality, integrity, and availability of Information and Information System and provide Buyer with a copy of the policy within 24 hours following a request from Buyer;

3.10 Designate a security professional to serve as a point of contact for Buyer for questions or communications relating to Seller cybersecurity activities under this Supplement; and

3.11 Apply the following additional controls to Seller Systems that involve access to or the transmission, storage, or processing of Buyer data or Sensitive Information:

a. limiting access to authorized users, processes acting on behalf of authorized users, or devices;

b. limiting access to the types of transactions and functions that authorized users are permitted to execute;

c. verifying and restricting connection to and use of other Information Systems;

d. controlling Information posted or processed on publicly accessible Information Systems;

e. identifying Information System users, processes acting on behalf of users, or devices;

f. authenticating the identities of those users, processes, or devices, as a prerequisite to allowing access to Seller System;

g. implement controls to terminate inactive sessions and restrict the connection times of idle/inactive sessions on Information Systems, network devices and applications;

h. remote access to Seller Systems and Seller's network must be approved and restricted to authorized personnel through secure access control protocols, strong encryption, authentication, and authorization;

i. sanitizing or destroying Information containing Sensitive Information before disposal or release for reuse;

j. limiting physical access to Seller Systems to authorized individuals;

k. escorting visitors and monitoring visitor activity, maintaining audit logs of physical access, and controlling and managing physical access devices;

l. implementing subnetworks for publicly accessible system components that are physically or logically separated from internal networks;

m. identifying, reporting, and correcting Information and Seller System flaws in a timely manner; and

n. performing periodic scans of Seller System and real-time scans of files from external sources as files are downloaded, opened, or executed.

4 Logging

Seller shall:

4.1 Maintain audit logs from Seller Systems as well as network devices, and applications for a minimum period of 12 months from the time of event or logging;

4.2 Store log files on a centralized logging server with sufficient details in order to assist in the identification of the source of an issue and enable a sequence of events to be recreated;

4.2.1 Logs must record date and time, user or service account, and IP address/hostname for all access and authentication attempts;

4.2.2 At the very least, log data must capture information system, network device and application security related event information, alerts, failures, and errors.

4.3 Integrity of logs files must be maintained and protected from tampering by restricting access to systems that store log files.

4.4 Logs must be continually monitored, reviewed and analyzed for suspicious and unauthorized activity and to verify the integrity of the logging process.

5 Personnel Security and Training

Unless otherwise prescribed in the Contract, Seller shall:

5.1 Upon request from Buyer, provide documentation detailing Seller's personnel screening process, criteria, and any changes or variations to Seller's personnel screening process;

5.2 Maintain a complete list of all Seller personnel with permission to access Buyer Systems, networks, applications, and their employment location;

5.3 Perform pre-employment screening, consistent with local laws and regulations, for all Seller personnel who will access, store, process or transmit Buyer's Sensitive Information;

5.4 Ensure that Seller personnel performing under the Contract receive annual cybersecurity awareness and training from Seller and provide associated training records to Buyer within seven (7) days following Buyer's request; and

5.5 Upon termination of employment, promptly remove Seller personnel access to Seller Systems, including networks and applications, and any Buyer Systems, networks, and applications, or other equipment used to support the Contract. Seller will also remind personnel that they must not retain any Sensitive Information.

6 Cybersecurity Compliance and Attestations

Seller shall:

6.1 contact Buyer Supply Chain Cybersecurity at suppliercybersecurity@boeing.com for access sponsorship to the online cybersecurity questionnaire;

6.2 complete the cybersecurity questionnaire on or before the date of the Contract;

6.3 update the cybersecurity questionnaire no less than every two years and following any significant change in Seller's security posture or any Security Incident;

6.4 conduct Seller System and network reviews or audits, including vulnerability assessments, no less than annually;

6.5 remediate, retest, and document Seller System and network vulnerabilities, gaps, or flaws found during an assessment within 30 days of identification;

6.6 provide Buyer with copies of reviews or audit reports, and remediation efforts described in Section 6.5 of this Supplement within 24 hours following a request from Buyer, including:

6.6.1 Seller records, procedures, and information relating to the security of Seller System, including all facilities where maintenance, storage or backup activities are performed; and

6.6.2 reports, summaries, and other materials relating to information security reviews or audits conducted by Seller or a third party within the past year, including the status of any remediation or corrective action plans. Covered reviews or audits may include vulnerability , network or host scans (including security policy implementation, configurations, patching, listening ports, and protocols), and penetration testing.

