## Section A: Definitions

"Raytheon Sensitive Information" includes any information in any form or medium, including derivative documents created by Seller relating to Raytheon, for which Seller is required to maintain confidentiality under an agreement with Raytheon.

## Section B: Additional Information Security Obligations for Raytheon Sensitive Information

1. **Information Security Program.** Seller's Security Plan shall be approved by its management and shall be designed to:

   a. Protect the confidentiality, security, integrity, and availability of all Raytheon Sensitive Information in Seller's possession or control or to which Seller has access;

   b. Protect against any anticipated threats or hazards to the confidentiality, security, integrity, and availability of Raytheon Sensitive Information;

   c. Protect against unauthorized or unlawful access, acquisition, use, disclosure, alteration, or destruction of Raytheon Sensitive Information;

   d. Implement and maintain written information security policies, controls, and procedures that incorporate the above requirements and that are consistent with generally accepted industry standards and practices ("Information Security Program");

   e. Protect against accidental loss or destruction of, or damage to, Raytheon Sensitive Information;

   f. Comply with other requirements of the Agreement and such additional security requirements as Raytheon and Seller may from time-to-time agree upon; and

   g. Provide appropriate training to its employees regarding its Information Security Program and protection of Raytheon Sensitive Information.

   Upon request of Raytheon, Seller further agrees to provide Raytheon with any information reasonably requested by Raytheon regarding Seller's Information Security Program, provided, however, that Seller is under no obligation to provide any information to Raytheon that Seller reasonably determines the disclosure of which would pose a security risk to Seller or its other customers.

2. **Email Security Requirements**

   Seller agrees and acknowledges that Raytheon requires Raytheon Sensitive Information to be maintained securely and to be encrypted using industry standard encryption methods if sent via email.

3. **Information Security Incidents**

   a. **Notification of Security Incidents.** If an event occurs whereby Seller believes, or reasonably believes, that Raytheon Sensitive Information has been actually or potentially disclosed to, or accessed or acquired by, an unauthorized individual or individuals ("Security Incident"), Seller shall notify Raytheon in writing promptly, but not later than seventy-two (72) hours after the event is discovered.

      Except as may be required by applicable law, Seller agrees that it will not inform any third party (excluding law enforcement) of any Security Incident without first obtaining Raytheon's prior written consent.

   b. **Investigation of Security Incidents and Remedial Actions.** Seller agrees to cooperate with Raytheon to investigate the Security Incident, and to preserve all information and evidence relating to the Security Incident (including, without limitation, by suspending routine overwriting or deletion of data or log files). In addition and without limiting the foregoing, upon Raytheon's written request, Seller

agrees to retain a mutually acceptable competent and objective third party to investigate the scope and cause of the Security Incident. In such case, Seller agrees to permit the third party to disclose any information and evidence to Raytheon related to the Security Incident; provided, however, the third party shall not disclose any data owned by Seller's other customers that is subject to a confidentiality or non-disclosure obligation.

d. **Costs Related to Security Incidents.** To the extent such Security Incident is caused by acts or omissions of Seller, Seller agrees to 1) bear all costs and expenses related to the investigation, including if necessary, retaining a mutually acceptable and competent third party to assist Seller in such investigation, and 2) reimburse Raytheon for costs incurred by Raytheon in responding to or mitigating such Security Incident.

e. **Remedial Actions.** Seller agrees to use commercially reasonable efforts to: (i) contain the Security Incident; (ii) mitigate and minimize the potential harm caused by the Security Incident; and (iii) repair, remediate, and secure affected information systems.

4. **Information Security Audits.** Seller agrees to perform, or to cause its auditor to perform, regular audits of its Information Security Program aligned with industry standards (for example, SSAE 16, SOC 1, SOC 2, and ISO 27001). Seller shall take appropriate steps to address any control weaknesses identified by Seller, or its auditor, as a result of such audit. Upon the request of Raytheon, Seller agrees to provide Raytheon with the results of the most recent security audit of Seller's Information Security Program; provided, however, Seller is under no obligation to provide any information to Raytheon that Seller reasonably determines the disclosure of which would pose a security risk to Seller or its other customers.

   a. Upon the request of Raytheon, Seller will submit its data processing facilities, data files and documentation needed for processing Raytheon Sensitive Information to auditing and/or review by Raytheon or any independent auditor or inspection entity reasonably selected by Raytheon to ascertain compliance with this Agreement, with mutually agreeable notice, scope and timing.

