CYBERSECURITY CONTRACT CLAUSES

1. General Security Statements

a) When supplying hardware or infrastructure to SES and/or services with or without access to SES's data, these shall only be delivered through systems and infrastructure that have specifically been approved by the Supplier following industry security best practices and shall be in scope of the Supplier's certification.

b) SES has developed its Information Security Management System to adhere to the requirements specified in ISO/IEC 27001:2013. The Supplier shall cooperate with SES in maintaining its adherence to these requirements, and the Supplier shall not, through its performance under its commitment to SES, negatively impact this Information Security Management System established by SES.

c) If providing services or interfaces to SES, the Supplier will maintain and comply with globally applicable policies, standards and procedures intended to protect data within their own environments (e.g., systems, networks, facilities) and such policies will govern and control in their environments. For clarity, the Supplier will comply with SES's policies when accessing or operating within SES's environments. The Supplier will provide timely notice of any changes to its policies that may materially degrade the security of the Services, after which the Parties will equitably adjust the terms of their commitment as necessary to appropriately address risk. The Supplier will not use software or hardware that is past its End of Life (EOL) in connection with any Services without a mutually agreed risk management process for such items.

d) Without limiting the generality of the foregoing and subject to any other express agreement between the Parties with respect to any contracted Services , the Supplier has implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect SES's data, services and infrastructure in its environments against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction, as set out below. To the extent SES's data includes personal data, the implementation of and compliance with these measures and any additional security measures set out in the contractual documents are designed to provide an appropriate level of security in respect of the processing of the SES's personal data and shall at all times comply with the applicable data protection laws and regulations.

2. Security Governance

a) *Security Awareness and Training*
If providing a service or interface to SES, the Supplier shall maintain an effective information security awareness, training, and education program, informing all employees and other relevant parties of their information security obligations. The Supplier shall ensure that employees and subcontractors involved in the Service being provided to SES maintain a requisite level of competence in the relevant information security systems in use by the Supplier. The Supplier shall have an information security policy that is communicated to and

available to its staff. Upon request, the Supplier shall provide the information security policy and evidence of the security awareness, training, and education program to SES.

b) *Security Role and Responsibilities*
If providing a service, solution, or interface to SES, the Supplier shall define and document roles and responsibilities related to information security for the service or solution. Roles and responsibilities to be defined include, but are not limited to, those related to the following activities:
- Administering access rights
- Performing configuration changes, system updates, and system backups
- Reviewing access rights
- Performing system monitoring

c) If providing a service, solution, or interface to SES, the Supplier shall maintain documentation regarding roles and responsibilities related to information security for the service or solution, and the Supplier shall review and update this documentation frequently, but at least once per year. Upon request, the Supplier shall provide such documentation to SES.

d) The Supplier personnel with access to SES's data shall comply with the applicable confidentiality obligations.

e) *Change Management*
If providing a service, solution, or interface to SES, the Supplier shall define and maintain processes to govern key security aspects related to system and application change management related to the service or solution. The processes to be implemented by the Supplier shall include, but are not limited to, the following aspects of the service or solution:
- Changes to existing software and the installation of new software shall require a formal request from authorized personnel. Any such request shall be orderly documented.
- Changes to existing software and the installation of new software shall require approval from authorized personnel prior to being put into production. Any such approval shall be orderly documented.
- An impact analysis and other testing shall be conducted before software is installed or changes are put in production. Results of the impact analysis and testing shall be orderly documented.
- Changes made to the production environment should be monitored in an automated manner. Results from such monitoring should be compared to and verified with approved change requests, and any deviations shall be reported and investigated promptly. In cases where a change was applied without appropriate approval, a security incident shall be raised. Documentation related to this process shall be maintained.