7 Security Incident Notification

Seller shall:

7.1 Have documented Security Incident response procedures that, at minimum, covers the reporting, analysis, monitoring, and resolution of security incidents, and is updated annually;

7.2 Notify Buyer within 24 hours following awareness, notification, or discovery of an actual or suspected Security Incident;

7.2.1 Notice to Buyer shall include whether Buyer information was accessed or lost and be sent to abuse@boeing.com, copying all related emails to Buyer's Authorized Procurement Agent, and reported to the Boeing Computing Security Operations Center by phone 1 888-373-7501, if Seller's email is not available;

7.2.2 Seller shall also:

a. immediately investigate any Security Incident;

b. make all reasonable efforts to secure Sensitive Information and mitigate the impact of the Security Incident;

c. provide timely and relevant Information to Buyer about the Security Incident on an ongoing basis; and

d. cooperate as applicable with Buyer to provide notice to affected third parties.

7.3 Promptly but no later than 72 hours following a Security Incident and request from Buyer, provide a copy of any Security Incident reports, including indicators of compromise and, if applicable, detailed lists of affected or impacted Sensitive Information, Buyer data, Buyer Systems, or other details agreed to by Buyer and Seller.

7.4 Not make or permit any statements concerning Security Incidents involving Buyer data, including Sensitive Information, Buyer Systems or other assets to a third-party without the written authorization of Buyer, unless provided to law enforcement or compelled by legal process;

7.5 Notify Buyer within 24 hours following receipt of a request by a third-party to provide access to Buyer data or Sensitive Information in connection with a Security Incident.

8 Business Continuity and Recovery.

8.1 Seller shall maintain and regularly update a comprehensive business continuity and recovery plan with detailed steps and procedures to be followed in the event of a cyber incident or any other disruptive event.

8.2 Seller's business continuity and recovery plan shall include:

8.2.1 strategies to minimize downtime, restore critical systems and data, and ensure the continuity of services to Buyer;

8.2.2 robust data backup and recovery plans to protect Buyer data, including data relating to products and services to be provided to Buyer, from loss, corruption, or unauthorized access;

8.2.3 regular backups of all systems, applications, and data used to provide products or services under the Contract. This includes securely storing backup copies and periodic testing of data restoration procedures. Backups must be performed at an appropriate frequency with sufficient redundancy;

8.2.4 encryption of Buyer information, including Sensitive Information, that is stored in backups using AES-256-bit or higher encryption or other strong encryption standard depending on backup method. Where applicable, backups that leave Seller's facilities must be protected against unauthorized access, misuse or corruption during transportation and storage.

8.3 In the event of a data loss incident, Seller shall promptly restore Buyer's data to the agreed-upon service levels and inform Buyer in accordance with Section 7 of this Supplement;

8.4 A copy of Seller's business continuity and data recovery plan shall be available within 24 hours following Buyer's request.

9 Indemnity

Seller shall indemnify, defend, and hold harmless Buyer and its respective officers, directors, shareholders employees, subcontractors, agents, suppliers and assignees from and against any and all third-party liabilities, obligations, losses, claims, damages, costs, charges, and other expenses of any kind, including attorneys' fees and legal expenses that arise out of or relate to (a) any failure by Seller, or its personnel or supply chain, to comply with any obligation under this Supplement or (b) the breach of any representation and warranty herein. Buyer may participate in the defense and settlement of any claim for which it is entitled to indemnification hereunder, using attorneys selected by Buyer.

10 Disclaimer and Exclusion of Liability

Seller hereby:

10.1 waives, releases and renounces all warranties, obligations and liabilities of Buyer, and rights, claims and remedies of Seller against Buyer, expressed or implied, arising by law or otherwise; and

10.2 acknowledges that Buyer has no obligation or liability in contract or tort for loss of use, revenue or profit or for any incidental or consequential damages.

11 Miscellaneous

11.1 This Supplement does not relieve Seller of any other applicable safeguarding requirements, remedies, or obligations regarding the protection of Sensitive Information required by the Contract or local, federal, state, or other governmental agencies or departments, including FAR 52.204-21 and DFARS 252.204-7012.

11.2 Any Seller access, communications or data transiting or stored on a Buyers Information Systems, networks or applications may be monitored, intercepted, recorded, or searched at any time and for any lawful purpose, and may be used or disclosed for any lawful purpose;

11.3 Seller shall provide prior written notification of material changes to any Seller System that affect Seller's compliance with this Supplement, including any new third-party agreements that will store, process or transmit Buyer's Sensitive Information on behalf of Seller.

11.4 Any regulatory change affecting the subject matter of this Supplement shall be treated in accordance with the "compliance with laws" provisions of the Contract.

11.5 In the event of any conflict or inconsistency between this Supplement or Addendum A and any other document forming part of the Contract, the provision with the more stringent requirement shall prevail.