## Section C: INFORMATION SECURITY REQUIREMENTS

Seller's Information Security Program shall include, but not be limited, to the following safeguards to ensure the protection of Raytheon Sensitive Information:

Access Controls on Information Systems. Appropriate procedures and measures to control access to all systems hosting Raytheon Sensitive Information and/or providing services on behalf of Raytheon ("Systems") through the use of physical and logical access control systems that uniquely identify each individual requiring access, grant access only to authorized individuals and, based on the principle of least privileges, prevent unauthorized persons from gaining access to Raytheon Sensitive Information, appropriately limit and control the scope of access granted to any authorized person, and log and monitor all relevant access events.

Authentication Credentials and Procedures. Appropriate procedures for authentication of authorized personnel, including use of commercially acceptable best practice authentication to access any Raytheon Sensitive Information on Raytheon's networks or other systems. Seller agrees to use two-factor authentication for Seller's Systems Administrators remotely accessing and supporting the systems and networks supporting the services provided to Raytheon (or mutually agreeable alternative).

Confidentiality Agreements. Requirement that Seller's employees, agents, subcontractors, and other third parties with access to Raytheon Sensitive Information, enter into signed confidentiality agreements and agree to use the Systems to perform only authorized transactions in support of their job responsibilities.

Qualification of Employees. Appropriate procedures and measures to ascertain the reliability, technical expertise, and personal integrity of all employees, agents, and subcontractors who have access to Systems or Raytheon Sensitive Information.

Obligations of Employees. Appropriate procedures and measures to verify that any employee, agent, or contractor accessing the Raytheon Sensitive Information knows his or her obligations and the consequences of any security breach.

Controls on Employees. Employee background checks, where and to the extent permitted under applicable Law and consistent with Seller's human resources policies, for employees with responsibilities for or access to Raytheon Sensitive Information.

Enforcement. Appropriate disciplinary procedures against individuals who access Raytheon Sensitive Information without authorization, or who otherwise commit security breaches.

Security Awareness and Training. A security awareness and training program for all members of Seller's workforce (including management), which includes training on how to implement and comply with its Information Security Program.

Seller shall monitor access and security logs using commercially acceptable practices and tools for unusual activity including the following:

- Excessive unauthorized/failed logon attempts,
- Use of admin accounts at unusual times,
- Unusual activity at any time,
- Missing activity date/time ranges within the logs,
- Failed backups

Seller should support integration with Raytheon's Simplified Sign-On (SSO) infrastructure, enabling Raytheon users to login to the service with their Raytheon SSO credentials.

Where user authentication via Raytheon SSO is not a current capability and is performed with reusable passwords, adherence to Raytheon Password Requirements is mandatory. At a minimum:

- Passwords are not easily guessed. Password complexity checking is enabled with minimum password length of eight characters. Initial passwords are changed by the user on first use. Passwords are changed immediately if compromise is suspected and are expired every 90 days.
- Passwords are not reused for a period of one year (e.g., history is 4 where supported).
- Passwords are not shared with others.
- Passwords are not displayed, stored or transmitted in plain text or readable form.
- Passwords are disabled after the fifth failed authentication attempt in succession.
- Additions and changes to access levels of users must be approved by appropriate Raytheon management.
- Accounts to be disabled will be communicated by Raytheon and must be enacted by Seller in a timely manner.
- Automated authentication processes such as logon scripts, are protected from unauthorized access and do not contain unencrypted passwords.
- Support procedures for remotely "resetting" a forgotten, lost or compromised means of user identity authentication must at a minimum:
    1) Incorporate multiple means of proving the user's identity when the user is not present to display positive photo identification.
    2) These means must be something that has a high probability of only being known to the user and not general knowledge or easily guessable.
    3) Identity verification data should only be viewable by authorized personnel.
    4) Provide a confirmation of the "reset" to the user via a method other than the method of access reset.

Security Incident Procedures. Policies and procedures to detect, respond to, and otherwise address security incidents, including procedures to monitor systems and to detect actual and attempted attacks on or intrusions into Raytheon Sensitive Information or information systems relating thereto, and procedures to identify and respond to suspected or known security incidents, mitigate harmful effects of security incidents, and document security incidents and their outcomes.

Intrusion Detection/Prevention and Malware. Appropriate and up-to-date procedures and safeguards to protect Raytheon Sensitive Information against the risk of intrusion and the effects of viruses, Trojan horses, worms, and other forms of malware; where appropriate, to monitor each and every access to the Systems or Raytheon Sensitive Information to detect same; and to promptly respond to same.