3. Asset/ Data Management

a) The Supplier shall at all times implement and maintain physical, electronic and organizational security measures in accordance with the best practices and highest industry standards to protect SES’s data, SES’s materials, and any deliverables against any unauthorized access, use, destruction, loss, disclosure, or improper alteration.

b) In the event of having access to SES’s data, the Supplier will maintain a complete asset inventory of its infrastructure, network, applications, and cloud environments. The Supplier will also maintain an inventory of all its media on which SES's data is stored. Access to the

inventories of such media will be restricted to that Parties' personnel authorized in writing to have such access.

c) In the event of having access to SES's data, the Supplier will classify it to help identify such data and to allow for access to it to be appropriately restricted.

d) In the event of having access to SES's data, the Supplier will require its personnel to obtain appropriate authorization prior to storing SES's data outside of contractually approved locations and systems, remotely accessing SES's data, or processing SES's data outside the Parties' facilities.

e) In the event that the Supplier handles SES's PII data, security controls will include measures such as: i) encryption of SES's data at rest and in motion ii) no less than 128-bit encryption or the maximum allowed by local law in the territory from which information is collected iii) digital certificates signed by a trusted certificate authority

f) In the event of having access to SES's data, the Supplier will have specific data recovery procedures with respect to its systems, in place designed to enable the recovery of SES's data being maintained in its systems.

g) In the event of having access to SES's data, the Supplier will review its data recovery procedures at least annually.

4. Physical and Environmental Security

a) In the event of having access to SES's data, the Supplier will only allow authorized individuals to access its facilities where information systems that process SES's data are located.

b) In the event of having access to SES's data, the Supplier will maintain records of the incoming and outgoing media containing SES's data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of SES's data they contain.

5. Communications and Operations Management

If accessing, processing, or storing SES's data, the following requirements will be applicable to the Supplier:

a) *Operational Policy*
The Supplier will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to SES's data.

b) *Mobile Device Management (MDM)/Mobile Application Management (MAM)*
The Supplier will maintain a policy for its mobile devices that i) enforces device encryption ii) prohibits use of blacklisted apps iii) prohibits enrolment of mobile devices that have been "jail broken."

c) *Malicious Software*

The Supplier will have anti-malware controls to help avoid malicious software gaining unauthorized access to SES's data, services and infrastructure including malicious software originating from public networks.

d) *Data Beyond Borders*

The Supplier will (i) encrypt SES's data that it transmits over public networks (ii) protect SES's data in media leaving its facilities (e.g., through encryption) iii) implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.

e) Event Logging

For its systems containing SES's data or used for providing the Services, the Supplier will log events consistent with its stated policies or standards.

f) Network Security

The Supplier will establish network security controls such as: i) the use of firewalls throughout the company network; ii) Application Gateways; iii) Intrusion Detection and/or Intrusion Prevention systems at ingress points; iv) network segmentation through the use of firewalls or Virtual Local Area Networks (VLANs); v) multifactor authentication for remote access; vi) state-of-the-art antivirus tools.

g) *Network and Application Design and Management*

The Supplier will:

i) Have controls to avoid individuals gaining unauthorized access to SES's data in its systems.
ii) Use email-based data loss prevention to monitor or restrict movement of sensitive data.
iii) Use network-based web filtering to prevent access to unauthorized sites.
iv) Use firefighter IDs or temporary user IDs for production access.
v) Use network intrusion detection and / or prevention in its systems.
vi) Use secure coding standards.
vii) Scan for and remediate OWASP vulnerabilities in its systems.
viii) Maintain up to date server, network, infrastructure, application and cloud security configuration standards.
ix) Scan their respective environments to ensure identified configuration vulnerabilities have been remediated.

h) *Patch Management*

The Supplier will have a patch management procedure that deploys security patches for its systems used to process SES's data or providing the Services that includes (i) defined time allowed to implement patches (not to exceed 90 days for high or medium patches as defined by the Party's respective standard); and (ii) established process to handle emergency or critical patches as soon as practicable.