11.6 Seller shall ensure all Buyer Sensitive Information is immediately removed from Seller-managed Computing Devices of those Seller personnel who are no longer involved with performance of the Contract.

11.7 Seller shall return, erase or destroy all Buyer Sensitive Information on completion or early termination of the Contract in accordance with NIST SP 800-88, Guidelines for Media Sanitization, or Buyer instructions.

11.8 Seller acknowledges that Buyer's Supplement for the Security of Personal Data[2] (or Buyer approved equivalent) applies when any personal data is shared further to the Contract.

[2] See www.boeingsuppliers.com/terms.html

Addendum A: Electronic Access to Buyer System.

1 Access Right

1.1 In connection with Seller's support of the Contract, Buyer may provide, at its sole discretion, a limited, nontransferable, and revocable right for Electronic Access to Buyer System during the term of the Contract. Such access is granted solely for purposes of performing work under the Contract, and only for the systems, applications, and data authorized by Buyer.

1.2 Any Seller access, communications, or data transiting or stored on Buyer Systems, networks or applications may be monitored, intercepted, recorded, or searched at any time and for any lawful purpose, and may be used or disclosed for any lawful purpose.

2 Electronic Access to Buyer System

Seller shall ensure that each person who has Electronic Access is aware of their individual responsibilities and of Seller's obligations under the Contact including:

2.1 limiting access to those persons directly supporting Seller's work under the Contract;

2.2 performing additional background screening may be required for some access levels;

2.3 maintaining Buyer Electronic Access credentials in confidence;

2.4 following all Buyer Access Controls issued by Buyer or anyone acting on Buyer's behalf; and

2.5 using only Seller-managed or Buyer-managed Computing Devices when connecting to a Buyer network.

3 Managing Electronic Access to Buyer System

Seller shall:

3.1 designate an access request point of contact to manage Seller's access needs, Buyer questions, and communications relating to Seller Electronic Access to Buyer System;

3.2 review access every 90 days and identify persons who no longer are working on the Contract, promptly request Buyer in writing to remove any accounts assigned to these persons, and within 30 days of Buyer's request provide copies of reconciliation records for validation by Buyer; and

3.3 notify promptly Buyer in writing of the name and BEMSID of any person who is reassigned, leaves their employment, or is terminated for cause.

4 Seller-Managed Computing Devices

In addition to the requirements outlined in the Supplement, Seller shall ensure that Seller managed Computing Devices have:

4.1 patched and current operating systems and applications;

4.2 up-to-date anti-virus/anti-Malware protection installed and running with the latest signature files;

4.3 up-to-date software firewalls installed, running, and configured to limit ports/protocols to only those necessary to support Seller's statement of work (software firewalls are required even when a local hardware firewall or enterprise firewall is used);

4.4 multifactor authentication to access or unlock Seller managed computing devices; and

4.5 full encryption using AES-256-bit or higher encryption where Buyer data is stored on Seller Systems, including personnel laptop/desktop computers, servers, or mobile devices.

5 Prohibited Acts

Seller, and any person acting on Seller's behalf, shall not, in any circumstance:

5.1 remove or otherwise modify or disable any Security Controls on Seller or Buyer managed Computing Devices connecting to Buyer System;

5.2 share Buyer Electronic Access credentials with any other person;

5.3 introduce non-approved or malicious code or software into Buyer System;

5.4 use Buyer System for non-Buyer business purposes;

5.5 negligently disrupt Buyer System;

5.6 access or attempt to access any Buyer Information where access has not been authorized;

5.7 access or attempt to access any restricted portions of a Buyer network or Buyer System;

5.8 modify or remove any restrictive markings from Buyer information;

5.9 add or connect any Computing Device to a Buyer System not specifically authorized by Buyer;

5.10 deliver (or attempt to deliver) any software or code to Buyer unless and until such software or code is governed by a contract that contains all usual requirements including those for assessments prior to delivery, delivery of code without defects that exceed the Common Vulnerability Scoring System (or equivalent) score of medium or higher, provision of current vulnerability scoring and remediation of defects following the earlier of self-discovery, public disclosure or Buyer notification;

5.11 save or transfer any Buyer data or materials from Buyer System unless stipulated by Buyer in the Contract;

5.12 employ, run, or use any data mining, automated code, scripts, software, or scraper tools, robots, or similar data gathering and extraction methods unless stipulated by Buyer in the Contract; or

5.13 access Buyer System through any mechanism other than the authorized Access Controls stipulated by Buyer in the Contract.

6 Seller Acknowledgment

Buyer may terminate or block access to Buyer System without notice or cause.