Standard Information Systems Development and Maintenance Methodology. A standard information systems development and maintenance methodology shall be developed and appropriately applied during development and maintenance projects, including projects that involve the selection and implementation of software that accesses or processes Raytheon Sensitive Information.

Contingency Planning. Policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages Raytheon Sensitive Information or systems that contain such Raytheon Sensitive Information, including a data backup plan and a disaster recovery plan.

Environmental Hazards. Measures to protect against destruction, loss, or damage of Raytheon Sensitive Information or information relating thereto due to potential environmental hazards, such as fire or water damage or technological failures, as well as uninterruptible power supply ("UPS") to ensure constant and steady supply of electricity.

Device and Media Controls. Policies and procedures that govern the receipt and removal of hardware and electronic media that contain Raytheon Sensitive Information into and out of a Seller facility, and the movement of these items within a Seller facility, including policies and procedures to address the final disposition of Raytheon Sensitive Information, and/or the hardware or electronic media on which it is stored, and procedures for removal of such Raytheon Sensitive Information from electronic media before the media are made available for re-use.

Audit controls. Hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic information, including appropriate logs and reports concerning these security requirements and compliance therewith.

Data Integrity. Policies and procedures to ensure the confidentiality, integrity, and availability of Raytheon Sensitive Information and protect it from disclosure, improper alteration, or destruction. Seller agrees to use only currently supported operating systems and versions of software to process Raytheon Sensitive Information.

Program Patching. Appropriate procedures and measures to regularly update and patch computer programs to eliminate vulnerabilities and remove flaws that could otherwise facilitate security breaches.

Data Encryption. Appropriate procedures and measures to encrypt all Raytheon Sensitive Information at rest, in transmission and in backup so that it cannot be accessed by unauthorized person.

Access Control via Internet. Appropriate procedures and measures to prevent the Systems or Raytheon Sensitive Information from being used by unauthorized persons by means of data transmission equipment via the Internet or otherwise.

Remote Control Access. Appropriate procedures and measures to prevent personnel performing remote System support from accessing Raytheon Sensitive Information without end-user permission and presence and/or accountability during remote control sessions and subject to all applicable confidentiality obligations.

Storage and Transmission Security. Technical security measures to guard against unauthorized access to Raytheon Sensitive Information that is being transmitted over an electronic communications network, including a mechanism to encrypt electronic information using industry standard encryption methods

whenever appropriate, such as while in transit or in storage on networks or systems to which unauthorized individuals may have access.

Secure Disposal. All Raytheon Sensitive Information must be securely returned or (ii) properly and immediately disposed of in a secure manner that is reasonably designed to render the information permanently unreadable and not reconstructable into a usable format (i.e., in accordance with the then-current U.S. Department of Defense, or similar data destruction standard or CESG standards, as applicable). Any such return or disposal shall occur at such time that any such Raytheon Sensitive Information is no longer reasonably required to perform the services hereunder, but in any event, no later than upon completion of the relevant services or upon written request of Raytheon. Upon request, Seller will certify that all such Raytheon Sensitive Information has been returned or disposed of in accordance with this Agreement.

System Changes That May Affect the Security of the System. Seller shall make no System change, nor implement any modification of its own Security Plan, that (i) may adversely affect the security of the System or the security of the Raytheon Sensitive Information or other data created, processed, or stored by Seller for Raytheon, (ii) requires Raytheon to install a new version, release, or upgrade of, or replacement for, any hardware or software or to modify any hardware or software, or (iii) requires Raytheon to pay any additional amount for the Services, in each case without first notifying Raytheon.

Subcontractors. To the extent Seller uses third parties to store or otherwise process Raytheon Sensitive Information on behalf of Seller, Seller agrees to: (i) exercise appropriate due diligence in selecting such third parties, (ii) have contracts with such third parties containing obligations and provisions no less protective of Raytheon Sensitive Information than those set forth in this Agreement, and (iii) monitor such third parties to confirm that they have satisfied such obligations and are in compliance with all applicable laws and regulations.

Assigned Security Responsibility. Seller shall designate a security official responsible for the development, implementation, and maintenance of its Information Security Program. Seller shall inform Raytheon as to the person responsible for security.

Testing. Seller shall regularly test the key controls, systems and procedures of its Information Security Program to ensure that they are properly implemented and effective in addressing the threats and risks identified. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

Adjust the Program. Seller shall monitor, evaluate, and adjust, as appropriate, the Information Security Program in light of any relevant changes in technology or industry security standards, internal or external threats to Seller or Raytheon Sensitive Information, requirements of applicable work orders, and Seller's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to information systems.