6. Access Control

If accessing, processing, or storing SES's data, the Supplier will comply with the following requirements:

a) The Supplier will have defined and implemented a formal process for the arrival, transfer, and departure of employees, covering logical and physical access, including access to the site, computer hardware, software, and access to information systems containing or used for processing SES's data.

b) *Access Authorization*

The Supplier will (i) maintain and update a record of personnel authorized to access SES's data via its systems; (ii) when responsible for access provisioning, promptly provision authentication credentials; (iii) deactivate authentication credentials where such credentials

have not been used for a period of time (such period of non-use not to exceed 90 days); (iv) deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days (v) Identify those personnel who may grant, alter or cancel authorized access to data and resources; (vi) ensure that where more than one individual has access to its systems containing SES's data, the individuals have unique identifiers/log-ins (i.e., no shared ids).

c) *Least Privilege*
The Supplier will (i) only permit its technical support personnel to have access to SES's data when needed; (ii) maintain controls that enable emergency access to productions systems via firefighter ids, temporary ids or ids managed by a Privileged Access Management (PAM) solution; (iii) restrict access to SES's data in its systems to only those individuals who require such access to perform their job function; (iv) limit access to SES's data in its systems to only that data minimally necessary to perform the services; (v) support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., developer/ reviewer, developer/tester).

d) *Integrity and Confidentiality*
The Supplier will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.

e) *Authentication (only for low level risk)*
The Supplier will use industry standard (e.g., ISO 27001 or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.

f) *Authentication*
The Supplier will use industry standard (e.g., ISO 27001 or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems. Where authentication mechanisms are based on passwords, the Supplier will (i) require that the passwords are renewed regularly; (ii) require the password to contain at least eight characters and three of the following four types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special (e.g., !, *, &, etc.); (iii) ensure that de-activated or expired identifiers are not granted to other individuals; (iv) monitor repeated attempts to gain access to its information systems using an invalid password; (v) maintain industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed; (vi) use industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.

g) *Multi-Factor Authentication*
The Supplier will implement Multi-Factor Authentication for remote access over virtual private network (VPN) to its systems.

7. Incident Management

a) Unless notification is delayed by the actions or demands of a law enforcement agency, the Supplier shall report all Information Security Incidents (as defined below) to SES following determination by the Supplier that an information security incident has occurred. The occurrence of an information security incident shall be reported immediately in detail to SES via alert@ses.com and in no event more than twenty-four (24) hours after the information security incident.

b) “Information Security Incidents” shall mean: (A) any unlawful access to the Supplier’s systems that store/process SES’s data or are part of a service provided to SES; (B) unauthorized access to the Supplier’s systems that results in potential loss, disclosure or destruction of SES's data or access to SES's services or infrastructure; and (C) any other unwanted or unexpected events that have a significant probability of compromising the security of SES’s data, services or infrastructure.

c) The Supplier shall take immediate reasonable measures to promptly mitigate the cause of an Information Security Incident and shall take immediate reasonable corrective measures to prevent future information security incidents. The Supplier shall keep a record of mitigation measures taken and shall inform SES of the mitigation measures immediately, but in no event more than twenty-four (24) hours after the mitigation measures have been implemented.

d) In the event of an Information Security Incident, the Supplier shall (i) conduct an investigation concerning the Information Security Incident and provide a copy of an Information Security Incident report to SES that sets forth details regarding the Information Security Incident and the steps taken to remedy the Information Security Incident, (ii) cooperate with any investigation concerning the Information Security Incident requested by SES or any regulator or other governmental body with oversight over the Information Security Incident; (iii) cooperate with SES to comply with applicable laws concerning such Information Security Incident, including any notification that may be required to individuals whose personally identifiable information was compromised as a result of an Information Security Incident; (iv) promptly correct any vulnerabilities and deficiencies related to the Information Security Incident at no additional charge to SES; and (v) be liable for any expenses associated with the Information Security Incident including without limitation the cost of any required legal compliance (e.g., notices required by applicable laws) and the expenses related to the investigation into the Information Security Incident. In no event will the Supplier serve any notice of or otherwise publicize an Information Security Incident that affects or relates to SES’s data, SES’s customer materials, and/or SES’s systems without the prior written consent of SES, unless required by law. The results of the investigation pursuant to this will be the Confidential Information of the Supplier.

e) SES agrees that Information Security Incidents do not include unsuccessful access attempts or similar events that do not compromise the security or privacy of the Supplier’s systems, including pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems.

f) *Security Breach Response Process*
The Supplier will maintain a record of its own security breaches in its systems with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.

g) *Service Monitoring*
The Supplier security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary.

h) The Supplier shall perform 24/7 monitoring of access to the Supplier’s environments using its network intrusion detection and / or prevention tools.

8. <u>Workstations</u>

If providing a service or solution with or without access to SES's data, the Supplier will implement controls for all workstations it provides that are used in connection with service delivery incorporating the following (i) software agent that manages overall compliance of workstation and reports at a minimum on a weekly basis to a central server (ii) encrypted hard drive (iii) patching process so that workstations are patched within the documented patching schedule (iv) ability to prevent blacklisted software from being installed (v) antivirus with a minimum weekly scan (vi) host firewall enabled

9. Regulatory Compliance

If providing a service or solution with or without access to SES's data, the following points will be applicable to the Supplier/contractor-

a) The Supplier shall use state-of-the-art technology and industry good practices in relation to information security. The Supplier shall maintain, until the completion of the Services, any and all standard certifications relevant to the Services and held by the Supplier at the time of this contractual commitment.

b) The Supplier shall ensure that all the Supplier owned and managed systems and facilities utilized in the performance of the applicable contractual documents shall be covered by and subject to the certification held as per item 9a) above.

c) If any of the certifications enumerated in 9a) are no longer held by the Supplier during the term of the contractual commitment, the Supplier shall inform SES immediately in writing and in any case no later than 72 hours after the loss of the certification. In such cases, at SES's option, the Supplier will fully support additional security assessments conducted by SES and will implement reasonable controls to adhere to a similarly strong security posture.

d) *Supplier's Supply Chain*
The Supplier shall ensure that its subcontractors involved in the service provision to SES implement the same level of information security required by this contractual commitment. Where relevant, the Supplier shall contractually impose and flow down the provisions of this Agreement to its subcontractors. This shall include the use of state-of-the-art technology; the use of industry good practices; the maintenance of standard certifications; the implementation of an Information Security Management Policy; and the implementation of an employee information security awareness, training, and education program. The Supplier shall at all times remain responsible and liable towards SES for the acts and omissions of its subcontractors.

10. Audit Rights

Upon SES's reasonable written request with no less than thirty (30) days' notice during the term, and no more than once per calendar year, the Supplier agrees to cooperate and assist SES with information security audits regarding the Supplier 's compliance with the terms and conditions regarding information security hereunder. This cooperation shall include, but not be limited to, (i) providing evidence of certification, policies, training and awareness program, and compliance related to information security; (ii) making available to SES an executive summary of the Supplier's most recent information security tests, including

remedial actions taken; and (iii) permit SES to review the Supplier's information security program.

11. Acquisition Process, Requirements / Properties, Documentation, Development Process

a) If the Supplier has been provided by SES with requirements, descriptions, and criteria including –

- Security and privacy functional requirements;
- Strength of mechanism requirements;
- Security and privacy assurance requirements;
- Controls needed to satisfy the security and privacy requirements as well as in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
- Security and privacy documentation requirements;
- Requirements for protecting security and privacy documentation;
- Description of the system development environment and environment in which the system is intended to operate;
- Allocation of responsibility or identification of parties responsible for information security, privacy, and supply chain risk management;
  Acceptance criteria.

, then the Supplier shall provide an IT system or service in consideration and compliance to these functional and non-functional requirements. In case of any deviations, they shall inform SES up front in writing and request written approval for such deviations.

b) If providing software, IT solution or IT services to SES, the Supplier shall provide a description of the functional properties, design and implementation information of the security controls as implemented or to be implemented. "Functional properties of security controls" shall describe the functionality (i.e., security or privacy capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls. "Design and Implementation of security controls" shall describe security-relevant external system interfaces, high-level design, low-level design, source code or hardware schematics, and design and implementation information at a level of detail to support anomaly analysis.

c) If providing software, IT solutions or IT services to SES, the Supplier shall provide a documented design specification and security and privacy architecture that:

- Accurately and completely describes the required security and privacy functionality, and the allocation of controls among physical and logical components, and
- Expresses how individual security and privacy functions, mechanisms, and services work together to provide required security and privacy capabilities.

d) If providing software to SES, the Supplier shall demonstrate the use of a Software Development Lifecycle (SDLC) process and Secure Engineering Principles (SEPs) that adhere to the requirements specified in NIST 800-53 r5, including –

- Industry best practice system/security engineering methods;
- Software development methods;

- Testing/evaluation/validation techniques;
- Quality control processes

e) If providing software to SES, the Supplier shall perform a criticality analysis (e.g. ref. NISTIR 8179) at major milestones of the Software Development Lifecycle (SDLC)at an adequate level of rigor. The output of this analysis shall be provided to SES for review and acceptance.

f) If using open-source software to provide an IT service or IT solution to SES, the Supplier shall use such open-source software from reputable sources only.

g) If providing software to SES, the Supplier shall demonstrate the use of a documented system and software development process that generally adheres to the requirements specified in NIST 800-53 r5 and shall provide SES with a copy of the respective documentation for review. Supplier shall comply with the following:
   - Explicit addressing of security and privacy requirements.
   - Identification of standards and tools used in the development process;
   - Documentation of specific tool options and tool configurations used in the development process;
   - Documentation, Management, and Assurance of integrity of changes to the process and / or tools used in development,
   - Review process of the afore mentioned requirements.

12. Security Configuration, Cryptographic Modules

If providing an IT service or IT solution to SES:

a) The Supplier shall ensure adequate hardening measures (Centre for Internet Security Benchmark or equivalent) have been applied with prior intimation to SES with respect to the security levels or profiles used. This agreed upon configuration baseline shall be used as the default for any subsequent system, component, or service reinstallation or upgrade / update.

b) The Supplier shall, throughout the IT system or service, only use information assurance and information assurance-enabled information technology products that have been successfully evaluated against a National Information Assurance Partnership (NIAP, ref. NIAP CCEVS), or rely on cryptographic modules that are Federal Information Processing Standard(FIPS)-validated or National Security Agency (NSA)-approved (ref. NIST CMVP).

13. Detailed Documentation Requirements

a) If delivering IT hardware, IT services, IT solutions or software to SES, the Supplier shall provide

(i) complete and accurate documentation of all functions, ports, protocols, and services intended for organizational use.

(ii) an administration documentation that describes –

- Secure configuration, installation, and operation of the system, component, or service;
- Effective use and maintenance of security functions / mechanisms.
- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

(iii) a user documentation for the system or service that describes:

- User-accessible security functions/mechanisms and how to effectively use those security functions / mechanisms;
- Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner;
- User responsibilities in maintaining the security of the system, component, or service.

14. Vulnerability Scanning

If providing software, IT solutions or service to SES:

a) The Supplier shall perform an automated vulnerability analysis using industry best practices tools, determine the exploitation potential for discovered vulnerabilities, determine potential risk mitigations for discovered vulnerabilities, and deliver the outputs of the tools and results to SES for review and acceptance.

b) The Supplier shall perform threat modelling and a vulnerability analysis for the information system at depth to include static analyses, dynamic analyses, simulations, and penetration testing that:

- Uses mission impact, operational environment, known or assumed threats, and acceptable risk levels;
  - Employs either Department Of Defense (DoD) or Industry Best Practices tools and methods;
  - Produces evidence that meets the level of objective quality evidence for the Agents of the Security Control Assessor (ASCA).